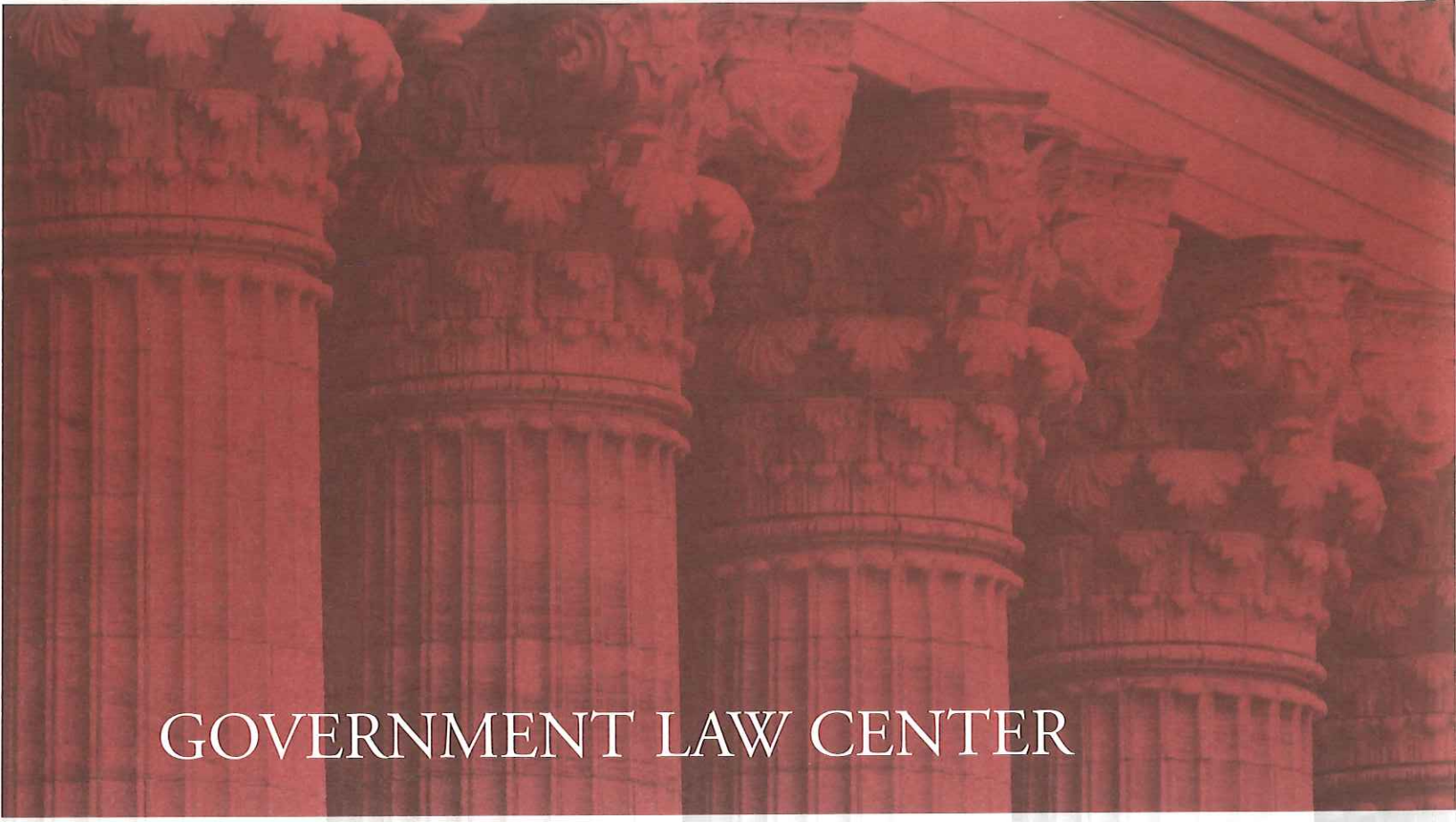


GOVERNMENT LAW CENTER

2017
Warren M. Anderson Legislative Breakfast Seminar Series

"Cybersecurity: Protection, Regulation and Privacy"

February 14, 2017

ALBANY LAW SCHOOL

Warren M. Anderson Legislative Breakfast Seminar Series
Cybersecurity: Protection, Regulation and Privacy

February 14, 2017

SPEAKER BIOGRAPHIES

ASSOCIATE DEAN ANTONY HAYNES joined Albany Law School in December 2015 as Associate Dean for Strategic Initiatives and Information Systems, Assistant Professor, and Executive Director of the Schaffer Law Library. He teaches a seminar on Cybersecurity Law and Policy designed to introduce students to the issues involved in cyber security law, both from a national policy standpoint and from a corporate counsel view. Dean Haynes has extensive litigation experience in the intellectual property, securities, and criminal defense areas. He served as Associate at the law firm Quinn Emanuel Urquhart & Sullivan, LLP, in Washington, D.C., and before that at Williams & Connolly LLP, in Washington, D.C. Prior to practicing law, Associate Dean Haynes was an Assistant Professor of Computer Science at the U.S. Air Force Academy, where he taught courses in programming, developed the Academy's Information Assurance curriculum, and created the intercollegiate Cyber Defense Exercise. He has extensive experience with a host of software and hardware technologies. He was an associate at Chatham Financial Corporation, Capital Markets, in Kennett Square, PA, where he led a company-wide software effort, wrote financial software and coordinated technical developers. As CEO and President of Exaprime LLC – a company he founded in Chadds Ford, PA, to provide technology consulting to academic institutions – he developed an online survey system for the University of Pennsylvania Center for Clinical Epidemiology and Biostatistics. Associate Dean Haynes received a J.D., *cum laude*, from Georgetown University Law Center, where he was a Lane Fellow, a Legal Writing Fellow, and Best Oralist for the Cardozo Moot Court Competition. He received an M.S. in Computer Science from the University of Illinois at Urbana-Champaign, where his thesis focused on machine learning and expert systems. He is a distinguished graduate of the U.S. Air Force Academy, where he was recognized as the top computer science graduate. Associate Dean Haynes is an entrepreneur who leverages his background in computer science, technology, business and the law to advise startup companies. In addition to advising startups, he has spent time acquiring and growing companies.

MARY KAVANEY, ESQ., currently serves as the Chief Administrative Officer for the Global Cyber Alliance. Her responsibilities include strategy, personnel, legal and work with the cyber risk task forces. Prior to GCA, Ms. Kavaney worked at the Center for Internet Security, where she developed relationships with law enforcement and other partners around the state. From 2007 to 2015 Ms. Kavaney served as the Assistant Deputy Secretary for Public Safety for the New York State Governor's Office working towards the passage of the state's first anti-human trafficking law, all crimes DNA law and New York's gun control law, (the Safe Act). Prior to working in the Governor's Office of Public Safety, she was appointed as General Counsel at the Division of Criminal Justice Services and for eight years she ran the Poughkeepsie Regional Office for the

New York State Attorney General. Ms. Kavaney served as an Assistant District Attorney for four and half years at the Orange County District Attorney's Office. She is a graduate of Syracuse University College of Law.

BRIAN NUSSBAUM, PhD is an assistant professor in the College of Emergency Preparedness, Homeland Security and Cybersecurity at the University at Albany. He focuses on cybersecurity and cyber threats, terrorism and terrorism analysis, homeland security, risk and intelligence analysis, and critical infrastructure protection. He also serves as a fellow of the Cybersecurity Initiative at New America in Washington D.C., an affiliate scholar of the Center for Internet and Society (CIS) at Stanford Law School, and a senior fellow with the Center for Cyber and Homeland Security (CCHS) at George Washington University. Dr. Nussbaum formerly served as senior intelligence analyst with the New York State Office of Counter Terrorism (OCT), a part of the New York State Division of Homeland Security and Emergency Services (DHSES). He oversaw both terrorism and cyber threat analysis efforts at New York's designated state fusion center, the New York State Intelligence Center (NYSIC). Dr. Nussbaum served as a subject matter expert on international terrorism, and helped to create NYSIC's Cyber Analysis Unit (CAU). He worked for almost a decade in New York State's homeland security agencies and was the author and project lead on the New York State risk-based funding formula, a formula that was used to distribute over $300 million in Homeland Security Grant Program (HSGP) funds between 2006 and 2014. Additionally, Dr. Nussbaum served as the first ever Visiting Professor of Homeland Defense in the Strategic Wargaming Division at the Center for Strategic Leadership and Development, part of the United States Army War College in Carlisle, PA (2012-2013). Nussbaum received a PhD and MA in Political Science from the University at Albany and a BA in Political Science from Binghamton University. His work has appeared in numerous books and journals including Studies in Conflict and Terrorism, Global Crime, and the Journal of Applied Security Research.

DEIRDRE O'CALLAGHAN, ESQ. is the Chief Counsel of the Center for Internet Security. In that role, she is responsible for the legal overview of the organization's activities, contracts and agreements and administrative matters. She is a member of the Executive Team and supports the CEO in the organization's strategic and business planning efforts. Ms. O'Callaghan has practiced law for over 25 years, and has extensive experience both as in-house counsel for Terra Mesa Development Group, Centex Homes and American Skiing Company, and as a partner in the Portland, ME, law firm Preti Flaherty. Prior to joining CIS, she served as General Counsel of Gas Turbine Efficiency, Ltd., an international manufacturing and technology company in Troy, NY. She is a graduate of Columbia University School of Law and the University of Maine.

Cybersecurity: Protection, Regulation and Privacy

February 14, 2017

List of Materials

S924/A3448: Cyber Security Initiative Bill text, summary and sponsor memo

S926/A3451: Cyber Security Report Bill text, summary and sponsor memo

S953/A3311: Cyber Terrorism in the First and Second Degree
Bill text, summary and sponsor memo

Ethics & Technology: The Risks and Legal Ethics of Technology and Legal Practice
Haynes 2017

Ethics and Cyber Ayiotis 2015

Cyber Security Ethics McCauley 2016

IRS Alert: Dangerous W-2 Phishing Scam 2017

MS-ISAC Security Primer: Spear Phishing 2016

State, Local, Tribal and Territorial (SLTT) Government Outlook from the Multi-State Information Sharing and Analysis Center (MS-ISAC) 2016

Getting Ahead of Advanced Threats: Achieving Intelligence-Driven Information Security -
A Security for Business Innovation Council Report

MS-ISAC Security Primer: Emergency Preparedness for Cyber Infrastructure 2016

Links to further reading

State of Michigan: Cyber Disruption Response Plan 2015

State of Iowa: Cybersecurity Strategy 2016

State of the States on Cybersecurity 2015

National Governors Association Issue Brief:
Enhancing the Role of Fusion Centers in Cybersecurity 2015

National Association of Chief Information Officers of States:
Cyber Disruption Response Planning Guide 2016

US Department of Homeland Security:
Strategic Principles for Securing the Internet of Things 2016

The CIS Critical Security Controls for Effective Cyber Defense 2016

Privacy Implications Guide for the CIS Critical Security Controls

Cybersecurity Initiative
Senate Bill 924, Assembly Bill 3448

State of New York

2017-2018 Regular Sessions
I N S E N A T E
January 5, 2017

_____

Introduced by Sens. CROCI, AKSHAR, AVELLA, DeFRANCISCO, FUNKE, GOLDEN -- read twice and ordered printed, and when printed to be committed to the Committee on Veterans, Homeland Security and Military Affairs

AN ACT to amend the executive law, in relation to a cyber security initiative

THE PEOPLE OF THE STATE OF NEW YORK, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. The executive law is amended by adding a new section 719 to read as follows:

S 719. NEW YORK STATE CYBER SECURITY INITIATIVE. 1. LEGISLATIVE FINDINGS. THE LEGISLATURE FINDS AND DECLARES THAT REPEATED CYBER INTRUSIONS INTO CRITICAL INFRASTRUCTURE, EFFECTING GOVERNMENT, PRIVATE SECTOR BUSINESS, AND CITIZENS OF THE STATE OF NEW YORK, HAVE DEMONSTRATED THE NEED FOR IMPROVED CYBER SECURITY.

THE LEGISLATURE FURTHER FINDS AND DECLARES THAT THIS CYBER THREAT CONTINUES TO GROW AND REPRESENTS ONE OF THE MOST SERIOUS PUBLIC SECURITY CHALLENGES THAT NEW YORK MUST CONFRONT. MOREOVER, THE SECURITY OF THE STATE OF NEW YORK DEPENDS ON THE RELIABLE FUNCTIONING OF NEW YORK STATE'S CRITICAL INFRASTRUCTURE, AND PRIVATE SECTOR BUSINESS INTERESTS, AS WELL AS THE PROTECTION OF THE FINANCES AND INDIVIDUAL LIBERTIES OF EVERY CITIZEN, IN THE FACE OF SUCH THREATS.

THE LEGISLATURE ADDITIONALLY FINDS AND DECLARES THAT TO ENHANCE THE SECURITY, PROTECTION AND RESILIENCE OF NEW YORK STATE'S CRITICAL INFRASTRUCTURE, AND PRIVATE SECTOR BUSINESS INTERESTS, AS WELL AS THE

PROTECTION OF THE FINANCES AND INDIVIDUAL LIBERTIES OF EVERY CITIZEN,
THE STATE OF NEW YORK MUST PROMOTE A CYBER ENVIRONMENT THAT ENCOURAGES
EFFICIENCY, INNOVATION, AND ECONOMIC PROSPERITY, AND THAT CAN OPERATE
WITH SAFETY, SECURITY, BUSINESS CONFIDENTIALITY, PRIVACY, AND CIVIL
LIBERTY.
THE LEGISLATURE FURTHER FINDS AND DECLARES THAT TO CREATE SUCH A SAFE
AND SECURE CYBER ENVIRONMENT FOR GOVERNMENT, PRIVATE SECTOR BUSINESS AND
EXPLANATION--Matter in ITALICS (underscored) is new; matter in brackets
[ ] is old law to be omitted.
LBD02129-01-7

INDIVIDUAL CITIZENS, NEW YORK MUST ADVANCE, IN ADDITION TO ITS CURRENT
EFFORTS IN THIS FIELD, A NEW YORK STATE CYBER SECURITY INITIATIVE, THAT
ESTABLISHES A NEW YORK STATE CYBER SECURITY ADVISORY BOARD; A NEW YORK
STATE CYBER SECURITY PARTNERSHIP PROGRAM WITH THE OWNERS AND OPERATORS
OF CRITICAL INFRASTRUCTURE, PRIVATE SECTOR BUSINESS, ACADEMIA, AND INDI-
VIDUAL CITIZENS TO IMPROVE, DEVELOP AND IMPLEMENT RISK-BASED STANDARDS
FOR GOVERNMENT, PRIVATE SECTOR BUSINESSES AND INDIVIDUAL CITIZENS; AND A
NEW YORK STATE CYBER SECURITY INFORMATION SHARING PROGRAM.
2. CRITICAL INFRASTRUCTURE AND INFORMATION SYSTEMS. AS USED IN THIS
SECTION, THE TERM "CRITICAL INFRASTRUCTURE AND INFORMATION SYSTEMS"
SHALL MEAN ALL SYSTEMS AND ASSETS, WHETHER PHYSICAL OR VIRTUAL, SO VITAL
TO THE GOVERNMENT, PRIVATE SECTOR BUSINESSES AND INDIVIDUAL CITIZENS OF
THE STATE OF NEW YORK THAT THE INCAPACITY OR DESTRUCTION OF SUCH SYSTEMS
AND ASSETS WOULD HAVE A DEBILITATING IMPACT TO THE SECURITY, ECONOMY, OR
PUBLIC HEALTH OF THE INDIVIDUAL CITIZENS, GOVERNMENT, OR PRIVATE SECTOR
BUSINESSES OF THE STATE OF NEW YORK.

3. NEW YORK STATE CYBER SECURITY ADVISORY BOARD. (A) THERE SHALL BE WITHIN THE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES, A NEW YORK STATE CYBER SECURITY ADVISORY BOARD, WHICH SHALL ADVISE THE GOVERNOR AND THE LEGISLATURE ON DEVELOPMENTS IN CYBER SECURITY AND MAKE RECOMMENDATIONS FOR PROTECTING THE STATE'S CRITICAL INFRASTRUCTURE AND INFORMATION SYSTEMS.

(B) THE BOARD MEMBERS SHALL CONSIST OF ELEVEN MEMBERS APPOINTED BY THE GOVERNOR, WITH THREE MEMBERS APPOINTED UPON RECOMMENDATION OF THE TEMPORARY PRESIDENT OF THE SENATE, AND THREE MEMBERS APPOINTED AT THE RECOMMENDATION OF THE SPEAKER OF THE ASSEMBLY. ALL MEMBERS SO APPOINTED SHALL HAVE EXPERTISE IN CYBER SECURITY, TELECOMMUNICATIONS, INTERNET SERVICE DELIVERY, PUBLIC PROTECTION, COMPUTER SYSTEMS AND/OR COMPUTER NETWORKS.

(C) THE BOARD SHALL INVESTIGATE, DISCUSS AND MAKE RECOMMENDATIONS CONCERNING CYBER SECURITY ISSUES INVOLVING BOTH THE PUBLIC AND PRIVATE SECTORS AND WHAT STEPS CAN BE TAKEN BY NEW YORK STATE TO PROTECT CRITICAL CYBER INFRASTRUCTURE, FINANCIAL SYSTEMS, TELECOMMUNICATIONS NETWORKS, ELECTRICAL GRIDS, SECURITY SYSTEMS, FIRST RESPONDER SYSTEMS AND INFRASTRUCTURE, PHYSICAL INFRASTRUCTURE SYSTEMS, TRANSPORTATION SYSTEMS, AND SUCH OTHER AND FURTHER SECTORS OF STATE GOVERNMENT AND THE PRIVATE SECTOR AS THE ADVISORY BOARD SHALL DEEM PRUDENT.

(D) THE PURPOSE OF THE ADVISORY BOARD SHALL BE TO PROMOTE THE DEVELOPMENT OF INNOVATIVE, ACTIONABLE POLICIES TO ENSURE THAT NEW YORK STATE IS IN THE FOREFRONT OF PUBLIC CYBER SECURITY DEFENSE.

(E) THE MEMBERS OF THE ADVISORY BOARD SHALL RECEIVE NO COMPENSATION

41 FOR THEIR SERVICES, BUT MAY RECEIVE ACTUAL AND NECESSARY EXPENSES, AND
42 SHALL NOT BE DISQUALIFIED FOR HOLDING ANY OTHER PUBLIC OFFICE OR EMPLOY-
43 MENT BY MEANS OF THEIR SERVICE AS A MEMBER OF THE ADVISORY BOARD.
44 (F) THE ADVISORY BOARD SHALL BE ENTITLED TO REQUEST AND RECEIVE, AND
45 SHALL BE PROVIDED WITH, SUCH FACILITIES, RESOURCES AND DATA OF ANY AGEN-
46 CY, DEPARTMENT, DIVISION, BOARD, BUREAU, COMMISSION, OR PUBLIC AUTHORITY
47 OF THE STATE, AS THEY MAY REASONABLY REQUEST, TO CARRY OUT PROPERLY
48 THEIR POWERS, DUTIES AND PURPOSE.
49 4. NEW YORK STATE CYBER SECURITY INFORMATION SHARING AND ANALYSIS
50 PROGRAM. (A) THE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES,
51 IN CONSULTATION WITH THE DIVISION OF THE STATE POLICE, THE STATE OFFICE
52 OF INFORMATION TECHNOLOGY SERVICES, AND THE CENTER FOR INTERNET SECURI-
53 TY, SHALL ESTABLISH, WITHIN SIXTY DAYS OF THE EFFECTIVE DATE OF THIS
54 SECTION, A VOLUNTARY NEW YORK STATE CYBER SECURITY INFORMATION SHARING
55 AND ANALYSIS PROGRAM.

1 (B) IT SHALL BE THE PURPOSE OF THE NEW YORK STATE CYBER SECURITY
2 INFORMATION SHARING AND ANALYSIS PROGRAM TO INCREASE THE VOLUME, TIMELI-
3 NESS, AND QUALITY OF CYBER THREAT INFORMATION SHARED WITH NEW YORK STATE
4 PUBLIC AND PRIVATE SECTOR ENTITIES SO THAT THESE ENTITIES MAY BETTER
5 PROTECT AND DEFEND THEMSELVES AGAINST CYBER THREATS AND TO PROMOTE THE
6 DEVELOPMENT OF EFFECTIVE DEFENSES AND STRATEGIES TO COMBAT, AND PROTECT
7 AGAINST, CYBER THREATS AND ATTACKS.
8 (C) TO FACILITATE THE PURPOSES OF THE NEW YORK STATE CYBER SECURITY
9 INFORMATION SHARING AND ANALYSIS PROGRAM, THE DIVISION OF HOMELAND SECU-

RITY AND EMERGENCY SERVICES, SHALL PROMULGATE REGULATIONS, IN ACCORDANCE
WITH THE PROVISIONS OF THIS SUBDIVISION.
(D) THE REGULATIONS SHALL PROVIDE FOR THE TIMELY PRODUCTION OF UNCLAS-
SIFIED REPORTS OF CYBER THREATS TO NEW YORK STATE AND ITS PUBLIC AND
PRIVATE SECTOR ENTITIES, INCLUDING THREATS THAT IDENTIFY A SPECIFIC
TARGETED ENTITY.
(E) THE REGULATIONS SHALL ADDRESS THE NEED TO PROTECT INTELLIGENCE AND
LAW ENFORCEMENT SOURCES, METHODS, OPERATIONS, AND INVESTIGATIONS, AND
SHALL FURTHER ESTABLISH A PROCESS THAT RAPIDLY DISSEMINATES THE REPORTS
PRODUCED PURSUANT TO PARAGRAPH (D) OF THIS SUBDIVISION, TO BOTH ANY
TARGETED ENTITY AS WELL AS SUCH OTHER AND FURTHER PUBLIC AND PRIVATE
ENTITIES AS THE DIVISION SHALL DEEM NECESSARY TO ADVANCE THE PURPOSES OF
THIS SUBDIVISION.
(F) THE REGULATIONS SHALL PROVIDE FOR PROTECTIONS FROM LIABILITY FOR
ENTITIES SHARING AND RECEIVING INFORMATION WITH THE NEW YORK STATE CYBER
SECURITY INFORMATION AND ANALYSIS PROGRAM, SO LONG AS THE ENTITY ACTED
IN GOOD FAITH.
(G) THE REGULATIONS SHALL FURTHER ESTABLISH A SYSTEM FOR TRACKING THE
PRODUCTION, DISSEMINATION, AND DISPOSITION OF THE REPORTS PRODUCED IN
ACCORDANCE WITH THE PROVISIONS OF THIS SUBDIVISION.
(H) THE REGULATIONS SHALL ALSO ESTABLISH AN ENHANCED CYBER SECURITY
SERVICES PROGRAM, WITHIN NEW YORK STATE, TO PROVIDE FOR PROCEDURES,
METHODS AND DIRECTIVES, FOR A VOLUNTARY INFORMATION SHARING PROGRAM,
THAT WILL PROVIDE CYBER THREAT AND TECHNICAL INFORMATION COLLECTED FROM
BOTH PUBLIC AND PRIVATE SECTOR ENTITIES, TO SUCH PRIVATE AND PUBLIC

35 SECTOR ENTITIES AS THE DIVISION DEEMS PRUDENT, TO ADVISE ELIGIBLE CRIT-
36 ICAL INFRASTRUCTURE COMPANIES OR COMMERCIAL SERVICE PROVIDERS THAT OFFER
37 SECURITY SERVICES TO CRITICAL INFRASTRUCTURE ON CYBER SECURITY THREATS
38 AND DEFENSE MEASURES.
39 (I) THE REGULATIONS SHALL ALSO SEEK TO DEVELOP STRATEGIES TO MAXIMIZE
40 THE UTILITY OF CYBER THREAT INFORMATION SHARING BETWEEN AND ACROSS THE
41 PRIVATE AND PUBLIC SECTORS, AND SHALL FURTHER SEEK TO PROMOTE THE USE OF
42 PRIVATE AND PUBLIC SECTOR SUBJECT MATTER EXPERTS TO ADDRESS CYBER SECU-
43 RITY NEEDS IN NEW YORK STATE, WITH THESE SUBJECT MATTER EXPERTS PROVID-
44 ING ADVICE REGARDING THE CONTENT, STRUCTURE, AND TYPES OF INFORMATION
45 MOST USEFUL TO CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS IN REDUCING
46 AND MITIGATING CYBER RISKS.
47 (J) THE REGULATIONS SHALL FURTHER SEEK TO ESTABLISH A CONSULTATIVE
48 PROCESS TO COORDINATE IMPROVEMENTS TO THE CYBER SECURITY OF CRITICAL
49 INFRASTRUCTURE, WHERE AS PART OF THE CONSULTATIVE PROCESS, THE PUBLIC
50 AND PRIVATE ENTITIES OF THE STATE OF NEW YORK SHALL ENGAGE AND CONSIDER
51 THE ADVICE OF THE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES,
52 THE DIVISION OF THE STATE POLICE, THE STATE OFFICE OF INFORMATION TECH-
53 NOLOGY SERVICES, THE CENTER FOR INTERNET SECURITY, THE NEW YORK STATE
54 CYBER SECURITY ADVISORY BOARD, THE PROGRAMS ESTABLISHED BY THIS SUBDIVI-
55 SION, AND SUCH OTHER AND FURTHER PRIVATE AND PUBLIC SECTOR ENTITIES,

1 UNIVERSITIES, AND CYBER SECURITY EXPERTS AS THE DIVISION OF HOMELAND
2 SECURITY AND EMERGENCY SERVICES MAY DEEM PRUDENT.
3 (K) THE REGULATIONS SHALL FURTHER SEEK TO ESTABLISH A BASELINE FRAME-

4 WORK TO REDUCE CYBER RISK TO CRITICAL INFRASTRUCTURE, AND SHALL SEEK TO
5 HAVE THE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES, IN
6 CONSULTATION WITH THE DIVISION OF STATE POLICE, THE STATE OFFICE OF
7 INFORMATION TECHNOLOGY SERVICES, AND THE CENTER FOR INTERNET SECURITY,
8 LEAD THE DEVELOPMENT OF A VOLUNTARY FRAMEWORK TO REDUCE CYBER RISKS TO
9 CRITICAL INFRASTRUCTURE, TO BE KNOWN AS THE CYBER SECURITY FRAMEWORK,
10 WHICH SHALL:
11 (I) INCLUDE A SET OF STANDARDS, METHODOLOGIES, PROCEDURES, AND PROC-
12 ESSES THAT ALIGN POLICY, BUSINESS, AND TECHNOLOGICAL APPROACHES TO
13 ADDRESS CYBER RISKS;
14 (II) INCORPORATE VOLUNTARY CONSENSUS STANDARDS AND INDUSTRY BEST PRAC-
15 TICES TO THE FULLEST EXTENT POSSIBLE;
16 (III) PROVIDE A PRIORITIZED, FLEXIBLE, REPEATABLE, PERFORMANCE-BASED,
17 AND COST-EFFECTIVE APPROACH, INCLUDING INFORMATION SECURITY MEASURES AND
18 CONTROLS, TO HELP OWNERS AND OPERATORS OF CRITICAL INFRASTRUCTURE IDEN-
19 TIFY, ASSESS, AND MANAGE CYBER RISK;
20 (IV) FOCUS ON IDENTIFYING CROSS-SECTOR SECURITY STANDARDS AND GUIDE-
21 LINES APPLICABLE TO CRITICAL INFRASTRUCTURE;
22 (V) IDENTIFY AREAS FOR IMPROVEMENT THAT SHOULD BE ADDRESSED THROUGH
23 FUTURE COLLABORATION WITH PARTICULAR SECTORS AND STANDARDS-DEVELOPING
24 ORGANIZATIONS;
25 (VI) ENABLE TECHNICAL INNOVATION AND ACCOUNT FOR ORGANIZATIONAL
26 DIFFERENCES, TO PROVIDE GUIDANCE THAT IS TECHNOLOGY NEUTRAL AND THAT
27 ENABLES CRITICAL INFRASTRUCTURE SECTORS TO BENEFIT FROM A COMPETITIVE
28 MARKET FOR PRODUCTS AND SERVICES THAT MEET THE STANDARDS, METHODOLOGIES,
29 PROCEDURES, AND PROCESSES DEVELOPED TO ADDRESS CYBER RISKS;
30 (VII) INCLUDE GUIDANCE FOR MEASURING THE PERFORMANCE OF AN ENTITY IN

IMPLEMENTING THE CYBER SECURITY FRAMEWORK;
(VIII) INCLUDE METHODOLOGIES TO IDENTIFY AND MITIGATE IMPACTS OF THE
CYBER SECURITY FRAMEWORK AND ASSOCIATED INFORMATION SECURITY MEASURES OR
CONTROLS ON BUSINESS CONFIDENTIALITY, AND TO PROTECT INDIVIDUAL PRIVACY
AND CIVIL LIBERTIES; AND
(IX) ENGAGE IN THE REVIEW OF THREAT AND VULNERABILITY INFORMATION AND
TECHNICAL EXPERTISE.
(L) THE REGULATIONS SHALL ADDITIONALLY ESTABLISH A VOLUNTARY CRITICAL
INFRASTRUCTURE CYBER SECURITY PROGRAM TO SUPPORT THE ADOPTION OF THE
CYBER SECURITY FRAMEWORK BY OWNERS AND OPERATORS OF CRITICAL INFRASTRUC-
TURE AND ANY OTHER INTERESTED ENTITIES, WHERE UNDER THIS PROGRAM IMPLE-
MENTATION GUIDANCE OR SUPPLEMENTAL MATERIALS WOULD BE DEVELOPED TO
ADDRESS SECTOR-SPECIFIC RISKS AND OPERATING ENVIRONMENTS, AND RECOMMEND
LEGISLATION FOR ENACTMENT TO ADDRESS CYBER SECURITY ISSUES.
(M) IN DEVELOPING THE NEW YORK STATE CYBER SECURITY INFORMATION SHAR-
ING AND ANALYSIS PROGRAM IN ACCORDANCE WITH THE PROVISIONS OF THIS
SUBDIVISION, THE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES,
IN CONSULTATION WITH THE DIVISION OF STATE POLICE, THE STATE OFFICE OF
INFORMATION TECHNOLOGY SERVICES, AND THE CENTER FOR INTERNET SECURITY,
SHALL PRODUCE AND SUBMIT A REPORT, TO THE GOVERNOR, THE TEMPORARY PRESI-
DENT OF THE SENATE, AND THE SPEAKER OF THE ASSEMBLY, MAKING RECOMMENDA-
TIONS ON THE FEASIBILITY, SECURITY BENEFITS, AND RELATIVE MERITS OF
INCORPORATING SECURITY STANDARDS INTO ACQUISITION PLANNING AND CONTRACT
ADMINISTRATION. SUCH REPORT SHALL FURTHER ADDRESS WHAT STEPS CAN BE
TAKEN TO HARMONIZE AND MAKE CONSISTENT EXISTING PROCUREMENT REQUIREMENTS

RELATED TO CYBER SECURITY AND THE FEASIBILITY OF INCLUDING RISK-BASED
SECURITY STANDARDS INTO PROCUREMENT AND CONTRACT ADMINISTRATION.
5. NEW YORK STATE CYBER SECURITY CRITICAL INFRASTRUCTURE RISK ASSESS-
MENT REPORT. (A) THE DIVISION OF HOMELAND SECURITY AND EMERGENCY
SERVICES, IN CONSULTATION WITH THE DIVISION OF STATE POLICE, THE STATE
OFFICE OF INFORMATION TECHNOLOGY SERVICES, AND THE CENTER FOR INTERNET
SECURITY, WITHIN ONE HUNDRED TWENTY DAYS OF THE EFFECTIVE DATE OF THIS
SECTION, SHALL PRODUCE A NEW YORK STATE CYBER SECURITY CRITICAL INFRAS-
TRUCTURE RISK ASSESSMENT REPORT.
(B) THE PRODUCTION OF THE NEW YORK STATE CYBER SECURITY CRITICAL
INFRASTRUCTURE RISK ASSESSMENT REPORT SHALL USE A RISK-BASED APPROACH TO
IDENTIFY CRITICAL INFRASTRUCTURE WHERE A CYBER SECURITY INCIDENT COULD
REASONABLY RESULT IN CATASTROPHIC REGIONAL OR STATE-WIDE EFFECTS ON
PUBLIC HEALTH OR SAFETY, ECONOMIC DISTRESS, AND/OR THREATEN PUBLIC
PROTECTION OF THE PEOPLE AND/OR PROPERTY OF NEW YORK STATE.
(C) THE PRODUCTION OF THE REPORT SHALL FURTHER USE THE CONSULTATIVE
PROCESS AND DRAW UPON THE EXPERTISE OF AND ADVICE OF THE DIVISION OF
HOMELAND SECURITY AND EMERGENCY SERVICES, THE DIVISION OF STATE POLICE,
THE STATE OFFICE OF INFORMATION TECHNOLOGY SERVICES, THE CENTER FOR
INTERNET SECURITY, THE NEW YORK STATE CYBER SECURITY ADVISORY BOARD, THE
PROGRAMS ESTABLISHED BY THIS SECTION, AND SUCH OTHER AND FURTHER PRIVATE
AND PUBLIC SECTOR ENTITIES, UNIVERSITIES, AND CYBER SECURITY EXPERTS AS
THE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES MAY DEEM
PRUDENT.

(D) THE NEW YORK STATE CYBER SECURITY CRITICAL INFRASTRUCTURE RISK ASSESSMENT REPORT SHALL BE DELIVERED TO THE GOVERNOR, THE TEMPORARY PRESIDENT OF THE SENATE, THE SPEAKER OF THE ASSEMBLY, THE CHAIR OF THE SENATE STANDING COMMITTEE ON VETERANS, HOMELAND SECURITY AND MILITARY AFFAIRS, AND THE CHAIR OF THE ASSEMBLY STANDING COMMITTEE ON GOVERN- MENTAL OPERATIONS.

(E) WHERE COMPLIANCE WITH THIS SECTION SHALL REQUIRE THE DISCLOSURE OF CONFIDENTIAL INFORMATION, OR THE DISCLOSURE OF SENSITIVE INFORMATION WHICH IN THE JUDGMENT OF THE COMMISSIONER OF THE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES WOULD JEOPARDIZE THE CYBER SECURITY OF THE STATE:

(I) SUCH CONFIDENTIAL OR SENSITIVE INFORMATION SHALL BE PROVIDED TO THE PERSONS ENTITLED TO RECEIVE THE REPORT, IN THE FORM OF A SUPPLE- MENTAL APPENDIX TO THE REPORT; AND

(II) SUCH SUPPLEMENTAL APPENDIX TO THE REPORT SHALL NOT BE SUBJECT TO THE PROVISIONS OF THE FREEDOM OF INFORMATION LAW PURSUANT TO ARTICLE SIX OF THE PUBLIC OFFICERS LAW; AND

(III) THE PERSONS ENTITLED TO RECEIVE THE REPORT MAY DISCLOSE THE SUPPLEMENTAL APPENDIX TO THE REPORT TO THEIR PROFESSIONAL STAFF, BUT SHALL NOT OTHERWISE PUBLICLY DISCLOSE SUCH CONFIDENTIAL OR SECURE INFOR- MATION.

S 2. This act shall take effect immediately.

S924 - Summary

Requires the formation of a cyber security advisory board and the implementation of a cyber security initiative.

S924 - Sponsor Memo

BILL NUMBER: S924

TITLE OF BILL:

An act to amend the executive law, in relation to a cyber security initiative

PURPOSE OR GENERAL IDEA OF BILL:

This bill would amend the executive law to establish the New York State Cyber Security Initiative, to create a New York State Cyber Security Advisory Board, a New York Cyber Security Partnership Program, and a New York State Cyber Security Information Sharing Program.

SUMMARY OF SPECIFIC PROVISIONS:

This bill would add a new section to the executive law to establish the New York State Cyber Security Initiative. Specifically, this new section would:

*Make legislative findings;

*Define "critical infrastructure and information systems";

*Establish within the division of homeland security (DHSES), a Cyber Security Advisory Board to make recommendations for protecting the state's critical infrastructure and information systems;

*Establish within DHSES, a Cyber Security Sharing and Threat Prevention Program, designed to increase the volume, timeliness, and quality of cyber threat information shared with the public and private sector; and

*Require DHSES, in consultation with the State Police, the Office of Information Technology Services, and the Center for Internet Security, to issue a New York State Cyber Security Critical Infrastructure Risk Assessment Report, identifying critical infrastructure and where a cyber security incident could reasonably result in catastrophic regional or state-wide effects on public: health or safety, economic distress, and/or threaten public protection of the people and/or property of New York State.

JUSTIFICATION:

According to the such entities as the United States Department of Homeland Security, Interpol and the New York State White Collar Crime Task Force, cybercrime is a pervasive and rapidly expanding threat. New York state is particularly at risk to cybercrime due to its status as a global hub of international business and commerce. As most major national and international banks, insurance companies and brokerage

houses also have headquarters or a significant presence within the state, such present a particularly attractive target to those who wish to engage in cyber crime or cyber terrorism.

By establishing a Cyber Security Advisory Board in state law, New York State can identify ways to protect the state's critical infrastructure and information systems. Innovative, actionable policies developed by the Advisory Board will further ensure that New York state is in the forefront of public cyber security defense.

Modeled after a successful federal initiative, the Information Sharing and Threat Prevention Program, established by this bill, seeks to assist both the public and private sector to develop practices that will better protect and defend their interests against cyber threats. Finally, the Risk Assessment Report, required under this legislation, will additionally allow New York, to leverage the expertise and advice of experienced and knowledgeable professionals, to identify security threats that are facing the state and its businesses and citizens, and develop effective ways to combat them.

PRIOR LEGISLATIVE HISTORY:

This is a new bill.

FISCAL IMPLICATIONS:

None noted.

EFFECTIVE DATE:
This act would take effect immediately.

Senate 926/Assembly 3451 Cyber Security Report

State of New York

926
2017-2018 Regular Sessions
I N S E N A T E
January 5, 2017

Introduced by Sens. CROCI, AKSHAR, AVELLA, DeFRANCISCO, FUNKE, GOLDEN, SEWARD -- read twice and ordered printed, and when printed to be committed to the Committee on Veterans, Homeland Security and Military
Affairs
AN ACT to amend the executive law, in relation to a cyber security report
THE PEOPLE OF THE STATE OF NEW YORK, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:
1 Section 1. The executive law is amended by adding a new section 719 to
2 read as follows:
3 S 719. QUINQUENNIAL CYBER SECURITY REPORT. 1. THE COMMISSIONER, IN
4 CONSULTATION WITH THE SUPERINTENDENT OF THE STATE POLICE, THE CHIEF
5 INFORMATION OFFICER, AND THE PRESIDENT OF THE CENTER FOR INTERNET SECU-
6 RITY, SHALL PREPARE A REPORT, TO BE DELIVERED TO THE GOVERNOR, THE
7 TEMPORARY PRESIDENT OF THE SENATE, THE SPEAKER OF THE ASSEMBLY, THE
8 CHAIR OF THE SENATE STANDING COMMITTEE ON VETERANS, HOMELAND SECURITY
9 AND MILITARY AFFAIRS, AND THE CHAIR OF THE ASSEMBLY STANDING COMMITTEE
10 ON GOVERNMENTAL OPERATIONS, ON OR BEFORE THE FIRST DAY OF SEPTEMBER, TWO
11 THOUSAND SEVENTEEN, AND THEN EVERY FIVE YEARS THEREAFTER, WHICH PROVIDES
12 A COMPREHENSIVE REVIEW OF ALL CYBER SECURITY SERVICES PERFORMED BY, AND
13 ON BEHALF OF, THE STATE OF NEW YORK.
14 2. THE REPORT REQUIRED PURSUANT TO SUBDIVISION ONE OF THIS SECTION,
15 SHALL INCLUDE A DETAILED ASSESSMENT OF EACH AND EVERY CYBER SECURITY
16 NEED OF THE STATE OF NEW YORK, INCLUDING BUT NOT LIMITED TO, ITS STATE

17 AGENCIES AND ITS PUBLIC AUTHORITIES, AND FOR EACH AND EVERY SUCH CYBER
18 SECURITY NEED SO IDENTIFIED, SHALL FURTHER INCLUDE A DETAILED
19 DESCRIPTION OF:
20 (A) THE TYPE OF CYBER SECURITY SERVICE USED TO ADDRESS SUCH NEED;
21 (B) THE SCOPE OF THE NEED SO ADDRESSED, AS WELL AS THE SCOPE OF THE
22 SERVICE USED TO ADDRESS SUCH NEED;
23 (C) THE COST OF THE SERVICE USED TO ADDRESS SUCH NEED;
EXPLANATION--Matter in ITALICS (underscored) is new; matter in brackets
[ ] is old law to be omitted.
LBD01791-01-7
S. 926 2
1 (D) THE EFFECTIVENESS OF THE CYBER SECURITY SERVICE USED TO ADDRESS
2 SUCH NEED;
3 (E) THE ENTITY PROVIDING SUCH CYBER SECURITY SERVICE USED TO ADDRESS
4 SUCH NEED;
5 (F) THE GOVERNMENT, INDUSTRY AND/OR ACADEMICALLY ACCEPTED BEST CYBER
6 SECURITY PRACTICE FOR ADDRESSING SUCH NEED;
7 (G) HOW OTHER STATES, AND THE FEDERAL GOVERNMENT HAVE ADDRESSED SUCH
8 NEED; AND
9 (H) HOW PRIVATE SECTOR ENTITIES ADDRESSED SUCH NEED.
10 3. DURING THE PREPARATION OF THE REPORT REQUIRED BY SUBDIVISION ONE OF
11 THIS SECTION, AND AFTER ITS DELIVERY TO THE PERSONS IDENTIFIED TO
12 RECEIVE SUCH REPORT, THE COMMISSIONER, THE SUPERINTENDENT OF THE STATE
13 POLICE, THE CHIEF INFORMATION OFFICER, AND THE PRESIDENT OF THE CENTER
14 FOR INTERNET SECURITY, AS WELL AS THE DIVISIONS, OFFICES AND CORPO-
15 RATIONS UNDER THEIR DIRECTION, SHALL PROVIDE TO SUCH PERSONS ENTITLED TO
16 RECEIVE SUCH REPORT, ANY AND ALL ADDITIONAL INFORMATION SUCH PERSONS MAY
17 REQUEST, WITH RESPECT TO ANY CYBER SECURITY ISSUE CONCERNING:
18 (A) THE STATE OF NEW YORK, INCLUDING BUT NOT LIMITED TO, ANY AGENCY,
19 BOARD, BUREAU, COMMISSION, DEPARTMENT, DIVISION, INSTITUTION, OFFICE, OR
20 PUBLIC AUTHORITY OF THE STATE;

(B) ANY LOCAL GOVERNMENT ENTITY, INCLUDING BUT NOT LIMITED TO, ANY
COUNTY, TOWN, CITY, VILLAGE, SCHOOL DISTRICT, SPECIAL DISTRICT, AND ANY
AGENCY, BOARD, BUREAU, COMMISSION, DEPARTMENT, DIVISION, INSTITUTION,
OFFICE, OR PUBLIC AUTHORITY OF SUCH LOCAL GOVERNMENT ENTITY;
(C) ANY REGULATED ENTITY OF THE STATE OF NEW YORK OR LOCAL GOVERNMENT
ENTITY;
(D) ANY NOT-FOR-PROFIT CORPORATION IN THE STATE OF NEW YORK;
(E) ANY PRIVATE SECTOR BUSINESS IN THE STATE OF NEW YORK, INCLUDING
BUT NOT LIMITED TO, A SOLE PROPRIETOR, PARTNERSHIP, LIMITED LIABILITY
COMPANY OR BUSINESS CORPORATION; AND/OR
(F) ANY CITIZEN OF THE STATE OF NEW YORK.
4. WHERE COMPLIANCE WITH THIS SECTION SHALL REQUIRE THE DISCLOSURE OF
CONFIDENTIAL INFORMATION, OR THE DISCLOSURE OF SENSITIVE INFORMATION
WHICH IN THE JUDGMENT OF THE COMMISSIONER WOULD JEOPARDIZE THE CYBER
SECURITY OF THE STATE:
(A) SUCH CONFIDENTIAL OR SENSITIVE INFORMATION SHALL BE PROVIDED TO
THE PERSONS ENTITLED TO RECEIVE THE REPORT AS PROVIDED BY SUBDIVISION
ONE OF THIS SECTION, AS FOLLOWS:
(I) IN THE CASE OF THE REPORT REQUIRED BY SUBDIVISION ONE OF THIS
SECTION, IN THE FORM OF A SUPPLEMENTAL APPENDIX TO THE REPORT; AND
(II) IN THE CASE OF A RESPONSE TO A REQUEST FOR INFORMATION MADE IN
ACCORDANCE WITH SUBDIVISION THREE OF THIS SECTION, IN A SECURE MANNER AS
DETERMINED BY THE COMMISSIONER;
(B) NEITHER A SUPPLEMENTAL APPENDIX TO THE REPORT, NOR ANY CONFIDEN-
TIAL OR SENSITIVE INFORMATION PROVIDED IN ACCORDANCE WITH SUBDIVISION
THREE OF THIS SECTION, SHALL BE POSTED ON THE DIVISION'S WEBSITE AS
REQUIRED BY SUBDIVISION FIVE OF THIS SECTION;
(C) NEITHER A SUPPLEMENTAL APPENDIX TO THE REPORT, NOR ANY CONFIDEN-

49 TIAL OR SENSITIVE INFORMATION PROVIDED IN ACCORDANCE WITH SUBDIVISION
50 THREE OF THIS SECTION, SHALL BE SUBJECT TO THE PROVISIONS OF THE FREEDOM
51 OF INFORMATION LAW PURSUANT TO ARTICLE SIX OF THE PUBLIC OFFICERS LAW;
52 AND
53 (D) THE PERSONS ENTITLED TO RECEIVE THE REPORT AS PROVIDED BY SUBDIVI-
54 SION ONE OF THIS SECTION, MAY DISCLOSE THE SUPPLEMENTAL APPENDIX TO THE
55 REPORT, AND ANY CONFIDENTIAL OR SENSITIVE INFORMATION PROVIDED IN
56 ACCORDANCE WITH SUBDIVISION THREE OF THIS SECTION, TO THEIR PROFESSIONAL
S. 926 3
1 STAFF, BUT SHALL NOT OTHERWISE PUBLICLY DISCLOSE SUCH CONFIDENTIAL OR
2 SECURE INFORMATION.
3 5. EXCEPT WITH RESPECT TO ANY CONFIDENTIAL OR SENSITIVE INFORMATION AS
4 DESCRIBED IN SUBDIVISION FOUR OF THIS SECTION, THE DIVISION SHALL POST A
5 COPY OF THE REPORT PREPARED IN ACCORDANCE WITH SUBDIVISION ONE OF THIS
6 SECTION, ON ITS WEBSITE, NOT MORE THAN FIFTEEN DAYS AFTER SUCH REPORT IS
7 DELIVERED TO THE PERSONS ENTITLED TO RECEIVE SUCH REPORT. THE DIVISION
8 MAY FURTHER POST ANY AND ALL FURTHER INFORMATION IT MAY DEEM APPROPRI-
9 ATE, ON ITS WEBSITE, REGARDING CYBER SECURITY, AND THE PROTECTION OF
10 PUBLIC AND PRIVATE COMPUTER SYSTEMS, NETWORKS, HARDWARE AND SOFTWARE.
11 S 2. This act shall take effect immediately.

S926 - Summary

Requires a comprehensive review of all cyber security services to be performed every five years.

S926 - Sponsor Memo

BILL NUMBER: S926

TITLE OF BILL:

An act to amend the executive law, in relation to a cyber security report

PURPOSE OR GENERAL IDEA OF BILL:

This bill would amend the executive law to requires a comprehensive review of all cyber security services to be performed every five years.

SUMMARY OF SPECIFIC PROVISIONS:

This bill would add a new section to the executive law to establish a Quinquennial Cyber Security Report.

Specifically, this new section would:

*Require the Commissioner of the Division of Homeland Security and Emergency Services, in consultation with the Superintendent of the State Police, the Chief Information Officer, and the President of the Center for Internet Security, to prepare and issue a quinquennial cyber security report; *Require that such report must include an assessment of each and every cyber security need of the state or New York and a detailed description of how that need is being met; and

*Further require, that persons statutorily entitled to receive the report, would also be entitled to request additional information to supplement the report.

JUSTIFICATION:

According to the such entities as the United States Department of Homeland Security, Interpol and the New York State White Collar Crime Task Force, cybercrime is a pervasive and rapidly expanding threat. New York State is particularly at risk to cybercrime due to its status as a global hub of international business and commerce. As, most major national and international banks, insurance companies and brokerage houses also have headquarters or a significant presence within the state, such present a particularly attractive target to those who wish to engage in cyber crime or cyber terrorism.

In addition to regulating the various business entities noted above, New York State government, also stores and maintains vast quantities of sensitive personal data pertaining to the citizens of our state. The state thereby has an incumbent duty to ensure that the cyber security needs of all entities with state government are being met in order to protect such information.

By requiring the Division of Homeland Security and Emergency Services' to identify the various cyber security needs of our state, and detail how the needs are being met, we can ensure that adequate cyber security measures are being taken, and that best practices are being employed to foster the public protection and security the people of our state deserve.

PRIOR LEGISLATIVE HISTORY:

S3405 of 2015/16: Passed in the Senate

FISCAL IMPLICATIONS:

None noted.

EFFECTIVE DATE:
This act would take effect immediately.

S953/A3311 Cyber Terrorism in the First and Second Degree
State of New York

953
2017-2018 Regular Sessions
I N S E N A T E
January 5, 2017

Introduced by Sens. CROCI, AVELLA, FUNKE, GOLDEN, MURPHY, O'MARA, RANZENHOFER -- read twice and ordered printed, and when printed to be committed to the Committee on Veterans, Homeland Security and Military Affairs AN ACT to amend the penal law, in relation to cyber terrorism in the first and second degree
THE PEOPLE OF THE STATE OF NEW YORK, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:
Section 1. The penal law is amended by adding two new sections 490.26 and 490.27 to read as follows:
S 490.26 CYBER TERRORISM IN THE SECOND DEGREE.
A PERSON IS GUILTY OF A CRIME OF CYBER TERRORISM IN THE SECOND DEGREE
WHEN, WITH INTENT TO CAUSE SERIOUS, WIDE-SPREAD FINANCIAL HARM, OR
COMMIT ANY OFFENSE CONTAINED WITHIN ARTICLE ONE HUNDRED FIFTY-FIVE OF
THIS CHAPTER AGAINST MORE THAN TEN PEOPLE, A PERSON USES A COMPUTER, A
COMPUTER PROGRAM, A COMPUTER NETWORK, COMPUTER MATERIAL, A COMPUTER
SERVICE, OR COMPUTER DATA, TO CAUSE SUCH WIDE-SPREAD FINANCIAL HARM OR
TO COMMIT ANY OFFENSE CONTAINED WITHIN ARTICLE ONE HUNDRED FIFTY-FIVE OF
THIS CHAPTER AGAINST MORE THAN TEN PEOPLE.
CYBER TERRORISM IN THE SECOND DEGREE IS A CLASS C FELONY.
S 490.27 CYBER TERRORISM IN THE FIRST DEGREE.
A PERSON IS GUILTY OF A CRIME OF CYBER TERRORISM IN THE FIRST DEGREE
WHEN, WITH INTENT TO INTIMIDATE OR COERCE A CIVILIAN POPULATION, INFLU-
ENCE THE POLICY OF A UNIT OF GOVERNMENT BY INTIMIDATION OR COERCION,
AFFECT THE CONDUCT OF A UNIT OF GOVERNMENT, OR CAUSE MASS INJURY,
DAMAGE, DESTRUCTION OR DEBILITATION TO PERSONS AND/OR PROPERTY, A PERSON
USES A COMPUTER, A COMPUTER PROGRAM, A COMPUTER NETWORK, COMPUTER MATE-

20 RIAL, A COMPUTER SERVICE, OR COMPUTER DATA, TO INTIMIDATE, INFLUENCE,
21 COERCE, AFFECT, INJURE, DAMAGE, DESTROY, OR DEBILITATE PERSONS OR PROP-
22 ERTY.
23 CYBER TERRORISM IN THE FIRST DEGREE IS A CLASS A FELONY.
24 S 2. This act shall take effect on the first of November next succeed-
25 ing the date upon which it shall have become a law.
EXPLANATION--Matter in ITALICS (underscored) is new; matter in brackets
[ ] is old law to be omitted.
LBD00544-01-7

S953 - Summary

Relates to cyber terrorism in the first and second degree.

S953 - Sponsor Memo

BILL NUMBER: S953

TITLE OF BILL:

An act to amend the penal law, in relation to cyber terrorism in the first and second degree

PURPOSE OR GENERAL IDEA OF BILL:

This bill would amend the penal law to create the new crimes of cyber terrorism in the first and second degrees.

SUMMARY OF SPECIFIC PROVISIONS:

This bill would add a new sections to the penal law, to create the new crimes of cyber terrorism in the second degree and cyber terrorism in the first degree, respectively.

Specifically, a person would be guilty of the new C felony crime of cyber terrorism in the second degree when: *with intent to cause serious, wide-spread financial harm, or commit any larceny offense against more than ten people, a person uses a computer, a computer program, a computer network, computer material, a computer service, or computer data, to cause such wide-spread financial harm or to commit any larceny offense against more than ten people.

Ethics & Technology:

The Risks and Legal Ethics of Technology and Legal Practice

Antony K. Haynes

February 14, 2017

Learning Outcomes

1. Gain knowledge and understanding of professional and ethical responsibilities.
2. Be able to exercise proper professional and ethical responsibilities to clients and to the legal system.

Everyone Is a Target

- Hackers in the past year have broken into computer systems at the White House, the State Department, the Pentagon, the Internal Revenue Service and the Office of Personnel Management
- Law firms are considered by attackers to be “one stop shops” for attackers because they have high value information and perhaps weaker security than other businesses.

The Panama Papers

- Files reveal the offshore holdings of 140 politicians and public officials from around the world
- Current and former world leaders in the data include the prime minister of Iceland, the president of Ukraine, and the king of Saudi Arabia
- More than 214,000 offshore entities appear in the leak, connected to people in more than 200 countries and territories
- Major banks have driven the creation of hard-to-trace companies in offshore havens

Cravath, Swaine & Moore

WSJ Post, March 29, 2016

- Hackers broke into the computer networks at some of the country's most prestigious law firms, and federal investigators are exploring whether they stole confidential information for the purpose of insider trading, according to people familiar with the matter.
- The firms include Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP, which represent Wall Street banks and Fortune 500 companies in everything from lawsuits to multibillion-dollar merger negotiations

The Cyber-Threat

• Robert Mueller, then the FBI Director, put it this way in an address at a major information security conference in 2012:

• I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.

Recent High Profile Data Breaches

- OPM, Fed'l Gov't
  - Suspected Chinese hackers
  - records of over 22 million federal employees and contractors, including covert operators and other military and intelligence personnel
- Anthem, January 2015
  - Suspected Chinese hackers
- Sony, November 2014
  - Suspected Korean hackers
- Target, 2013
  - Suspected Russian hackers

ABA Cybersecurity Task Force 2012 Report and Resolution

5 Essential Principles for Government to consider when making policy to address cyber-attacks

- Public/private frameworks
- Public/private collaboration and sharing
- Legal and policy environments must be modernized to keep up with technology
- Privacy and civil liberties remain a priority
- Training, workforce development, adequate resources and investing

Basic Terms/Definitions

- **Cyber Security**: also known as cybersecurity or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.
- **Data Breach**: the intentional or unintentional release of secure information to an untrusted environment.

Basic Terms/Definitions

- **Two-Factor Authentication:** a security process in which the user provides two means of identification from separate categories of credentials; one is typically a physical token, such as a card, and the other is typically something memorized, such as a security code.

Basic Terms/Definitions

- **The "Cloud"**: the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Basic Terms/Definitions

- **“Phishing”**: the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.
- **Encryption**: the process of encoding messages or information in such a way that only authorized parties can read it.

Basic Terms/Definitions

- **Botnet:** (also known as a zombie army) refers to Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet.
- **Patch:** a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually called bug fixes, and improving the usability or performance.

Rule 1.1*

(a) A lawyer should provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

* “Rule #.#” refers to the New York Rules of Professional Conduct, Effective April 1, 2009, as amended through January 1, 2014, with Commentary as amended through March 28, 2015. Except where noted otherwise, NY Rules are generally used interchangeably with the ABA Model Rules of Professional Conduct in this presentation.

Rule 1.1 Comment 8

Maintaining Competence

To maintain the requisite knowledge and skill, a lawyer should (i) keep abreast of changes in substantive and procedural law relevant to the lawyer's practice, (ii) ***keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information***, and (iii) engage in continuing study and education and comply with all applicable continuing legal education requirements under 22 N.Y.C.R.R. Part 1500 (emphasis added).

Rule 1.1 References

Latest ABA Guidance: Old Wine in a Tech-Ethics Bottl*e? NYSBA Journal November/December 2012*, Article pg. 20, by Devika Kewalramani

This article addresses the importance of lawyers and law firms in keeping up with the advancement in technology while maintaining client confidentiality and the attorney-client relationship. “Lawyers perhaps deal with more confidential and privileged information than any other professionals. That is why it is imperative that law firms and legal departments understand how to protect and secure the information clients entrust to them. Today, every law firm and legal department maintains electronic client data in some shape or form. This makes the ABA guidance on a lawyer’s use of technology critical to every lawyer’s practice.”

Rule 1.6

(c) A lawyer shall exercise *reasonable care* to prevent the lawyer's employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client … (emphasis added).

Rule 1.6 Ethics Opinions

NYSBA Opinion 820 - 02/08/2008

Topic: Use of e-mail service provider that scans e-mails for advertising purposes.

Digest: A lawyer may use an e-mail service provider that conducts computer scans of e-mails to generate computer advertising, where the e-mails are not reviewed by or provided to human beings other than the sender and recipient.

Rules: DR 4-101; EC 4-3.

Rule 1.6 Ethics Opinions

NYSBA Opinion 1019 (8/6/2014)

Topic: Confidentiality; Remote Access to Firm's Electronic Files

Digest: A law firm may give its lawyers remote access to client files, so that lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing the client of the risks.

Rules: 1.0(j), 1.5(a), 1.6, 1.6(a), 1.6(b), 1.6(c), 1.15(d).

Rule 1.6 Ethics Opinions

ABA Formal Opinion 11-459 (8/4/2011)

Topic: Duty to Protect the Confidentiality of E-mail Communications with One's Client

Digest: A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party.

ABA Rule 1.6

- (c) A lawyer shall make *reasonable efforts* to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client (emphasis added).

Duty to Safeguard Confidential Information

- Common law duty--ACP
- Legal—statutes protecting medical, financial and personal identification information
- Fiduciary/Agency
- Legal Ethics—ABA MR 1.6
  - (c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.
    - VA adopted new Va. Rule 1.6(d) which is identical, eff. March 1, 2016.

Va. Rule 1.6(c)—What Are Reasonable Efforts to Protect Client Data?

- Comments 19, 19a, 20 and 21 explain.
- Comment 19—factors to consider:
  - Sensitivity of the information
  - Risk of disclosure if additional measures not taken
  - Employment/use of IT professionals
  - Cost of additional safeguards
  - Difficulty of implementing additional safeguards
  - Extent to which safeguards interfere unreasonably with representation of client.

Va. Rule 1.6(c)—What Are Reasonable Efforts to Protect Client Data?

- Comment 20—”safe harbor”
- lawyer is not subject to discipline under this Rule if the lawyer has made reasonable efforts to protect electronic data, even if there is a data breach, cyber-attack or other incident resulting in the loss, destruction, misdelivery or theft of confidential client information.
- Perfect security is not attainable
- Even large businesses and government organizations with sophisticated data security systems have suffered data breaches.
- What’s reasonable may depend on size of firm.
- Lawyer need not be “tech-savvy” but may need to employ someone who is.

Va. Rule 1.6(c)—What Are Reasonable Efforts to Protect Client Data?

- Comment 21—Lawyers should keep abreast on an ongoing basis and periodically review security measures including:
- Staff security training and evaluation
- Procedures to address departing employees
- Access to stored client data by third parties
- Back up/storage/and erasure of data on devices
- Strong passwords and authentication on devices and networks.
- Use of hardware/software to prevent, detect and respond to intrusion, malicious software and activity.

Other Things to Consider

- There is no such thing as “set it and forget it” security. The threats and the defenses to those threats change constantly and firms must strive to keep up with the changes.
- So the new mantra is Identify (assets that need to be protected), Protect, Detect, Respond and Recover.
- 100% Prevention is not possible—you will lose credibility if you think and assert this.

General Counsel, Ethics and Cyber

Christina Ayiotis

As most in-house lawyers have realized over the years, the American Bar Association (ABA) Model Rules of Professional Conduct[1] do not generally distinguish between in-house lawyers and outside counsel (with the exception of Rule 5 relating to *Law Firms and Associations*). This raises interesting questions regarding ultimate accountability when corporate information is inappropriately disclosed in the greater legal ecosystem.

It should come as no surprise that the very first requirement for Professional Conduct is ***Competence***:

> *A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.*[2]

As many know, maintaining competence in today's world remains challenging. The ABA updated Comment 8[3] to Rule 1.1 several years ago to recognize the importance of **technology** to the competent practice of law, although not all State Bars immediately followed suit. Virginia, for example, only updated its Competence Comments this year (effective March 1, 2016) to add "the language 'in the areas of practice in which the lawyer is engaged. Attention should be paid to the **benefits and risks associated with relevant technology**.' "[4] [**EMPHASIS ADDED**]

---

[1] American Bar Association Model Rules of Professional Conduct: Table of Contents http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html (Last accessed May 17, 2016)

[2] American Bar Association Model Rule 1.1 Competence (Client-Lawyer Relationship) http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html (Last accessed May 17, 2016)

[3] "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html (Last accessed May 17, 2016)

[4] Virginia State Bar Professional Guidelines – 5/17/2016 Rule 1.1 Committee Commentary http://www.vsb.org/pro-guidelines/index.php//main/print_view (Last accessed May 17, 2016)

In a data-driven economy, few entities function without information systems and tools. In-house lawyers must understand enough technology to know how to use those systems and tools appropriately to meet their ethical duties as lawyers, particularly with respect to maintaining ***Confidentiality of Information***.[5] That obligation transcends the method of providing legal advice (whether directly through personal knowledge or with the assistance of third party vendors of legal services such as law firms). In addition to law firms, in-house lawyers very often engage other types of third party vendors such as e-discovery companies, contract management companies, forensics experts, etc. Cybersecurity competence necessarily comes into play in the Legal Department's management of all those various external entities. So, in-house lawyers must preserve Confidentiality (an ethical obligation), as well as ensure the Attorney-Client Privilege (an evidentiary concept regarding communications providing legal advice) is not broken and they must do both within their organizations, ***and***, with all the third party vendors they engage.

The good news is that the standard for meeting the **Confidentiality** obligation is ***reasonableness***. Virginia, for example, amended its Rule 1.6 Comments to provide guidance:

> ***"Acting Reasonably to Preserve Confidentiality***
> [19] Paragraph (d) requires a lawyer to act reasonably to safeguard information protected under this Rule against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to,

[5] American Bar Association Model Rule 1.6: **Confidentiality of Information** (c): "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html; Effective March 1, 2016, the Virginia State Bar amended its Rule 1.6 **Confidentiality of Information** to include (*d) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information protected under this Rule.* Virginia State Bar Professional Guidelines – 5/17/2016 Rule 1.6 Committee Commentary http://www.vsb.org/pro-guidelines/index.php//main/print_view (Last accessed May 17, 2016)

or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of this Rule if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the employment or engagement of persons competent with technology, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

[19a] Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other laws, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of this Rule.

[20] Paragraph (d) makes clear that a lawyer is not subject to discipline under this Rule if the lawyer has made reasonable efforts to protect electronic data, even if there is a data breach, cyber-attack or other incident resulting in the loss, destruction, misdelivery or theft of confidential client information. **Perfect online security and data protection is not attainable.** Even large businesses and government organizations with sophisticated data security systems have suffered data breaches. Nevertheless, security and data breaches have become so prevalent that some security measures must be reasonably expected of all businesses, including lawyers and law firms. Lawyers have an ethical obligation to implement reasonable information security practices to protect the confidentiality of client data. **What is "reasonable" will be determined in part by the size of the firm.** See Rules 5.1(a)-(b) and 5.3(a)-(b). The sheer amount of personal, medical and financial information of clients kept by lawyers and law firms requires reasonable care in the communication and storage of such information. A lawyer or law firm complies with paragraph (d) if they

have acted reasonably to safeguard client information by employing appropriate data protection measures for any devices used to communicate or store client confidential information.
To comply with this Rule, a lawyer does not need to have all the required technology competencies. The lawyer can and more likely must turn to the expertise of staff or an outside technology professional. ***Because threats and technology both change, lawyers should periodically review both and enhance their security as needed; steps that are reasonable measures when adopted may become outdated as well.***

[21] Because of evolving technology, and associated evolving risks, law firms should keep abreast on an ongoing basis of reasonable methods for protecting client confidential information, addressing such practices as:
(a) Periodic staff security training and evaluation programs, including precautions and procedures regarding data security;
(b) Policies to address departing employee's future access to confidential firm data and return of electronically stored confidential data;
(c) Procedures addressing security measures for access of third parties to stored information;
(d) Procedures for both the backup and storage of firm data and steps to securely erase or wipe electronic data from computing devices before they are transferred, sold, or reused;
(e) The use of strong passwords or other authentication measures to log on to their network, and the security of password and authentication measures; and
(f) The use of hardware and/or software measures to prevent, detect and respond to malicious software and activity."[6] [**EMPHASES ADDED**]

While the Virginia State Bar Rule Comments seem to only "speak" to "[solo practitioner] lawyers and law firms," in-house lawyers can extrapolate to

[6] Virginia State Bar Professional Guidelines – 5/17/2016 Rule 1.6 Comments 19-21 http://www.vsb.org/pro-guidelines/index.php//main/print_view (Last accessed May 17, 2016)

determine what their individual obligations are. The recommendation to law firms to provide periodic "staff security training and evaluation programs" could be similarly applied to Legal Departments. While there may be a designated "Cyber Lawyer" within any Legal Department, it is every in-house lawyer's responsibility to understand cybersecurity: to not only meet ***individual ethical*** obligations but to also be able to ***competently provide legal advice*** given that almost every legal issue has some technology component to it that will implicate data (flows) that need to be appropriately protected and/or exploited.

The recent news stories regarding law firm breaches and concerns about cybersecurity[7] have put all in-house lawyers on notice regarding their own "supervisory" responsibilities. Again, the ABA Model Rules and Virginia State Bar Rules were written with law firm infrastructure in mind but supervisory obligations can be extrapolated to in-house counsel. ABA Model Rule 5.1 ***Responsibilities of Partners, Managers, and Supervisory Lawyers***[8] essentially obligates a lawyer to ensure she is responsible for all lawyers who work for her, including adherence to Rules of Professional Conduct. ABA Model Rule 5.3 ***Responsibilities Regarding Nonlawyer Assistant (sic)***[9] essentially extends Rule 5.1 to Nonlawyers.

The Model Rules focus on lawyers and nonlawyers under the direct (presumably employment) supervision of law firm partners, managers and lawyers. "Outsourcing" has come to mean a law firm hiring lawyers or paralegals to provide support services. The term arises from the

---

[7] Nicholas Gaffney, *Law Firm Data Hack Attack, Part I* **Law Practice Today** (April 14, 2016) http://www.lawpracticetoday.org/article/law-firm-hack-part-i/; Gregg Wirth, *Cybersecurity & Data Breach Reaction: Law Firms Ask Patience, GCs Want Assurances* **Legal Executive Institute** (April 6, 2016) http://legalexecutiveinstitute.com/cybersecurity-law-firms-ask-patience-gcs-want-assurances/ (Last accessed May 17, 2016)

[8] "(b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct." American Bar Association Rule 5.1: Responsibilities of a Partner or Supervisory Lawyer http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_1_responsibilities_of_a_partner_or_supervisory_lawyer.html (Last accessed May 17, 2016)

[9] American Bar Association Rule 5.3: Responsibilities Regarding Nonlawyer Assistance http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant.html (Last accessed May 17, 2016)

presumption that the law firm is the center of the legal ecosystem universe. From a corporate perspective, the law firm is actually just another vendor.

Extrapolating from the Model Rules and Legal Ethics Opinions on Outsourcing of Legal Services, in-house lawyers have some level of "supervisory" responsibility despite there not being a "direct" employment relationship. As the practice of law morphs into a new paradigm where the law firm model (including the billable hour) fades (effective disaggregation), in-house counsel will be increasingly playing the role of "general contractor" ensuring all the various legal services "subcontractors" do their part so she can deliver high quality legal services to her internal corporate Client. This delivery of legal services will require the efficient, safe transfer of information (often globally). While not a perfect analogy, substituting "Legal Department" wherever "firm" is found, Virginia Legal Ethics Opinion 1850 ***Outsourcing of Legal Services*** (December 28, 2010) provides in-house counsel with a potential future model:

> "A lawyer may ethically outsource legal support services to a nonlawyer who is not associated with the firm or working under the direct supervision of a lawyer in the firm if the lawyer (1) rigorously supervises the nonlawyer so as to avoid aiding the nonlawyer in the unauthorized practice of law and ensuring the nonlawyer's work meets the lawyer's requirements of competency, (2) preserves the client's confidences, (3) bills for services appropriately, and (4) obtains the client's informed consent to outsourcing the work."[10]

The proper oversight and management of legal services vendors (to ensure the full lifecycle protection of a corporation's data assets, particularly its most sensitive at issue in legal disputes) is not only an ethical duty but also an important business imperative. With third (and N^{th})[11] party vendor cyber risk being one of the top concerns of all corporations, in-house lawyers will

[10] https://www.vsb.org/docs/LEO/1850.pdf (Last accessed May 17, 2016)

[11] *FOR IMMEDIATE RELEASE: Third-Party Vendors are Key Concern for Business, Data Privacy Survey Finds* **Treliant Risk Advisors** (April 4, 2016) http://www.treliant.com/News-and-Events/Announcements-and-Releases/Announcements-Details/ArticleID/26983/FOR-IMMEDIATE-RELEASE-Third-Party-Vendors-are-Key-Concern-for-Business-Data-Privacy-Survey-Finds (Last accessed May 17, 2016)

be called upon to do their part with respect to vendors engaged by the Legal Department.

In addition to managing data relating to legal matters, in-house lawyers (and their outside counterparts) need to be thinking strategically regarding organizational information: how to best exploit it while also meeting compliance requirements. As the ethical rules state, lawyers do not have to become technology experts; they can engage experts to advise them. The most important thing we need to remember is that we will continue to remain in a ***constant state of change*** that will only increase in intensity and velocity. We must all become continuous learners and keep an ear to the ground to know what is coming down the road. Just a few years ago, quantum computers seemed like science fiction but now the National Institute of Standards and Technology is advising organizations to "be prepared to transition away from these [quantum resistant cryptography] algorithms as early as 10 years from now."[12] In-house lawyers do not have to know how to write the algorithms but they do need to know when and how the strategies to protect the corporate Client and its assets change.

[12] Brian Robinson, *Prep for next-gen encryption should start yesterday* **CYBEREYE** (May 6, 2016) https://gcn.com/blogs/cybereye/2016/05/nist-quantum-encryption.aspx?s=security_170516&admgarea=TC_SecCybersSec (Last accessed May 17, 2016)

Cybersecurity Law Institute—Georgetown University

May 25-26, 2016

Material prepared by James M. McCauley, Ethics Counsel, Virginia State Bar

I. The duty of confidentiality (Model Rule 1.6) as it applies to digital communications and materials provided in the course of representation

Effective, March 1, 2016 the Supreme Court of Virginia adopted amendments to Rules 1.1 (Competence) and 1.6 (confidentiality). The changes were based on the American Bar Association's modifications to the Comments of Model Rule 1.1 respecting Competence ("…a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology…") and Model Rule 1.6 respecting Confidentiality ("(c) A lawyer shall make reasonable efforts to prevent the unintended disclosure of, or unauthorized access to, information relating to the representation of a client.")

What's reasonable? The Comments list these relevant factors:

1.the sensitivity of the information

2.the likelihood of disclosure if additional safeguards are not employed

3.the cost of employing additional safeguards

4.the difficulty of implementing the safeguards

5.adverse effect on the lawyer's ability to represent clients

There was pushback throughout the process leading up to the adoption of the so-called "technology amendments." Many lawyers complained, "I believe it is unreasonable to expect a lawyer to become an IT professional in addition to all of our other responsibilities." This is a misunderstanding of the rule's requirement. The rule amendments do not require lawyers to become "tech-savvy," but they do need to employ or consult with IT professionals to ensure that their means of transmitting, receiving and storing electronic data include reasonable measures to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, confidential information protected under Rule 1.6.

Other "pushback" came in the form of comments that solo and small firms could not afford to hire IT personnel. However, many of the reasonable security measures involve common sense and utilization of processes that are already in the software and operating systems installed on our computers, including file encryption, logging, password generation, automatic log-off, authentication, firewall, etc. The expense of meeting the "reasonableness" standard under Rule 1.6(c) is pretty nominal when compared with other law firm overhead expenses.

Moreover, there is a "safe harbor" included in the rule amendments. A lawyer is not subject to discipline if the lawyer has made reasonable efforts to protect electronic data, even if there is a data breach, cyber-attack or other incident resulting in the loss, destruction, misdelivery or theft of confidential client information.

We once thought that we could prevent cyber-attacks on our law firm networks and we focused all our energies there. We know now that a skilled hacker with sufficient funding and advanced technology is very likely to succeed in attacking us. So the new mantra is Identify (assets that need to be protected), Protect, Detect, Respond and Recover.

Robert Mueller, then the FBI Director, put it this way in an address at a major information security conference in 2012:

> I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.

Even with our best efforts, a data breach may occur. We have only to look around to see major law firms that have been breached – and major companies as well. So the essential message of our new rules is "Don't let perfection be the enemy of the good." Our focus is on reasonable efforts, which will certainly vary by size of law firm.

The law firms of Weil Gotschal and Cravath, Swaine & Moore have recently acknowledged that their IT systems have been breached. Indeed, data breaches have become so prevalent that some security measures must be reasonably expected of all businesses, including lawyers and law firms. Comment 20, Va. Rule 1.6.

Multiple members of the AmLaw 200 have suffered data breaches, and a major law firm in Panama alleged to be involved in money laundering and helping clients avoid taxes through offshore tax havens, suffered the breach of almost 40 years of client information apparently due to very lax information security. We have learned that the FBI is now partnering with the ABA to deliver Private Sector Cyberalerts to lawyers. The initial alert revealed that at least one cybercriminal has posted on a cybercrime site a "who's who" list of mostly American law firms (nearly 50 of them) that he seeks to compromise with the assistance of a skilled hacker, promising to pay the hacker and share profits from insider trading with the hacker.

Shane McGee, the general counsel and vice president of legal affairs at Mandiant Corp., explained the sophistication of attacks on law firms in a September, 2013 *ABA Journal* article:

> Law firms need to understand that they're being targeted by the best, most advanced attackers out there … These attackers will use every resource at their disposal to compromise law firms because they can, if successful, steal the intellectual property and corporate secrets of not just a single company but of the hundreds or thousands of companies that the targeted law firm represents. Law firms are, in that sense, 'one-stop shops' for attackers.[1]

In spite of the cyber-threat, many law firms all ill-prepared. Many law firms lack critical security measures that help ensure HIPAA compliance, according to a new poll from Legal Workspace, a leading provider of cloud-based

[1] Joe Dysart, "New hacker technology threatens lawyers' mobile devices," *ABA Journal Law News Now* (September 1, 2103). www.abajournal.com/magazine/article/new_hacker_technology_threatens_lawyers_mobile_devices.

work environments designed specifically for law firms. A poll conducted from November 2015 through January 2016, showed that only 13 percent of the 240 law firms had key technology and processes in place to support HIPAA compliance and provide secure environments. This includes items such as executed business associate agreements, email encryption, keeping and reviewing access logs and intrusion detection systems.

So what are "reasonable efforts" to secure electronic data these days? The Supreme Court of Virginia gave some guidance in the comments to newly amended Rule 1.6. Newly added Comment [21] states:

> Because of evolving technology, and associated evolving risks, law firms should keep abreast on an ongoing basis of reasonable methods for protecting client confidential information, addressing such practices as:
>
> (a) Periodic staff security training and evaluation programs, including precautions and procedures regarding data security;
>
> (b) Policies to address departing employee's future access to confidential firm data and return of electronically stored confidential data;
>
> (c) Procedures addressing security measures for access of third parties to stored information;
>
> (d) Procedures for both the backup and storage of firm data and steps to securely erase or wipe electronic data from computing devices before they are transferred, sold, or reused;
>
> (e) The use of strong passwords or other authentication measures to log on to their network, and the security of password and authentication measures; and
>
> (f) The use of hardware and/or software measures to prevent, detect and respond to malicious software and activity.

More specifically, some steps that should be considered include:

1. All security patches should be promptly installed.
2. Software which is no longer supported, and therefore not receiving security updates, cannot ethically be used.
3. Authentication – passwords which are used to gain access to law firm data should be a minimum of 14 characters, using capital and lower case letters, numbers as well as special characters.
4. Passwords should not be shared or used in multiple places.
5. Law firms should have a password policy including some of the advice above as well as mandating that passwords be changed regularly (the recommended time period is every 30 days).
6. Where two-factor authentication is available, it should be utilized.

7. All mobile devices should be encrypted and have the ability to be remotely wiped if they are lost or stolen. They should also be protected by security software.

8. We are rapidly reaching the point where e-mails containing confidential data should be encrypted. Several years ago, encryption was cumbersome. Today, it is inexpensive and simple. Lawyers may wish to have an IT professional install and configure their encryption solution. See Texas State Bar Op. 648 (April 2015) identifying circumstances where lawyers should use encryption for e-mail communications with clients. http://www.legalethicstexas.com/getattachment/9936985b-f798-41c6-bc9f-97d4e0bff9de/Opinion-648.aspx

9. There should be a checklist for departing employees to ensure that all law firm data is returned to the firm and that no further access to the law firm network is technically possible.

10. Law firms should consider annual security assessments.

11. All law firms should have anti-malware software – larger firms should have enterprise grade software. Today's software is not just antivirus software, but can also filter spam, recognize and prevent dangerous components in e-mails and attachments and remove them, and use heuristics to identify potentially dangerous communications.

12. Larger firms will want to explore intrusion detection systems and data loss prevention hardware/software.

13. All firms, of any size, should have an Incident Response Plan, in addition to other security related policies, including disaster recovery plans, BYOD (bring your own device), BYON (bring your own network), etc.

14. Identify all laws and regulations which may apply to your data. Do you hold data which is governed by HIPAA, HITECH or Sarbanes Oxley? Do you hold PII (personally identifiable information)?

15. All firms should have an updated network diagram so it is clear where all data resides and to assist digital forensics experts in the event of a security incident.

16. The security of all third party vendors which hold law firm confidential data (including data in the cloud) should be investigated – again, the standard of reasonableness applies. Lawyers certainly need to read the Terms of Service of anyone who holds their confidential data.

17. Law firms should conduct annual training about data security, including the dangers of phishing and social engineering.

18. As ransomware has evolved, it is now critical that backups be engineered to be impervious to ransomware. In a very small firm, with an external hard drive backup, it may suffice to simply unplug the drive. But more complex backup systems are needed by larger firms.

19. Backups need to be tested on a regular basis.

20. Wireless networks should protected by WPA2 encryption – the only encryption which has not yet been broken.

21. Logging should be enabled on servers whenever possible to aid in the investigation of security incidents.

22. Physical security is also important. Servers should be physically protected. Depending on the size of the law firm, lawyers may include server room door keys, prox cards, alarm codes, video cameras, etc. as part of physical security.

23. If you permit access to your wireless network for guests, their access should be on a properly configured guest network so that they cannot access your confidential data.

24. Make sure there is access control to important data – as an example, there is no reason why a secretary needs to access the firm's financial data.

25. Change all default IDs and passwords – they are freely available on the Internet.

26. Consider a redundant Internet connection, in case your primary connection goes down.

One final point—what is "reasonable" now will quickly become obsolete and inadequate in a rapidly changing technology environment. We simply cannot "set and forget" information security efforts and expect to remain in compliance with our ethical obligations.

2. The duty of competency (Model Rule 1.1) and the evaluation of suitable technology

While evaluating and using appropriate technologies to secure electronic data is important, the "human factor" may be even more important. Security experts agree that a firm's or business's biggest security weakness is the staff or employees. Good security includes staff training, polices regarding BYOD, procedures for personnel leaving the company or firm, social media policy, opening file attachments in e-mail, log-off procedures. The International Legal Technology Association (ILTA), a professional organization devoted to technology for law firms and law departments, regularly provides security education and materials and has peer groups that regularly exchange information.[2]

For the smaller firms, the de facto standard has become the National Institute of Standards and Technology (NIST) Cybersecurity Framework. It is spelled out in *Small Business Information Security: The Fundamentals* (24 pages) which is freely available at http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf. Law firms can self-certify that they are compliant or, if desired or required by a third party, engage an independent third-party auditor.

[2] www.iltanet.org

Larger law firms may choose to be certified under ISO 27001 from the International Organization for Standardization (ISO). This certification is well beyond the reach of all but large firms – it is expensive – and takes time and resources – and there are annual surveillance audits and recertification every three years.

The Legal Cloud Computing Association (LCCA) has developed basic and concise standards that lawyers and laws firms should use in selecting a cloud computing provider. http://www.legalcloudcomputingassociation.org/standards/. The LCCA Standards can be outlined as follows:

As far as relevant security measures, law firms should consider these elements:

- Physical security of confidential information and network resources
- Secure configuration (network and endpoints)
- Firewall and network appliances
- Security software: current version + update
- Patch management (network and endpoints)
- Authentication and access control
- Manage password/passphrase age and complexity
- Change all default passwords
- Block access after multiple failed attempts
- Timeout after inactivity (automatic logoff or screensaver requiring password)
- Strong authentication for remote access (two factor best)
- Encryption of confidential data on laptops and portable media
- Encryption of confidential data transmitted over the Internet or wireless networks
- Monitoring and logging
- Equipment or vendor for secure disposal

Most state bar ethics opinions agree that lawyers may store client data "in the cloud" if they use reasonable care in the selection of a cloud computing provider. See attached "Ethics Opinions and Articles re Cloud Computing."

3. Is there an ethical duty for lawyers to use encryption?

The consensus in the late 1990s is that, in general, and except in special circumstances, the use of email, including unencrypted email, is a proper method of communicating confidential information. See, e.g., ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011); State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 (2010); Prof'l Ethics Comm. of the Maine Bd. of Overseers of the Bar, Op. No. 195 (2008); N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 820 (2008); Alaska Bar Ass'n Ethics Comm., Op. 98-2 (1998); D.C. Bar Legal Ethics Comm., Op. 281 (1998); Ill. State Bar Ass'n Advisory Opinion on Prof'l Conduct, Op. 96-10 (1997); State Bar Ass'n of N.D. Ethics Comm., Op. No. 97-09 (1997); S.C. Bar Ethics Advisory Comm., Ethics Advisory Op. 97-08 (1997); Vt. Bar Ass'n, Advisory Ethics Op. No 97-05 (1997).

A Texas state bar ethics opinion has indicated that there may be circumstances where lawyers may have to encrypt e-mail communications with their clients. Attorneys who handle divorce, employment and criminal defense

matters may in some circumstances have a duty "to consider whether it is prudent to use encrypted email" to communicate with clients, the Texas bar's ethics committee concluded in April 2015. The opinion addresses an issue that many experts have urged bar authorities to look at anew: whether technological changes and escalating concerns over computer hacking has made it necessary to revisit existing guidance on using e-mail to communicate with clients. See State Bar of Texas Ethics Op. 648 (April 2015) found at http://www.legalethicstexas.com/getattachment/9936985b-f798-41c6-bc9f-97d4e0bff9de/Opinion-648.aspx

What are the circumstances that would require encryption? The committee identifies these examples:

1. communicating highly sensitive or confidential information via email or unencrypted email connections;

2. sending an email to or from an account that the email sender or recipient shares with others;

3. sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer (see ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011));

4. sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;

5. sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or

6. sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.

In 2011, Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility issued Formal Opinion 2011-200 that states as follows:

> …Compounding the general security concerns for email is that users increasingly access webmail using unsecure or vulnerable methods such as cell phones or laptops with public wireless internet connections. Reasonable precautions are necessary to minimize the risk of unauthorized access to sensitive client information when using these devices and services, possibly including precautions such as encryption and strong password protection in the event of lost or stolen devices, or hacking.

Thus, in the 17 years since the ABA issued Formal Op. 99-413, increasing attention is being paid to additional precautions lawyers should take when transmitting sensitive confidential information and the particular circumstances under which those communications are made. As reported in the *Lawyers' Manual*:

> …University of Georgia law professor Lonnie T. Brown said the consensus on communicating with clients through unencrypted email—driven by a 1999 ABA ethics opinion that approved the practice—may be giving way as authorities reconsider the risks of email interception.

Speaking at a ABA Center for Professional Responsibility Conference session in 2015 on developments in confidentiality, Brown said “we have come a long way in [the] 16 years” since the ABA opinion was issued, and that a number of state ethics panels have shown a willingness to impose more onerous security requirements on lawyers. - *31 Law. Man. Prof. Conduct 320* (2015).

One of the more simple and straightforward ways to encrypt e-mail communications is to copy and paste the e-mail contents into Adobe Acrobat Pro, and save the document with password encryption. Adobe Acrobat Pro uses 256-bit encryption. The client can view the document unencrypted by downloading the free Adobe Acrobat Reader, if they haven’t already installed that application.

For a concise and readable explanation of how lawyers can use encryption--see David G. Ries and John w. Simek, *Encryption Made Simple for Lawyers,* found at http://www.americanbar.org/publications/gp_solo/2012/november_december2012privacyandconfidentiality/encryption_made_simple_lawyers.html

Ethics Opinions and Articles re: "Cloud Computing"

http://apps.americanbar.org/lpm/lpt/articles/pdf/ftr10106.pdf
Have Attorneys Read the iCloud Terms and Conditions?
Sharon D. Nelson and John W. Simek
http://www.slaw.ca/2012/01/30/have-attorneys-read-the-icloud-terms-and-conditions/
Alabama Opinion 2010-020: Retention, Storage, Ownership, Production and Destruction of Client Files
http://www.alabar.org/ogc/fopDisplay.cfm?oneId=425
State Bar of Arizona Ethics Opinion 09-04: Confidentiality; Maintaining Client Files; Electronic Storage; Internet
http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=704
California Opinion 2010-179
http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=837
Iowa Opinion 11-01
http://www.iabar.net/ethics.nsf/e61beed77a215f6686256497004ce492/02566cb52c2192e28625791f00834cdb/$FILE/Ethics%20Opinion%2011-01%20--%20Software%20as%20a%20Service%20-%20Cloud%20Computing.pdf
Maine Opinion #194: Client Confidences: Confidential Firm Data Held Electronically and Handled By Technicians For Third-Party Vendors
http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions&id=86894&v=article
Massachusetts Ethics Opinion 12-03
http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03
New Jersey Opinion 701
http://www.judiciary.state.nj.us/notices/ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf
New York Opinion 842
http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=42697&TEMPLATE=/CM/ContentDisplay.cfm
North Carolina 2011 Formal Ethics Opinion 6
http://www.ncbar.com/ethics/printopinion.asp?id=855
Oregon Opinion 2011-188
http://www.osbar.org/_docs/ethics/2011-188.pdf
Pennsylvania Formal Opinion 2011-200: Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property
http://www.padisciplinaryboard.org/newsletters/2012/pdfs/2011-200-Cloud-Computing.pdf
Vermont Opinion 2010-6
https://www.vtbar.org/FOR%20ATTORNEYS/Advisory%20Ethics%20Opinion.aspx

Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others

IR-2017-20, Feb. 2, 2017 Español

WASHINGTON — The Internal Revenue Service, state tax agencies and the tax industry issued an urgent alert today to all employers that the Form W-2 email phishing scam has evolved beyond the corporate world and is spreading to other sectors, including school districts, tribal organizations and nonprofits.

In a related development, the W-2 scammers are coupling their efforts to steal employee W-2 information with an older scheme on wire transfers that is victimizing some organizations twice.

"This is one of the most dangerous email phishing scams we've seen in a long time. It can result in the large-scale theft of sensitive data that criminals can use to commit various crimes, including filing fraudulent tax returns. We need everyone's help to turn the tide against this scheme," said IRS Commissioner John Koskinen.

When employers report W-2 thefts immediately to the IRS, the agency can take steps to help protect employees from tax-related identity theft. The IRS, state tax agencies and the tax industry, working together as the Security Summit, have enacted numerous safeguards in 2016 and 2017 to identify fraudulent returns filed through scams like this. As the Summit partners make progress, cybercriminals need more data to mimic real tax returns.

Here's how the scam works: Cybercriminals use various spoofing techniques to disguise an email to make it appear as if it is from an organization executive. The email is sent to an employee in the payroll or human resources departments, requesting a list of all employees and their Forms W-2. This scam is sometimes referred to as business email compromise (BEC) or business email spoofing (BES).

The Security Summit partners urge all employers to be vigilant. The W-2 scam, which first appeared last year, is circulating earlier in the tax season and to a broader cross-section of organizations, including school districts, tribal casinos, chain restaurants, temporary staffing agencies, healthcare and shipping and freight. Those businesses that received the scam email last year also are reportedly receiving it again this year.

Security Summit partners warned of this scam's reappearance last week but have seen an upswing in reports in recent days.

New Twist to W-2 Scam: Companies Also Being Asked to Wire Money

In the latest twist, the cybercriminal follows up with an "executive" email to the payroll or comptroller and asks that a wire transfer also be made to a certain account. Although not tax related, the wire transfer scam is being coupled with the W-2 scam email, and some companies have lost both employees' W-2s and thousands of dollars due to wire transfers.

The IRS, states and tax industry urge all employers to share information with their payroll, finance and human resources employees about this W-2 and wire transfer scam. Employers should consider creating an internal policy, if one is lacking, on the distribution of employee W-2 information and conducting wire transfers.

Steps Employers Can Take If They See the W-2 Scam

Organizations receiving a W-2 scam email should forward it to phishing@irs.gov and place "W2 Scam" in the subject line. Organizations that receive the scams or fall victim to them should file a complaint with the Internet Crime Complaint Center (IC3,) operated by the Federal Bureau of Investigation.

Employees whose Forms W-2 have been stolen should review the recommended actions by the Federal Trade Commission at www.identitytheft.gov or the IRS at www.irs.gov/identitytheft. Employees should file a Form 14039, Identity Theft Affidavit, if the employee's own tax return rejects because of a duplicate Social Security number or if instructed to do so by the IRS.

The W-2 scam is just one of several new variations that have appeared in the past year that focus on the large-scale thefts of sensitive tax information from tax preparers, businesses and payroll companies. Individual taxpayers also can be targets of phishing scams, but cybercriminals seem to have evolved their tactics to focus on mass data thefts.

Be Safe Online

In addition to avoiding email scams during the tax season, taxpayers and tax preparers should be leery of using search engines to find technical help with taxes or tax software. Selecting the wrong "tech support" link could lead to a loss of data or an infected computer. Also, software "tech support" will not call users randomly. This is a scam.

Taxpayers searching for a paid tax professional for tax help can use the IRS Choosing a Tax Professional lookup tool or if taxpayers need free help can review the Free Tax Return Preparation Programs. Taxpayers searching for tax software can use Free File, which offers 12 brand-name products for free, at www.irs.gov/freefile. Taxpayer or tax preparers looking for tech support for their software products should go directly to the provider's web page.

Tax professionals also should beware of ongoing scams related to IRS e-Services. Thieves are trying to use IRS efforts to make e-Services more secure to send emails asking e-Services users to update their accounts. Their objective is to steal e-Services users' credentials to access these important services.

See also:

- Affected employers and companies should also alert the state tax agencies by notifying StateAlert@taxadmin.org.

Follow the IRS on Social Media

Subscribe to IRS Newswire

Page Last Reviewed or Updated: 02-Feb-2017

MULTI-STATE Information Sharing & Analysis Center™

MS-ISAC Security Primer
Spear Phishing

March 23, 2016, SP2016-0518

TLP: WHITE **Overview:** Cyber threat actors utilize phishing emails to compromise systems, networks, and/or gather information using social engineering techniques. A phishing email is designed to prompt a response from the recipient, such as clicking on a link or opening an attachment. Through the response, the recipient may download malware or be redirected to a website prompting them to provide sensitive information, such as login credentials, that will be sent to the cyber threat actors. Spear phishing involves a cyber threat actor sending targeted emails to a small group of users.

Other types of phishing include:
- Smishing ("SMS phishing") involves a user opening a malicious SMS, or text, message on a mobile device.
- Vishing involves a cyber threat actor attempting to gather information over Voice over IP (VoIP) phones.
- Whaling is a spear phishing attempt directed towards a senior executive or other high profile target.

TLP: WHITE **TECHNICAL RECOMMENDATIONS:**

- Implement filters at the email gateway to filter out emails with known phishing indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- Consider blocking attachments that are file types commonly associated with malware, such as .dll and .exe, and file types that cannot be thoroughly scanned by antivirus software, such as .zip files.
- Utilize Sender Policy Framework (SPF), a validation system that minimizes spam emails by detecting email spoofing and allowing administrators to specify who is allowed to send email from a given domain by creating a SPF record in the Domain Name System (DNS).
- Adhere to the principal of least privilege, whereby a user and/or application only has the rights necessary to carry out their daily activities. If a user has no need for administrative access on a machine, they should not have an administrative account. This will help minimize the damage caused by malicious activity carried out under the user's credentials.
- Apply appropriate patches and updates provided by Microsoft, Oracle, Adobe, and other third party application providers to vulnerable systems immediately after appropriate testing. Malware frequently exploits vulnerabilities for which a software patch was released.
- Use antivirus programs with automatic updates of signatures and software.
- Provide social engineering and phishing training to employees. Urge them not to open suspicious emails, not to click links contained in such emails, not to post sensitive information online, and to never provide usernames, passwords, and/or personal information to any unsolicited request.
- Create a policy for reporting phishing emails to the Information Technology (IT) department.

TLP: WHITE **USER RECOMMENDATIONS:**

- Do not open suspicious emails or attachments, as they may contain malware. Only open expected attachments from trusted senders.
- The easiest way to check a link is by hovering over it with your mouse. This action allows the true destination of the link to appear in the bottom left corner of your browser window or next to your mouse pointer in Microsoft Outlook.
- Never reveal personal or financial information in response to an email. Legitimate organizations and financial institutions will never ask for this information in an unsolicited email.
- If the message appears to be a phishing or spam email, do not respond. Report it to the IT department immediately and await further instruction.

TLP: WHITE *For more information regarding this cyber threat actor please contact the Multi-State Information Sharing and Analysis Center (MS-ISAC), 31 Tech Valley Drive, East Greenbush, NY 12064, 866-787-4722, SOC@cisecurity.org, www.cisecurity.org.*

TLP: WHITE

Image Credit: iStockphoto/Thinkstock

2016 SLTT Government Outlook

February 2016

MS-ISAC

Multi-State Information Sharing and Analysis Center

TLP: WHITE

2016 SLTT Government Outlook

INTRODUCTION

In 2016, the Multi-State Information Sharing and Analysis Center (MS-ISAC) expects new and more sophisticated tactics, techniques, and procedures (TTPs) will target state, local, tribal, and territorial (SLTT) governments with increasing frequency, although routine malware infections will remain the most prevalent problem. New and existing cyber threat actors[1] will likely target specific SLTT governments in a pattern of limited-duration campaigns. We estimate that more cyber threat actors, primarily financially motivated, will identify SLTT governments as repositories of information in 2016 and will target them for personally identifiable information (PII), personal health information (PHI), and financial data, although this targeting will remain limited compared with targeting of the commercial sector.

31 Tech Valley Drive
East Greenbush, NY 12061
518-266-3460,
info@cisecurity.org,
www.cisecurity.org

MS-ISAC is virtually certain that the 2016 cybersecurity workforce demand will continue to outstrip the available workforce, creating challenges in SLTT government cybersecurity efforts.

TACTICS, TECHNIQUES, and PROCEDURES

Malware

The sophistication of cyber crime TTPs is highly likely to continue to increase in 2016, as cyber threat actors combine TTPs to create new attack and scam variants, and develop enhanced malware capabilities and more sophisticated delivery mechanisms. Financially motivated cyber threat activity will remain the most prevalent type of activity during 2016, with most malware and attacks motivated by this purpose. Malware and attacks that focus on the data's integrity are likely to become more common in 2016, although these attacks will still be vastly outnumbered by the attacks against the confidentiality and/or availability of data. We believe there is a slight chance that the rare cyber attacks that intentionally cause physical harm will effect SLTT governments, although not intentionally. Similarly, there is a slight chance that purely destructive cyber attacks, which are currently occurring outside of the SLTT government sector, could unintentionally effect SLTT government entities.

Financially motivated malware is highly likely to continue to dominate the SLTT government threat domain. It is highly probable that keyloggers will remain a popular method of financial theft, while exploit kits, Trojan horses, and worms will continue to focus on pay-per-install revenue, click-jacking, and coopting of SLTT government resources for use in botnets and spam campaigns. Cyber threat actors will increasingly look to malvertising as a way to distribute their malware, due to its effectiveness.

DDoS

We expect that distributed denial of service (DDoS) attacks targeting SLTT governments will become more prevalent with targeting ranging from unknown causes to motivations as specific as preventing a school exam or in response to an incident involving a perceived injustice or the alleged use of excessive force by a law enforcement official. In large part, we believe singular cyber threat actors and hacktivist use of DDoS as a common TTP will drive this trend. Although we believe it will be rare in occurrence, the occasional DDoS attack will likely be used to divert SLTT government agency attention away from other malicious activity.

[1] An identified cyber threat actor is an identifiable individual person who participates in malicious cyber activity . while explicitly noting they work independent of other cyber threat actors and without claiming allegiance to one cyber threat actor group or movement.

Extortion

Extortion related TTPs, primarily ransomware, will almost certainly pose an increasing threat to SLTT governments in 2016. It is highly likely that the 2016 ransomware threat will include new variants deployed by an expanding array of cyber threat actors eager to cash in on ransomware's simplicity. The movement to ransomware-as-a-service will only expand this trend as ransomware becomes more available to a broader range of less sophisticated cyber threat actors who are likely to use additional deployment techniques. Some extortion-related TTPs, such as DDoS attacks, in which the attackers extort money in order to stop the attacks, are likely to be rare in the SLTT government domain in 2016. We anticipate that this will begin to impact critical infrastructure operators on 2016.

TARGETED DATA and SYSTEMS

Data Compromises

We are convinced that data compromises, especially small scale, publicly shared data dumps, will continue to threaten SLTT government cybersecurity in 2016. It is highly probable that the reuse of user names, email addresses, and passwords between SLTT government accounts and personal accounts will remain the largest threat from data dumps. Additionally, some SLTT government data will likely be compromised in online postings or sold to other malicious actors following intrusions against federal or SLTT government agencies. However, we expect the majority of these incidents to be limited impact events based on opportunistic targeting.

Targeting of PII, PHI, and Financial Data

In 2016, we believe that a few cyber threat actors will likely identify SLTT governments as repositories of information and specifically target them for this reason. In particular, it is highly likely these efforts will focus on PII, PHI, and financial data. However, we also believe that while SLTT government compromises in these areas will slightly increase, the majority of cyber threat actors will continue to focus their efforts on the data available in the commercial sector and not SLTT government entities. It is possible that the one exception to this will be the healthcare sector, as it is likely that hospitals will be an increasingly common target due to the rising interest in PHI, and the hospitals public or private affiliation will not be a consideration in the compromise attempts.

Content Management Systems

It is highly likely that content management systems (CMS) will remain a primary target for web server compromises in 2016 as they remain a highly vulnerable and infrequently updated platform. The number of MS-ISAC identified website defacements and compromises has increased each year over the past several years, and this trend will likely continue in 2016, with out-of-date CMS as a prime target. While a spike in printer defacements in 2015 appeared opportunistic, we believe there is a potential that another spike in defacement activity could reoccur.

Point of Sale Systems

The compromise of SLTT government owned or operated point of sale (POS) devices will likely increase in 2016, although we believe the majority of SLTT government POS compromises will be opportunistic in nature. Similarly, the compromise of mobile devices will increase in 2016, but we believe that cyber threat actor targeting of SLTT government owned devices will be almost completely opportunistic.

Internet of Things

The introduction of new non-traditional computing devices, broadly categorized as the Internet of Things (IOT), will almost certainly challenge SLTT governments operations and pose new threats to the security of SLTT government networks. End-users

are highly likely to expand the number of personal Internet-enabled devices introduced into the workplace, prompting new wireless connectivity, data sharing, and security concerns. The use of drones, body worn cameras, wearables, and other network-enabled approved tools, as well as the push for smart cities and pervasive WiFi access, will create a greater burden on information technology (IT) departments as they seek to incorporate these devices into the network and ensure cybersecurity remains a priority.

TARGETED SECTORS

Universities

We have high confidence that cyber threat actors will continue to routinely target universities in 2016, for the purposes of financial gain, to gain access to PII and/or sensitive research, or for notoriety or… launching point. This threat will likely continue to develop, although MS-ISAC believes the threat and reporting will both slightly increase, resulting in a biased threat perspective of a larger increase.

Supply Chain

The supply chain threat to SLTT governments is highly likely to continue to be high in 2016, although there are limited examples of instances where governments were specifically targeted. Opportunistic targeting through counterfeit or compromised software and equipment is likely to remain a high threat and unchanged in 2016, and will continue to pose a substantial risk to SLTT governments as counterfeit software and equipment often prevents patching and updating, thereby increasing the software's exposure to exploitation.

Industrial Control Systems

The 2016 threat against Industrial Control Systems (ICS) remains a wildcard. Security researchers are interested in ICS vulnerabilities, malicious actors show interest in ICS honeypots, exploits exist to target ICS, and tools such as SHODAN and Censys make identifying Internet-facing systems extremely easy but these factors have existed together for the last several years with only a few major attacks occurring. We believe that attacks on ICS systems will continue to slowly increase in frequency, regardless of whether or not a major, successful attack occurs. However, MS-ISAC believes that it is unlikely that cyber threat actors will specifically target SLTT government entities for such an attack. Instead, if such an attack occurs, it will likely be focused on the critical infrastructure itself.

CYBER THREAT ACTORS

Cross-Pollination of TTPs Between Cyber Threat Actor Groups

The cross-pollination of TTPs between cyber threat actor groups, specifically, nation-state actors, hacktivists, and financially motivated cyber criminals, is highly likely continue in 2016 as hacktivists and cyber criminals continue to adopt more advanced techniques such as spear phishing and watering holes. As part of this, the ripple-effect will likely continue to grow, as cyber threat actors learn from one-another and replicate the techniques they see reported in open source media and discussed within their communities.

Cyber Criminals and Hacktivists

The pattern of singular cyber threat actors, primarily cyber criminals and hacktivists, appearing and conducting a multitude of limited-duration campaigns against SLTT governments will continue to occur into 2016, creating prominent, but unpredictable spikes in activity. We believe activity by singular cyber threat actors will account for the majority of SLTT government targeting by identified cyber threat actors. This activity is unpredictable in nature, although we have moderate-high confidence that some periods of the year will sustain heavier activity than others. In 2016, MS-ISAC has moderate confidence that

hacktivist activity against SLTT governments will be motivated by incidents involving the alleged use of excessive force by law enforcement personnel, and that SLTT governments should prepare to react to non-cyber threats from hacktivists, such as doxing and protests, as well as traditional cyber threats, such as DDoS attacks. We also estimate that the most common motivation behind general cyber threat actor activity will be related to attention seeking and/or Internet notoriety.

Tradecraft

Over the next one to three years, MS-ISAC expects that cyber threat actors' tradecraft will increase, as they become more aware of the social media research practices used by private intelligence firms and federal, SLTT government, and law enforcement agencies, and seek to counter intelligence gathering practices. This tactic will make it more difficult to differentiate legitimate attacks from false or opportunistic claims taking advantage of unrelated network outages. In addition, it will simultaneously make a proactive approach to cybersecurity more challenging as defenders will have less cyber threat actor intelligence to incorporate when making decisions.

Nation-State Actors

In 2016, MS-ISAC expects to identify and/or become aware of more nation-state activity targeting SLTT governments, although it will be difficult to tell if that is due to increased activity or increased reporting. Also unclear is whether nation-state actors will target SLTT governments in order to gain access to the SLTT's data, with the intention of using the SLTT government as a hop point, or opportunistic targeting. SLTT governments should be aware of the changing nation-state threat landscape, affected by national political changes, such as the cyber agreement with China and the nuclear agreement with Iran.

DEVELOPING ISSUES

User Demand

Encryption, and especially the encryption of data at rest and in transmission, will continue to be a major issue in cybersecurity. We also believe that in 2016, residents and SLTT government employees are likely to increase their demands on IT infrastructure, with the desire for more user-friendly, accessible, and/or innovative solutions, which will further stretch SLTT government IT resources and pose cybersecurity challenges.

IPv6

IPv6 adoption is current at approximately 18% of the United States-based Internet,[2] and will continue to increase throughout 2016. With this increase, and as IPv6 is enabled on most devices by default, SLTT governments should be aware of the increasing interest in this technology by cyber threat actors. While unlikely to significantly affect SLTT governments in 2016, we recommend that SLTT governments monitor the continuing transition to IPv6, disable IPv6 on IPv4 networked devices where it is enabled by default, and consider developing their own transition plans.

Workforce

MS-ISAC is virtually certain that the 2016 cybersecurity workforce demand will continue to outstrip the available workforce, creating an employment gap that will place stress on SLTTs cyber security functions. This gap will in particular endanger SLTT government cybersecurity efforts, as SLTT government entities face challenges in matching private sector salaries and providing the flexible, engaging work environments that many new college graduates prefer.

Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive, East Greenbush, NY 12061, 518-266-3460, info@cisecurity.org, www.cisecurity.org

[2] Based on requests made to Akamai's dual-stacked customer web properties, as available at https://www.stateoftheinternet.com/trends-visualizations-ipv6-adoption-ipv4-exhaustion-global-heat-map-network-country-growth-data.html on February 1, 2016.

Report *based on* discussions *with the*

Security for Business Innovation Council

An industry initiative sponsored by RSA

ABN AMRO
DR. MARTIJN DEKKER, *Senior Vice President, Chief Information Security Officer*

ADP INC.
ROLAND CLOUTIER, *Vice President, Chief Security Officer*

AIRTEL
FELIX MOHAN, *Senior Vice President and Chief Information Security Officer*

THE COCA-COLA COMPANY
RENEE GUTTMANN, *Chief Information Security Officer*

CSO CONFIDENTIAL
PROFESSOR PAUL DOREY, *Founder and Director; Former Chief Information Security Officer, BP*

EBAY
DAVE CULLINANE, *Chief Information Security Officer and Vice President, Global Fraud, Risk & Security*

EMC
DAVE MARTIN, *Chief Security Officer*

GENZYME
DAVID KENT, *Vice President, Global Risk and Business Resources*

HDFC BANK
VISHAL SALVI, *Chief Information Security Officer and Senior Vice President*

HSBC HOLDINGS plc
ROBERT RODGER, *Group Head of Infrastructure Security*

JOHNSON & JOHNSON
MARENE N. ALLISON, *Worldwide Vice President of Information Security*

JPMORGAN CHASE
ANISH BHIMANI, *Chief Information Risk Officer*

NOKIA
PETRI KUIVALA, *Chief Information Security Officer*

NORTHROP GRUMMAN
TIM MCKNIGHT, *Vice President and Chief Information Security Officer*

SAP AG
RALPH SALOMON, *Vice President, IT Security & Risk Office, Global IT*

T-MOBILE USA
WILLIAM BONI, *Corporate Information Security Officer (CISO), VP Enterprise Information Security*

WITH GUEST CONTRIBUTOR:
WILLIAM PELGRIN, *President & CEO, Center for Internet Security; Chair, Multi-State Information Sharing and Analysis Center (MS-ISAC); and Immediate Past Chair, National Council of ISACs (NCI)*

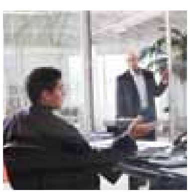
GETTING AHEAD OF ADVANCED THREATS

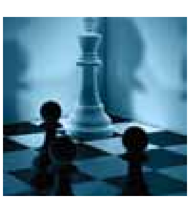
Achieving Intelligence-Driven Information Security

RECOMMENDATIONS FROM GLOBAL 1000 EXECUTIVES

INSIDE THIS REPORT:

Contents





Report Highlights

IN TODAY'S THREAT landscape, organizations worldwide face a growing number of sophisticated cyber adversaries.

"ADVANCED THREATS" ARE increasingly targeting corporations and governments in order to conduct industrial espionage, undermine business and financial operations, and/or sabotage infrastructure.

THE HARD TRUTH IS MOST organizations don't know enough about the threats or their own security posture to defend themselves adequately against the rising tide of cyber attacks.

THE TIME HAS COME WHEN successful defense requires evolving past conventional approaches in information security.

A NEW APPROACH IS NEEDED. Called "intelligence-driven information security," this approach includes:

- The consistent collection of reliable cyber-risk data from a range of government, industry, commercial, and internal sources to gain a more complete understanding of risks and exposures.
- Ongoing research on prospective cyber adversaries to develop knowledge of attack motivations, favored techniques, and known activities.
- The growth of new skills within the information team focused on the production of intelligence.
- Full visibility into actual conditions within IT environments, including insight that can identify normal versus abnormal system and end-user behavior.
- A process for efficient analysis, fusion, and management of cyber-risk data from multiple sources to develop actionable intelligence.
- Practices to share useful threat information such as attack indicators with other organizations.
- Informed risk decisions and defensive strategies based on comprehensive knowledge of the threats and the organization's own security posture.

THE VISION IS TO HARNESS THE power of information to prevent, detect, and ultimately *predict* attacks.

THE VALUE PROPOSITION IS clear. By maximizing the use of available information, the organization can create and implement more precise defensive strategies against evolving threats. Security will not only improve but also become more cost-effective because it will be targeted at countering the most significant threats and protecting the most strategic assets.

NOTE ON THE SCOPE OF THIS REPORT:

THIS REPORT is focused on the collection and analysis of cyber-risk data. However, many organizations' intelligence programs may include a broader set of data. For example, they may include physical-security data (building access, travel), manufacturing supply chain risks (availability, delivery), and/or data on competitors (financials, product developments). Although the scope of this report is cyber-risk intelligence, the goal for some organizations' intelligence programs is to build a complete picture of operational risks.

THIS REPORT PROVIDES A SIX-step roadmap for achieving intelligence-driven information security.

THE GUIDANCE ANSWERS critical questions such as:

- What are the basic requirements for building an intelligence capability?
- What does it take to develop broad organizational support and obtain funding?
- What is the skill set required of a cyber-risk intelligence team?
- What are the best sources of data?
- How can an organization design a process that will consistently produce actionable intelligence and the right defensive strategies?
- What type of automation can help create efficiencies for handling large volumes of data?

A CRITICAL ASPECT OF achieving intelligence-driven information security is sharing cyber-risk data with other organizations. But there are many significant challenges to creating information-sharing mechanisms.

FORTUNATELY, THERE IS A growing number of industry and government-led initiatives as well as public/private partnerships that are working to enable large-scale data exchange.

1 Introduction: The Need to Know

Corporations and governments worldwide are increasingly targeted by cyber adversaries with a range of goals from political activism and sabotage to intellectual-property theft and financial gain. As cyber attacks intensify and tactics rapidly evolve, organizations could find the escalating threat landscape overwhelming their abilities to manage the risks.

The hard truth is most organizations don't know enough about the threats or their own security posture to defend themselves adequately. For example, they can't see signs of an attack because they haven't sufficiently analyzed data on the latest attack techniques. They can't identify malicious activity because they haven't developed baselines for normal activity.

Today's dedicated adversaries have the means to evade commonly used defenses such as signature-based detection. In the era of advanced threats, greater situational awareness is essential to detect and mitigate cyber attacks effectively. Organizations need to obtain the latest data on threats, relate that to real-time insights into their dynamic IT and business environments, determine what's relevant, make risk decisions, and take defensive action.

Intelligence gathering and analysis have become essential capabilities for a successful information-security program, yet most enterprise IT

Cyber-risk intelligence is table stakes in 21st-century commerce. If you want Internet access to a global array of customers and suppliers, then you have to invest in developing the intelligence capabilities to defend against global threats.

WILLIAM BONI,
Corporate Information Security Officer (CISO),
VP Enterprise Information Security,
T-Mobile USA

security organizations have not been built with this objective in mind. In fact, many cyber adversaries have developed better intelligence capabilities than their targets.

While many organizations may have access to the right data, they may not be set up to make use of it. Internal data collection is often tuned for compliance reporting not cyber-threat analysis. There are many external sources of threat data available, such as government channels, industry associations, and commercial data feeds. However, most organizations are not fully utilizing these sources. In addition, in order to maximize their value, many current information-sharing mechanisms would require increased participation.

This ninth report of the Security for Business Innovation Council (SBIC) features the perspectives of top security leaders from Global 1000 companies, as well as a guest contributor from the U.S. National Council of ISACs (NCI). Today's threats are dynamic and increasing in sophistication, requiring a fresh and more comprehensive approach to defense. This report provides a playbook for creating a new approach based on building an organizational competency in cyber-risk intelligence and fully leveraging data from internal and external sources. Advanced threats represent an escalating risk to business innovation. This report lays out a roadmap to achieving intelligence-driven information security in order to get ahead of the threats and protect critical information assets.

2 What Do Organizations Need to Know?

Organizations need to understand the cyber threats they face and their security posture against those threats. For this report, "cyber-risk intelligence" is defined as "knowledge about cyber adversaries and their methods combined with knowledge about an organization's security posture against those adversaries and their methods." The goal is to produce "actionable intelligence," which is knowledge that enables an organization to make risk decisions and take action. To gain that knowledge, organizations must take input data and process it. In this report, the term for that input data is "cyber-risk data" and is broadly defined as "data that is collected and analyzed in order to prevent, detect, predict, and defend against cyber attacks."

Sample code from the Ice IX Trojan which was derived from the leaked code of the prolific banker Trojan, ZeuS.

Cyber-risk data

Data used to produce intelligence is available from a range of sources either external or internal to the organization. Open source is obtained from publicly available sources such as websites, as opposed to data from classified sources such as national-security agencies. It comes in many formats, such as word-of-mouth, emails, news feeds, automated data streams, output of numerous internal and external sensing platforms, and custom research. Some types, such as a list of IP addresses on a watch list, are generally applicable to all organizations. Other types are unique to one organization, for example notification that it is being targeted by a particular group.

To understand the intelligence process, it is important to recognize the distinction between "intelligence" and "data" or "information." Data received from various sources as described above is typically raw data that needs to be reviewed, analyzed, and put in context in order to develop intelligence which can then be used to make risk decisions.

Not all organizations will choose to collect all types of data from all sources. Some data may not be considered useful or may not be cost-effective to obtain. Other data may be deemed useful but not feasible to acquire yet, because an organization's processes and/or technology for handling that particular type of data still need to be set up and integrated.

Moreover, collecting more and more data is not the end goal. Having volumes of unanalyzed or unused data is of no value to an organization. Ultimately, for the data to be valuable, the organization must be able to apply it defensively, for immediate action in combatting a current or imminent cyber attack and/or for informing defensive strategies. As discussed in subsequent sections of this report, the defensive application must be determined through analysis, including fusing the data with other relevant facts and making a risk decision.

Charts 1 to 5 present categories of cyber-risk data including examples of sources, formats, and potential defensive applications. The charts reflect some typical examples of data formats that are used today. However, it should be acknowledged that over time, for an intelligence program to be effective, many categories of data must become machine-readable. Currently, many organizations are heavily dependent on highly skilled analysts to process, for example, long lists of text. Instead, it would make sense to automate the processing of basic data, freeing up the analysts' time to do actual analyzing.

Charts 1-5: Categories of Cyber-Risk Data with Examples

Each category answers a different question about the threats and an organization's security posture against them

ACRONYMS USED *in charts:*

CERT: Computer Emergency Response Team
ISAC: Information Sharing and Analysis Center
WARP: Warning, Advice, and Reporting Point
MSSP: Managed Security Service Provider
DDoS: Dedicated Denial of Service
NVD: National Vulnerability Database
SQL: Structured Query Language
SIEM: Security Information and Event Management
DLP: Data Loss Prevention
GRC: Governance, Risk, and Compliance

CHART 1

INPUT DATA ON CYBER ADVERSARIES AND THEIR METHODS – EXTERNAL SOURCES

CYBER-ATTACK INDICATORS

WHAT SIGNS ARE OTHER ORGANIZATIONS SEEING THAT COULD BE USED BY US TO PREVENT, DETECT, OR PREDICT A CYBER ATTACK?

Example Input Data	Example Sources	Example Formats	Potential Defensive Application (dependent on analysis)
Description of spear-phishing emails	• Open source • Government sources • Industry partners • Sector ISACs	• Email alert	• Identify and block these emails
Lists of domains hosting malware	• Open source • Government sources • Industry partners • Sector ISACs	• Email alert • Listserv	• Identify and block traffic to these domains
List of black-listed IP addresses	• Open source • Government sources • Industry partners • Sector ISACs • Vendor lists	• Email alert • Threat feed	• Identify and block traffic to these IP addresses
Set of binaries used by attackers	• Vendor lists • Tool output • MSSP • Cloud service	• Threat feed	• Identify and remove malware

CYBER-ATTACK TECHNIQUES

WHAT HAVE OTHERS LEARNED ABOUT ATTACK TECHNIQUES THAT COULD BE USED TO PREVENT, DETECT, PREDICT, OR DEFEND AGAINST CYBER ATTACKS?

Description of attack pattern using multiple vectors including social engineering	• Law enforcement cyber-intelligence agencies • Industry partners	• Briefing • In-person meeting	• Update detection methods and implement ways to block this attack technique
Description of new exploit involving mobile devices	• Government CERTs • Vendor community	• Email alert	• Update controls on mobile devices

CHART 1 (CONTINUED)

Example Input Data	Example Sources	Example Formats	Potential Defensive Application (dependent on analysis)
CYBER ATTACKERS' MOTIVES AND TARGETS			
WHAT ARE OUR ACTUAL OR POTENTIAL CYBER ADVERSARIES TRYING TO ACCOMPLISH?			
Explanation of trend whereby attackers select corporations with certain policies to hit with aggressive DDoS attacks	• Government agencies • Law enforcement cyber-intelligence agencies • Industry partners	• Information on hacktivism	• Shore-up DDoS defenses
Evidence that attackers are pursuing company's intellectual property such as new product plans or proprietary financial figures	• Commercial threat-intelligence services • Law enforcement cyber-intelligence agencies	• Threat feed • Custom research	• Increase protection of targeted assets
Evidence that nation-state operatives are stealing proprietary information from companies in the same industry	• Government agencies • Commercial threat-intelligence services • Law enforcement cyber-intelligence agencies	• Classified briefing • Custom research • In-person meeting	• Increase protection of targeted assets
CYBER ATTACKERS' IDENTITIES			
WHO ARE OUR ACTUAL OR POTENTIAL ATTACKERS?			
Specific information on attackers' identities: name and location of particular criminal groups which are targeting the company	• Government agencies • Commercial threat-intelligence services • Law enforcement cyber-intelligence agencies	• Classified briefing • Custom research • In-person meeting	• Learn to recognize specific attackers' footprints

CHART 2

INPUT DATA ON CYBER INCIDENTS AND COUNTER MEASURES – EXTERNAL SOURCES

EXTERNAL INCIDENT INFORMATION			
WHAT CAN WE LEARN FROM INCIDENTS AT OTHER ORGANIZATIONS TO PREVENT, DETECT, PREDICT, OR DEFEND AGAINST CYBER ATTACKS?			
Details regarding company in the same industry disclosing massive data breach	• Media • Sector ISACs • Industry partners	• News websites • Email alert • Information portals	• Integrate lessons learned into defensive strategies
COUNTER-MEASURES AND DEFENSIVE TECHNIQUES			
WHAT BEST PRACTICES CAN WE LEARN FROM OTHER ORGANIZATIONS TO DEFEND AGAINST CYBER ATTACKS?			
Description of new procedures for protecting admin accounts from hijacking	• Peer organizations • Sector ISACs	• Email alert • Information portals • In-person meeting	• Implement new controls around admin accounts

CHART 3

INPUT DATA ON AN ORGANIZATION'S SECURITY POSTURE RELATIVE TO CYBER THREATS – EXTERNAL SOURCES

Example Input Data	Example Sources	Example Formats	Potential Defensive Application (dependent on analysis)
GENERAL VULNERABILITIES			
ARE THERE VULNERABILITIES IN SOFTWARE/HARDWARE THAT COULD MAKE US PRONE TO ATTACK?			
Description of operating system vulnerability	• Government CERTs • Vendor community	• NVD data feed	• Implement patch
Description of SQL injection vulnerability	• Sector ISACs • Vendor community • Commercial threat-intelligence services	• Email alert	• Update application
SPECIFIC VULNERABILITIES			
ARE THERE SPECIFIC VULNERABILITIES REGARDING OUR SYSTEMS THAT COULD MAKE US PRONE TO ATTACK?			
Discovery of a set of the company's access credentials on hacker websites	• Cybercrime-intelligence service vendors	• Custom research	• Update credentials

"The threat can be broken down into three components: intent, opportunity, and capability. Organizations need to know, 'What is the intent of adversaries? What are the opportunities available to them? And what capabilities do they have to exploit the opportunities?'"

FELIX MOHAN, Senior Vice President and Chief Information Security Officer, Airtel

CHART 4

INPUT DATA ON AN ORGANIZATION'S SECURITY POSTURE RELATIVE TO CYBER THREATS – INTERNAL SOURCES

INFORMATION-ASSETS INVENTORY

WHAT ARE OUR MOST IMPORTANT INFORMATION ASSETS TO PROTECT AND WHERE ARE THEY LOCATED?

Example Input Data	Example Sources	Example Formats	Potential Defensive Application (dependent on analysis)
Periodic inventory of high-value assets including asset type, relative value to the organization, location, and security exposure	• Risk-management team	• Internal report	• Establish status and location of systems containing IP to ensure adequate protection

EMPLOYEE OBSERVATIONS

WHAT SUSPICIOUS ACTIVITIES ARE EMPLOYEES OBSERVING THAT COULD BE SIGNS OF A CURRENT OR FUTURE CYBER ATTACK?

Reports of phone calls being received by members of the R&D team asking about colleagues	• Employees' communications • Employees' entries into knowledge-management system	• Emails to Security • Knowledge-management system alert	• Determine attackers' methods and increase security controls to protect targeted assets

BUSINESS STRATEGY

WHAT ELEMENTS OF OUR STRATEGY WOULD CREATE POSSIBLE OPPORTUNITIES FOR A CURRENT OR FUTURE CYBER ATTACK?

Information regarding outsourcing of business processes to external providers	• Business/mission owners	• Internal reporting	• Implement real-time monitoring of new business partners' IT systems and security controls
Notice that company will be undergoing merger negotiations	• Finance department • Legal department	• Confidential memo to Security	• Implement increased monitoring and controls around privileged users involved in negotiations
Evidence that reduction in workforce is creating disgruntled employees	• Human resources department	• Confidential memo to Security	• Implement increased monitoring and controls for employees with access to protected assets

INTERNAL INCIDENT INFORMATION

WHAT CAN WE LEARN FROM PAST CYBER INCIDENTS TO PREVENT, DETECT, PREDICT, OR DEFEND AGAINST FUTURE ONES?

Report regarding malware that was detected and remediated	• Security-operations team	• Incident report	• Integrate lessons learned and strategy to shorten kill chain in the future

CHART 5

INPUT DATA ON AN ORGANIZATION'S SECURITY POSTURE RELATIVE TO THE CYBER THREATS – IT AND SECURITY SOURCES

CYBER-RISK INFRASTRUCTURE EVENTS

ARE EVENTS WITHIN THE SECURITY INFRASTRUCTURE SIGNS OF A CURRENT OR FUTURE ATTACK?

Example Input Data	Example Sources	Example Formats	Potential Defensive Application (dependent on analysis)
Warning that unauthorized connections to servers attempted	• Correlated SIEM events	• System alerts	• Determine source of attack and target of interest; disrupt attacker and investigate further
Signs of command and control activity, data exfiltration, or other lateral movement	• Full packet capture, DLP or SIEM events	• System alerts	• Determine source of attack and target of interest; disrupt attacker and investigate further

END-USER AND SYSTEM BEHAVIOR DATA

IS END-USER OR SYSTEM BEHAVIOR SIGNALING A POSSIBLE CURRENT OR FUTURE CYBER ATTACK?

Sign of an unusual admin remote login – comparison with baseline	• Authentication log • SIEM	• Log analysis alerts	• Determine source of attack and target of interest; disrupt attacker and investigate further
Sign of increasing password resets – notable trend	• Full packet capture • Application logs	• System alerts	• Determine source of attack and target of interest; disrupt attacker and investigate further
Sign of unusual data movement – traffic outside of the norm or to unusual destinations	• Full packet capture • Application logs	• System alerts	• Determine source of attack and target of interest; disrupt attacker and investigate further

STATUS OF CONTROLS

WHAT IS THE CONDITION OF OUR CURRENT CYBER DEFENSES?

Notification that major business line did not complete mandatory password resets for all users	• GRC system	• System report	• Increase monitoring on specific systems until remediated
Notification of upload-policy violations	• DLP system	• System report	• Increase monitoring on specific systems and investigate further

3 Time for a New Approach

Intelligence-Driven Information Security

Depending on the maturity of the information-security program, organizations may already integrate cyber-risk data into their defensive strategies. For example, it is fairly common for organizations to have a basic vulnerability-management program for collecting data on software and hardware vulnerabilities and ensuring systems are adequately patched and updated. Many security professionals read industry publications such as vendor reports on malware and data breaches and consider this information when creating security strategies.

For most information-security programs, however, data collection and analysis are not strong suits. Collection from external sources is often fragmented and not integrated with internal data sources. And although many organizations collect reams of data from applications and security systems, they aren't harvesting and analyzing the data to gain an understanding of their environment, such as developing baselines for normal activity. Instead, much of the data ends up as dead logs.

Most organizations do not have a concerted effort to collect, amalgamate, analyze, operationalize, and manage cyber-risk data in order to develop intelligence. Yet more and more organizations need this capability in order to defend against advanced threats.

DEFINITION

Intelligence-driven information security

Developing real-time knowledge on threats and the organization's posture against those threats in order to prevent, detect, and/or predict attacks, make risk decisions, optimize defensive strategies, and enable action.

There is mounting evidence that organizations in a wide range of industries are increasingly targeted by sophisticated adversaries. For example, a recent report by the U.S. Office of the National Counterintelligence Executive[1] states, "The pace of foreign economic collection and industrial espionage activities against major U.S. corporations and U.S. government agencies is accelerating." A major reason is the accessibility of sensitive data in cyberspace. The report also indicates that many companies are unaware when their sensitive data is pilfered. Further, it suggests that areas of great interest to cyber spies include information and communications technology, natural resources, defense, energy, and healthcare/pharmaceuticals.

> *"It can be hard to digest having to develop a multi-year plan to learn who your adversaries are and how they're going to steal from you. Quarter-by-quarter, you may not see any losses. It could be years until you see the losses – when all of a sudden, out of the blue, a company in another part of the world becomes the leader in your space, having subsidized itself with your R&D investments."*

TIM MCKNIGHT
Vice President and Chief Information Security Officer, Northrop Grumman

[1] "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," Office of the Director of National Intelligence/Office of the National Counterintelligence Executive, October 2011

Other studies indicate that companies across the globe are being targeted. For example, the Enterprise Strategy Group surveyed companies in the U.S. and Europe regarding advanced persistent threats (APTs) and found that 59% of security professionals surveyed at U.S. companies[2] and 63% of those at European companies[3] believe it is "highly likely" or "likely" that their organizations have been APT targets.

In today's threat landscape, organizations face targeted, complex, multi-modal attacks which can be carried out over periods of time. They need to fuse together data drawn from multiple sources to effectively detect and mitigate attacks. They need comprehensive, accurate, and timely information to make informed decisions about defensive strategies. The time has come when successful defense requires evolving past conventional approaches in information security to developing competencies in data fusion, knowledge management, and analytics.

Change of mind-set required

Currently, many information-security programs are compliance-led: Decision making about defensive strategies is based on the audit cycle or the need to simply meet a regulatory baseline. Another common approach is incident-led: Decision making is based on day-to-day fire-fighting. What is needed is an intelligence-driven approach, whereby decisions are made based on real-time knowledge regarding the cyber adversaries and their attack methods, and the organization's security posture against them.

Some security professionals may see gaining intelligence about potential cyber threats as the government's responsibility, but it is unrealistic for any national government to take on threat analysis for each specific organization, especially in the private sector. Governments don't have the resources nor do they have the mandate. It is the organization itself that knows its own business or mission, market position, asset valuation, and vulnerabilities and can make the best determination of the cyber threats it confronts. However, governments can play an important role in providing cyber-risk intelligence and fostering information sharing.

Building an intelligence capability will also require developing a counterintelligence and operational security mind-set among the entire extended security team. This means seeing one's own organization from the perspective of the adversaries who are targeting it, being able to understand their tools and techniques, and identifying potential vulnerabilities before they do.

Key features

An intelligence capability applies expertise, processes, and tools to:

- consistently collect the right data from the right sources
- efficiently amalgamate, analyze, and manage the data
- develop knowledge and produce actionable intelligence
- make risk decisions and take action by modifying controls or planning new defenses
- share relevant pieces of data such as attack indicators with other organizations

Building this capability will require investments in people, process, and technology. Of course, not every organization has to achieve the intelligence capability of a national-security agency. But there is a large spectrum between having no accountability for intelligence and achieving the level required by a highly specialized threat environment. Every organization will need to determine its level of investment based on the particular threats it faces, the value of the assets it needs to protect, and its risk profile.

Organizations don't have to make huge investments to get started. They can start today using existing personnel, for example, to improve the collection and analysis of log data or to integrate open source threat intelligence. Over time, a key element will be automation to help decrease manual processes. Otherwise the collection and analysis of greater amounts of data could become onerous and resource-intensive. Another important aspect is having an agile program whereby protection methods can be dynamically put into place in response to the intelligence.

The vision is to harness the power of information to prevent, detect, and ultimately predict attacks. Getting ahead of threats requires an ability to see what's coming in order to determine appropriate action before an attack happens.

[2] *U.S. Advanced Persistent Threat Analysis: Awareness, Response, and Readiness among Enterprise Organizations, Enterprise Strategy Group, October 2011*

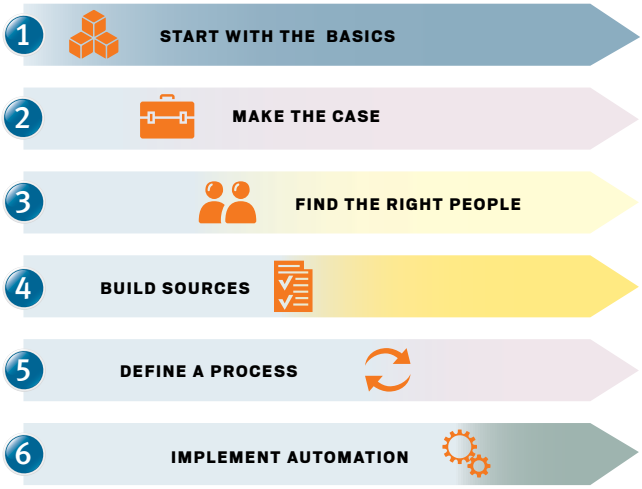
[3] *Western Europe Advanced Persistent Threat (APT) Survey, Enterprise Strategy Group, October 2011*

4 Roadmap to Intelligence-Driven Information Security

"If you're really serious about having an intelligence-driven program, you have to have the resources and a process for risk decision-making that enable rapid changes to your protection platform. You can have all the intelligence in the world, but if you're not going to do anything with it, don't go down this road because it's a lot of wasted effort."

ROLAND CLOUTIER
Vice President, Chief Security Officer, Automatic Data Processing, Inc.

The following roadmap lays out a basic route for developing an intelligence-driven approach to information security. While the exact route an organization takes will depend on its own unique circumstances, this roadmap offers some general direction and things to consider at various stages. The steps will likely be parallel endeavors but the focus of the program will move from one step to the next in sequence.



Step 1: Start with the Basics

Inventory of strategic assets

A fundamental requirement of intelligence-driven information security is to have an inventory of strategic assets since it will be impossible to collect data on everything and protect everything. Organizations need to know what are the most important assets to protect and where they are located. Over the past several years, many organizations have established an inventory of assets through a data-discovery process as part of their risk and compliance programs.

Incident-response process

Another requirement is a Security Operations Center (SOC) or Computer Emergency Response Team (CERT), either internally managed or run by a managed security services provider. To be ready to take on an intelligence program, the organization needs to have a foundation in place for monitoring the network for intrusions and a workflow process for responding to incidents. Ideally, this is a systematic process with well-defined roles.

Risk assessment

Organizations must also do a risk assessment. This involves determining the value of protected information assets, identifying potential sources of harm to those assets (threat assessment), determining the extent of existing vulnerabilities (vulnerability assessment), and evaluating the probability that the vulnerabilities could be successfully exploited and the potential impact to the organization. There are several good sources, including the National Institute for Science and Technology (NIST) and the SANS Institute, which provide detailed guidance on how to perform threat, vulnerability, and risk assessments.

Many organizations already routinely perform risk assessments as part of their security program. As the intelligence program progresses, there will be more data and better understanding which can be fed into ongoing risk assessments. But it is essential for an organization to begin with a basic understanding of the threats it faces and its risk posture.

"You need to align the intelligence process with your risk-management process. How the company identifies and measures risk needs to be understood and agreed to across the organization."

RALPH SALOMON
Vice President, IT Security & Risk Office, Global IT, SAP AG

Step 2: Make the Case

An essential component of developing an intelligence capability is communicating the benefits to executive management and key stakeholders in order to garner support and funding as well as to ensure ongoing enterprise-wide involvement in the effort. To be successful, intelligence-driven security must be an enterprise-wide core competency.

The value proposition

The main benefit is that the organization will be much better protected. By maximizing the use of available information, the organization can create and implement more precise defensive strategies against evolving threats.

Security will not only improve but also become more cost-effective because it will be targeted at countering the most significant threats and protecting the most strategic assets. Knowledge will enable the security team to perform fact-based prioritization. They will know how to concentrate their efforts and where to make the right investments in controls.

An intelligence-driven approach enables the security team to actually achieve proactive security management. By asking the right questions, combining multiple pieces of key external and internal data, looking at the bigger picture, and examining threats and vulnerabilities on a longer-term horizon, an intelligence-driven approach provides a view of more than single events or day-to-day incidents. It allows the team to see emerging attack patterns and developments over time, and eventually attain the necessary expertise to predict attacks and get ahead of the threats.

Key stakeholders

The communications strategy should not only convince key stakeholders of the benefits but also obtain their ongoing input to ensure success. Since intelligence-driven security is a new approach for many organizations, often it begins with developing a common language to use as the basis for discussions.

The list below suggests possible key stakeholders and how they might be involved in the intelligence effort:

- Executive Management and the Board
  Top-level support
  Risk decisions
- Finance
  Funding strategies
- Human Resources
  Employee-activity monitoring
- Corporate Security
  Collaborative data collection and investigations
- Procurement
  Third-party risk management
- Business/Mission Owners
  Identification of strategic assets and risks to business
- Production/Operations
  Identification of strategic assets and risks to manufacturing operations
- Business Risk Officers
  Enterprise view of risks

- Legal
  - Compliance to privacy regulations
  - Legal frameworks for obtaining threat data and sharing information with other organizations
  - Employee-activity monitoring
- IT
  - Programming, analytics, and automation
  - IT architecture and defensive strategies
  - IT operations for data sharing and service-level management

Opportunities for a "quick win"

Strategically, developing a fully deployed intelligence capability is going to be a multi-year effort. Typically, it makes sense for the security team to start small with the objective of quickly showing some good results. A "quick win" will help them gain the support and funding needed.

Since cyber attacks have recently received a lot of media attention, there is generally an elevated level of awareness among executive leaders and boards regarding the risks posed by advanced threats. Security teams can take advantage of this increased interest to propose cyber-risk intelligence projects as an integrated part of their security strategy. Leadership may be more open to providing the required funding and support than in the past. However, the proposed project must align to current top priorities and be able to deliver information that is specific and critical to the business. Information on vague, broad risks will not be useful.

More often than not, an intelligence-driven approach gets started because the security team seizes an opportunity. For example, a specific risk is identified as critical to the business and intelligence is proven to be very useful in mitigating that specific risk. Or a security incident occurs and intelligence is proven to be very useful in detecting the attack and/or reducing the risk of future incidents. Chart 6 provides some possible examples of opportunities, drawn from real-world experiences of Council members and their peers.

OPPORTUNITIES

6. EXAMPLES OF "QUICK WIN" OPPORTUNITIES TO SHOW VALUE

EXAMPLE OPPORTUNITY	PROJECT	RESULTS
Executives express concerns regarding hacktivism based on media reports. Many other organizations with a similar risk profile are being targeted by hacktivists and some have suffered shut-down of websites.	Data collection and analysis on this new class of threat: • A member of the incident-response team is assigned to do research on the likelihood of the company being targeted by hacktivists, impact, and how to defend against attacks • Based on research, specific adjustments made to DDoS defenses	Threat briefing to executives leads to support for more technology resources for threat analysis.
A critical component of the organization's business strategy depends on partnering with a new strategic partner.	Data collection and analysis on a potential business partner: • Short engagement with a threat-intelligence service to do research on potential threats to the business partner and the relationship • Based on research, specific recommendations are made regarding security requirements for doing business with the partner	Threat briefing to executives leads to support for more funding for threat-intelligence services
An insider incident involving systems containing IP leads to the awareness for increased protection of particular information assets.	Data collection and analysis on internal environment: • Security team requests assistance from business-intelligence team in developing baselines for end-user behavior in accessing a set of critical systems • Baselines established • Able to monitor activity on those systems for anomalies	Security team has support of organization to expand the number of systems for which to develop baselines of end-user behavior
A series of suspicious events leads to concern that certain systems have been compromised.	Use of external threat data • A short engagement with a threat-discovery service to monitor outgoing communications for signs of attack based on the vendor's attack-indicator database • A botnet is detected and remediated	Security team has support of organization to expand the number of systems for which to develop baselines of end-user behavior

PETRI KUIVALA
Chief Information Security Officer, Nokia

"In many organizations, improvements in security happen when there are incidents. It's human nature. Management will listen to the security team and agree to improvements at other times but they seem to get more interested and provide funding when there is an incident."

Step 3: Find the Right People

The skill set for cyber-risk intelligence professionals is quite different from the traditional skill set within the security department. Historically, security professionals required technical skills such as system administration or network administration skills, but cyber-risk intelligence teams require a different set of skills which are focused on determining how attack techniques might be used against the organization's IT infrastructure. It is a relatively senior role that also requires an ability to evaluate risks and make reasoned judgement calls.

Analytical skills and experience are crucial in order to look at what appear to be unrelated pieces of data to draw linkages, uncover patterns, see trends, and make predictions. Knowing how to construct and refine analytical models and work with other professionals such as programmers are also necessary skills, as well as specific expertise in network- and system-behavior analysis.

One of the most important aspects of the role is building and maintaining good relationships. Communication and writing skills are essential, such as being able to craft messages for various audiences. Other facets of the job will require skills in designing and managing processes, developing procedures, and implementing tools for the intelligence program.

Being inquisitive and investigative are useful traits for performing research. Depending on the organization's threat level and objectives for the program, there may be a need for people on the intelligence team who have the skills to do active research such as working in "underground" channels in order to collect intelligence on the adversaries. This could require specialized technical knowledge and skills in foreign languages and cultures. However, most organizations that decide to pursue detailed information on adversaries and their specific plots turn to threat-intelligence services.

The advantages are that the threat-intelligence services already have established methodologies for active research and have amassed a wealth of experience working with a wide spectrum of clients. The drawbacks are that the services can be costly for smaller organizations and an external service provider may not have a deep understanding of each individual organization's business. If an organization works with a threat-intelligence service, internal team members must be able to define the search parameters so that the service provider can deliver relevant information and also be able to put the information provided in context.

The title for the emerging role of cyber-risk intelligence professional is "analyst." Job descriptions vary depending on the goals and maturity of the program as well as the organizational structure. A sample job description for a "Cyber-Risk Intelligence Analyst" is provided in the sidebar on page 16.

This could be challenging for a single individual to accomplish. One approach is to have a multi-disciplinary team, combining people who have the various requisite skills. Many organizations do not have the resources to build a large dedicated team, especially in the early stages of an intelligence program. Instead, they might start by forming a virtual team by getting people from various departments to spend some time looking at security threats from different angles. Or, they might designate existing security resources, for example enlist senior members of the team to allocate time

"Cyber-risk intelligence requires a skill set combining abilities to understand threats, the business environment, and security controls in order to determine the risks to the business and what controls would mitigate those risks."

DAVE MARTIN
Chief Security Officer, EMC Corporation

to cyber-intelligence functions. Over time, the organization may dedicate full-time resources and/or hire people.

Finding the right people can be a challenge. Since cyber-risk intelligence is an emerging discipline, the skills are not widely available yet. But there are several good potential sources, including developing people from within the existing incident-response or forensics team or hiring professionals with a background in federal law enforcement, military intelligence, or banking-fraud analysis. Depending on the organizational structure, the cyber-risk intelligence team could reside within the information-security department or in an enterprise intelligence "fusion center," which includes other analysts working in areas such as physical security, supply chain, and competitive intelligence.

> *"Intelligence is all about relationships. Most companies have tons of information internally but it's not being shared. They have tons of information accessible through their service providers but they're not asking the right questions. You need people who can create trusted communication channels to leverage all of these sources."*

MARENE N. ALLISON
Worldwide Vice President of Information Security, Johnson & Johnson

JOB DESCRIPTION: CYBER-RISK INTELLIGENCE ANALYST

- Determining sources of intelligence
- Ensuring consistent and effective collection of data from those sources
- Doing research
- Consuming information such as reading bulletins, memos, and reports
- Performing tests on the IT environment to check for attack indicators or known techniques
- Implementing automated methods of consuming data
- Analyzing information
  - *Constructing and refining analytical models and running analytical tools*
  - *Developing threat scenarios*
- Writing and presenting threat briefings for various audiences (daily, weekly, and quarterly briefings)
- Developing relationships and networks of contacts
  - *Internal such as IT team and business lines*
  - *External such as law enforcement, information-sharing associations, and peers at other companies*
- Developing trusted communication channels
- Building an end-to-end intelligence process
- Working with other teams to act on the intelligence, such as improving detection or defensive strategies

Step 4: Build Sources

Good sources of cyber-risk data depend on what information is sought. Based on the current knowledge of threats and the organization's security posture against them, the cyber-risk intelligence team needs to determine what additional data would help prevent, detect, or predict attacks.

For instance, the team may decide to improve the collection of cyber-attack indicators from external sources to increase the likelihood of catching a potential problem. There may be a surge of spear-phishing emails affecting one of the business units and the team wants to know if and when other units get hit. They may see potential for an APT-style attack and want to know who could be targeting them.

Once information requirements are determined, the team can seek out good sources. Various types and key factors are presented in Charts 7-11. Finding good sources is an ongoing process – information requirements need to be reviewed, current sources assessed to determine if they meet requirements, and new sources researched and evaluated. As well, as data is collected and analyzed, sources may need to be adapted on-the-fly. Even trusted sources could get things wrong. Keep in mind that sources vary significantly in quality and scope. Some of the best sources may cost very little and some of the worst may cost a lot. The value of the data from each source should be tracked so that, over time, the team can judge how good particular sources are.

Evaluation criteria

The cyber-risk intelligence team should not only consider the attributes of the source but also the organization's ability to make use of the data from that source. Questions include:

- How trustworthy is the source?
  - Does the source provide consistent, reliable, accurate, trustworthy data?
  - Are we able to effectively collect and consume data from this source?
  - Is the data machine-readable or does it require human intervention?
  - If it is machine-readable, what format is it in and do we have the right tools in place to use it in an automated fashion? (For example, could we integrate the data with our Security Information and Event Management (SIEM) system?)
  - If it requires human intervention, do we have the right people to review it, analyze it, and/or use it to manually perform tests on our environment?
  - Do we have a data-management process that can ensure the confidentiality and integrity of the data and handle sensitive data (for example, if the source can't be quoted)?
- If the source is our internal IT infrastructure, do we have the right tools to capture or generate the right data?
  - Could we reconfigure logging or correlation rules to get the data we need? Or would we need additional tools to generate the required data?
- Do we have the time to invest in fostering the relationships that may be required to work with this source? (Internal or external sources often require relationships.)

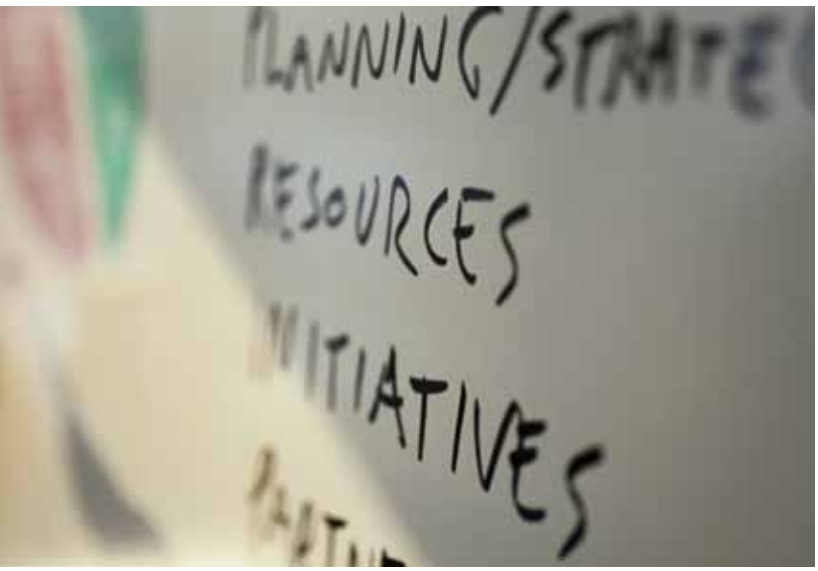
"If something happens at your organization, the first question you'll ask is, 'Is it just me or is everybody else getting hit with this attack?' You can't answer that for yourself. And it takes too long to call 20 of your closest friends. You've got to be part of a larger gene pool to get an immediate answer to that question."

RENEE GUTTMANN
Chief Information Security Officer,
The Coca-Cola Company

- What are the costs involved?
  - Are there up-front costs to receive the information? Is there a membership fee? Subscription-based fee? Service fee? Would it be a custom engagement?
  - How many personnel will it take to collect and make use of the data?
- If it's an information-sharing arrangement, are the required processes in place?
  - Do we trust that the data we provide to others will be handled with care, for example be kept confidential or de-identified if distributed?
  - Do we have a policy for determining what data will be shared with external entities and how?
  - Have we established the legal frameworks, rules of engagement, and/or agreements (NDA) for working with this source?
  - How much time and effort will it require to package up our data in order to share with external entities?
- Is the data provided by this source actionable?
  - Or is it too vague and broad to use?
- Is the data additive?
  - Does it provide corroborating information?
  - Or is it redundant data that we already obtain from another source?

> *Build your source material – whether from government or commercial sources, individuals in your organization, or business-intelligence processes. Your sources have to be broad enough to catch what might be disconnected elements of a common risk."*

DAVID KENT, Vice President, Global Risk and Business Resources, Genzyme



Relationships: the underpinning of good sources

Finding good sources is often predicated on building good relationships. Getting information requires having the right contacts who will share data based on trust. Relationships must be developed and maintained with colleagues throughout the organization, peers at other companies, law enforcement, government officials, and personnel from industry associations, in order to cultivate useful sources of intelligence.

The team needs to collect enough information to perform meaningful analysis but the goal is not to collect data on everything from everywhere. The team has to prioritize based on the threat model and information they are trying to protect, as well as the total costs of data collection and use. In addition, it should be recognized that often the team has to begin an analysis with incomplete information.

SOURCES OF CYBER-RISK DATA

7 GOVERNMENT SOURCES

Type of Source	Examples	Data Provided	Key Factors
Computer Emergency Response Agencies	• U.S.: U.S.- CERT • Europe: CERT-FI (Finland), DFN-CERT (Germany), GOVCERT.NL (Netherlands), GovCERT and CPNI (UK) • India: CERT-In • Global: FIRST • Australia: AusCERT	• Reports, advisories, and alerts on threats and vulnerabilities • Best practices and security tips • Attack indicators*	• Threat data is mainly non-automated via emails and web postings • Vulnerability data often in machine-readable formats • Some CERTs are membership-based
Federal Government Security Agencies	• U.S.: DHS, NSA • UK: GCHQ, Home Office • Germany: BSI • Australia: DSD	• Reports, advisories, and alerts on threats and vulnerabilities • Threat briefings • Attack indicators	• Publicly available data on the threats is mainly non-automated via web postings • Vulnerability data sometimes provided in machine-readable formats • Indicator databases starting to be available (DHS) • Classified data cannot be shared widely • Unclassified briefings provided to certain enterprises
Law Enforcement	• Local police: cyber-crime offices • National police such as: FBI/InfraGard (U.S.), SOCA (UK), BKA (Germany) • International: INTERPOL	• Cyber-crime reports • Data on attack techniques • Validation of criminal activity • Attack indicators	• For specific information (versus public reports) need to navigate through the system to find good contacts • Mostly non-automated data

**Attack indicators include: black-listed IP addresses, domain names, command and control servers, phishing sites, email addresses, file names, binaries, and malware signatures.*

8 INDUSTRY ASSOCIATIONS AND NETWORKS

Type of Source	Examples	Data Provided	Key Factors
Information-Sharing Associations	• U.S. sectorial: ISACs such as the FS-ISAC and IT-ISAC, and ES-ISAC • U.S. Energy: EnergySec • U.S. Defense Industrial Base: DCISE • U.S. public/private: ESF • Europe: ENISA • UK: WARPs, UKPA • Global IT industry: ICASI • Regional: PRISEM, ACSC • Vendor: RSA eFraudNetwork	• Reports, advisories, and alerts on threats and vulnerabilities • Best practices and security tips • Attack indicators	• Mainly non-automated data provided via emails and web postings • Some associations are moving towards providing some automated data feeds • Typically membership-based with range of fees
Informal Information-Sharing Groups	Informal networks of security professionals from a local area or a vertical industry	• Information on threats and vulnerabilities	• Mostly face-to-face meetings
Peers at Other Companies	Members of the security, incident-response, and/or intelligence teams	• Best practices and security tips • Validation of similar activity on their networks • Attack indicators	• Mainly non-automated data shared via personal contact, phone calls, and emails • Presentations at conferences
Security Researchers	Academic or industry-supported	• Vulnerability information • Potential threat scenarios • Defensive methods	• Mainly information provided through personal contact, networking events, and conferences

9 COMMERCIAL SOURCES

Threat Feeds	ZeusTracker, Bit9, SANS Internet Storm Center, Malware Domain List, Stopbadware, Team-Cymru, IPtrust.com, RSA AFCC	• Attack indicators	• Typically subscription fee-based or pay-per-view • Machine-readable data in various formats • Threat feeds are integrated with technology platforms such as threat-detection and security-intelligence systems
Threat-Intelligence Research Services	Cyveillance, iDefense, iSightPartners, RSA CyberCrime Intelligence Service, Mandiant	• Data on specific attackers and their techniques as well as investigations of compromise	• Various types of engagements • Delineate services to be provided via a statement of work

10 EXTENDED ENTERPRISE SOURCES

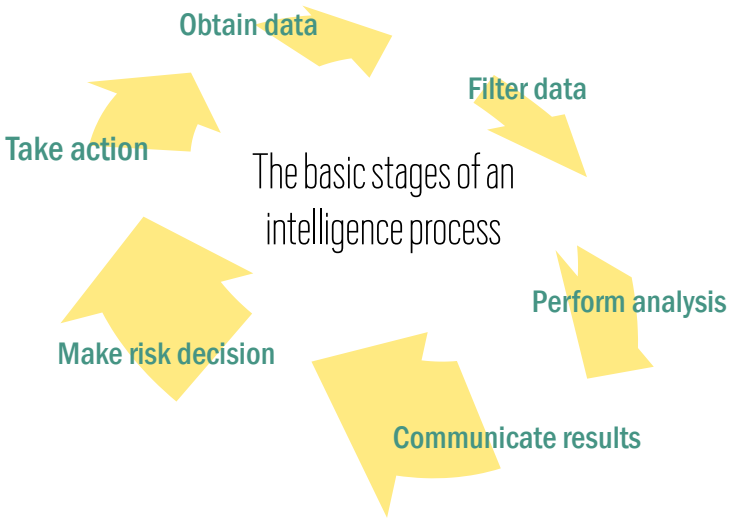
Business Partners	• Supply chain • Business-process outsourcers • Service providers	• Best practices and security tips • Validation of similar activity on their networks • Attack indicators	• Mainly non-automated data via personal contact, phone calls, and emails • Include information-sharing obligations in contract
Managed Security Service Providers	• AT&T • Verizon	• Validation of similar activity on other networks	• Include information-sharing obligations in contract

Type of Source	Examples	Data Provided	Key Factors
11 ORGANIZATION'S INTERNAL SOURCES			
Employees, Contractors	• Enterprise employees • Resident contractors	• Observations of suspicious activities and/or incidents	• Employee awareness required • Automated mechanism required for handling volumes of reporting • Hot line
Executives	Departments such as finance, corporate strategy, business lines	• Discussions regarding business strategies and associated risks	• Executive awareness required • Information-sharing working groups and/or forums
IT and Security Infrastructure	Business applications, GRC systems, SIEM systems, network-monitoring systems	• Logs, alerts, and reports	• Machine-readable data • Advanced analysis tools often used to amalgamate data from these sources, for example to baseline normal activity

Step 5: Define a Process

For designing a cyber-risk intelligence program, the goal is a standardized methodology that produces actionable intelligence and ensures an appropriate response. Given the nature of intelligence, the process will need to work on both a tactical and strategic timescale. Certain information such as precise, real-time attack indicators will call for immediate action while other information such as knowledge of protracted attack techniques will require longer-term defensive initiatives. Intelligence needs to inform not only day-to-day operations but also provide a more strategic outlook over a period of years.

The diagram below is an illustration of a basic process for collecting data, extracting meaning, making risk decisions, and taking action. It is set up as a feedback loop so as knowledge is gained, it's fed back into the system. For example, if an action is taken to modify security controls, data on the updated security posture becomes new input data.



The basic stages of a process can be described as follows:

- Obtain data
  - Input data from external and internal sources is collected and indexed.
- Filter data
  - Data that is irrelevant, not credible, or too vague is removed.
  - Irrelevant data could be exploits involving technologies not used or attacks targeting assets that are not owned by the organization.
  - Data that is judged not credible could be based on previous experience with that source providing unreliable data or on receiving conflicting data.
- Perform analysis
  - Various pieces of data are amalgamated, correlated, and studied to determine how they all relate.
  - Analysis is typically a mix of manual and automated techniques (from white-boarding to interactive analytics).
  - Analyses include an initial assessment of the risk and options for risk mitigation.
- Communicate results
  - Ideally, exigent risks are surfaced to an automated dashboard for immediate attention by the Security Operations Center (SOC). *For example, if the analysis finds evidence within the IT environment of outbound traffic to an adversary's command and control server.*

- For communicating the results of ongoing analyses, an effective method is a system of regular intelligence briefings to key stakeholders.
  For example, the results of analysis may include intelligence on the intent of adversaries, potential opportunities available to them, and/or the capabilities they may have to exploit the opportunities.
- Briefings can be provided to different audiences at various time intervals.
  For example, daily briefings to the security team, weekly briefings to IT, monthly briefings to an executive risk committee, and quarterly briefings to executive leadership.
- Besides regular briefings, out-of-band procedures for communicating high risks are also needed.
  For example, proof of an imminent attack affecting critical systems might be communicated right away versus indications of a possible future attack which would be included in a regular threat briefing.

→ Make risk decision

- Ideally, for exigent risks, a protocol has been set for the SOC to make a risk determination and take immediate action.
- For other critical risks, once they are identified and communicated by the intelligence team, depending on the risk, other stakeholders (such as IT, business/mission owners, risk officers, executives) may weigh in on the risk assessment and options for mitigation.
- A risk calculation is performed considering the potential impact to the organization versus the costs to mitigate the risk.
- A decision is made regarding actions to be taken for each specific risk.

→ Take action

- The action required will range from reconfiguring security tools to overhauling network architecture and implementing new security controls.
- A few examples of possible actions that could be taken in response to intelligence include:

  Change a firewall rule across the organization.

  Develop a new correlation rule for the SIEM.

  Rein-in access privileges for a set of critical assets.

  Segment the network to isolate certain critical assets.

  Implement encryption for certain critical business processes.

The cyber-intelligence team cannot work in isolation. The security-management process should delineate who is involved at every stage. For example, the team must have the right relationships across the organization to coordinate a response to the intelligence. It will require relationships with members of SOC, network operations, system administrators, and/or business lines, and so on. Certain situations may call for outside expertise such as malware forensics if not available in-house. Having a flexible protection platform is also essential for rapid response. For example, with a centralized management architecture, large-scale firewall changes could be made quickly across hundreds of control points.

Operational responsibility for information security is typically dispersed throughout an organization but center-led by the Chief Information Security Officer (CISO). Therefore, creating an effective cyber-risk intelligence process will require bridging between organizational and data-management silos. It may be possible to leverage existing systems for facilitating data flows. For example, some organizations have set up a common database for all information- and physical-security incidents and/or have built knowledge-management and workflow processes for an enterprise risk-management program. An intelligence program could piggy-back on these types of efforts. However new technologies may also be required.

"The process needs to be fast, fluid, and enable dynamic response – not be fixed, rigid, or stratified. If the goal is for the organization to outmaneuver cyber adversaries, the cyber-intelligence team can't get bogged down by bureaucracy."

WILLIAM BONI
Corporate Information Security Officer (CISO), VP Enterprise Information Security, T-Mobile USA

If you have intel on a threat which has not yet materialized into an attack, there may be a tendency to say, 'Well, it has not happened to us so far, why do we need to worry about it now?' Response prioritization becomes very important and at the same time very challenging when it's a prospective threat."

VISHAL SALVI
Chief Information Security Officer
and Senior Vice President,
HDFC Bank Limited

Step 6: Implement Automation

To facilitate the intelligence process, organizations should look at opportunities for automation. A cyber-risk intelligence program inherently involves "big data." For example, to keep up on current threats, an organization will probably be collecting cyber-attack indicators from as many reliable sources as possible. To gain insights into its entire IT environment, it will be amassing logs and full packet information from relevant systems and network devices across the organization.

The whole point of the intelligence effort is to correlate and analyze data from multiple sources in order to understand the threats and the organization's security posture against them. This program can easily accumulate vast amounts of data. It's simply not realistic to have humans handle all of it at every step. An effective program necessitates automation and planning the storage, analytic, and network architectures.

It is important to recognize, though, that implementing technology solutions does not equal developing an intelligence-analysis process. Automated systems make the large data sets manageable and accessible so that the analysts can more easily see relationships among disparate data types, identify connections, and notice patterns of activity forming; but they do not fulfill the requirements for the complete analysis.

Although there is no silver-bullet technology for a cyber-risk intelligence program, there are several technologies available today for automating elements of data collection, analysis, and management. There are four general areas in which leading organizations make technology investments for a cyber-risk intelligence program:

a. Automating the consumption of threat feeds

The format of cyber-attack indicators is sometimes a list of unstructured data. When it is delivered in a non-automated fashion, such as via email text or website posting, it has to be processed manually. For example, an analyst will enter it into a database to check the IT infrastructure for these signs of attack.

Fortunately, there are a growing number of government, industry-association, and commercial sources that provide automated threat feeds: machine-readable data such as comma-delimited ASCII. The technologies used to consume automated threat feeds are typically security information and event management (SIEM) systems, network-monitoring and forensics systems, and/or security-intelligence databases.

One of the challenges in working with automated threat feeds is that there is no standardization for how the content is organized. The order of data fields varies from one feed to the next. Therefore,

"You get a fire hose of information from potentially thousands of sources and need somewhere to put it – ideally a platform that enables fast searches in an un-normalised form, rapid analysis, and automated anomaly detection."

ROBERT RODGER,
Group Head of Infrastructure Security,
HSBC Holdings plc

"One of the biggest problems in the world of intelligence is that you quickly drown in data. You get masses of data, but you have to be able to derive knowledge from it, make it relevant and actionable – that takes good tools and better still excellent analysts."

PROFESSOR PAUL DOREY,
Founder and Director, CSO Confidential and
Former Chief Information Security Officer, BP

the data may need to be parsed before it is readable by a particular technology platform. However, there are aggregated threat-feed services that provide indicators from multiple sources, pre-process the data, and parse it into a consistent format.

Another way that organizations can integrate automated threat feeds into their current environment is by implementing technology platforms such as routers, anti-malware products, and adaptive-authentication solutions that automatically contain threat data.

b. Automating the collection of employee observations

Collecting information from thousands of employees across a large global enterprise is ultimately not feasible without some way to automate the process. If the intelligence team is interested in gathering data from employees on potential or actual incidents, reporting methods such as emails or phone calls to security simply do not scale. Increasingly, organizations implement knowledge-management systems for employees to report events to the intelligence team. These systems enable searching based on various parameters and can be customized to provide alerts. The main challenge will be getting employees to understand what events are to be reported and consistently use the system for reporting.

c. Automating log analysis and full packet capture

An area of focus for many cyber-risk intelligence programs is gaining visibility into the organization's own internal IT environment. Security-data analytics has emerged as an innovative approach modeled on business-intelligence systems, which process massive amounts of customer data to spot fraud or business opportunities. "Security intelligence" systems process data such as end-user behavior and system activity to spot cyber-attack indicators. The concept is to aggregate data logs and full packet data, such as application-access logs or network data that many organizations already routinely collect, then perform various functions such as baseline normal activity, discover anomalies, create alerts, develop trending, and even predict incidents.

d. Automating the fusion of data from multiple sources

Some organizations are taking an even bigger-picture view and amalgamating cyber-risk data from both internal and external sources into a "fusion center" or "security-data warehouse." The idea is to merge current data from the organization's IT and business environments with the latest information on threats into one large-scale analysis engine to achieve precise situational awareness.

The vision is a "big data" view of information security which will enable security teams to have real-time access to the entirety of information relevant to security risks. Advances in database technologies, data-storage systems, computing power, and analytics are helping organizations to realize this vision.

5 No Organization is an Island

Improving Information Sharing

"Sharing information is not the end state. The end state is to get actionable information that will help improve corporations' and governments' cyber-security posture and continually raise the bar."

WILLIAM PELGRIN, President & CEO, Center for Internet Security; Chair, Multi-State Information Sharing and Analysis Center (MS-ISAC); and Immediate Past Chair, National Council of ISACs (NCI)

Sharing cyber-risk intelligence and defensive strategies has become imperative in today's threat landscape. No organization can realistically sit in isolation and still be able to defend itself.

One of the most propitious aspects is the exchange of cyber-attack indicators. If large communities of organizations could readily and continuously exchange data on current attack methods, it would seriously impede attackers' operations. With an online early-warning system, organizations under attack could share attack profiles, so that others could prepare to defend themselves against similar (or even the very same) attacks.

Most information-security professionals have established informal networks of trusted contacts at other companies. Informal networks can be invaluable; they are often the most frequent way organizations share information. However, informal networks do not enable information sharing on a large scale.

For achieving large-scale exchange of information, there are a growing number of industry or government-led information-sharing initiatives as well as public/private partnerships. A few examples from various geographies are provided in the chart below.

12. EXAMPLES OF INFORMATION-SHARING INITIATIVES

Geography	Information sharing initiatives
International	• Forum of Incident Response and Security Teams (FIRST) • Industry Consortium for Advancement of Security on the Internet (ICASI)
National	• Computer Emergency Response Teams (CERTs) throughout Europe and Asia • Warning, Advice and Reporting Point (WARP) and CESG in the UK • Sectorial Information Sharing and Analysis Centers (ISACs), EnergySec, U.S.-CERT, Defense Industrial Base Collaborative Information Sharing Environment (DCISE), and Enduring Security Framework (ESF) in the U.S.
Regional	• Public Regional Information Security Event Management (PRISEM) in Washington • Advanced Cyber-Security Center (ACSC) in Massachusetts

"You have to invest time in being an active member of an external network. To fight threats requires data. Other companies need to be willing to share data with you."

DR. MARTIJN DEKKER
Senior Vice President, Chief Information Security Officer, ABN Amro

Models of operation and profiles of members vary, but all of these entities have similar information-sharing goals. Also, since some are relatively new – formed in the past few years – they continue to evolve. Some entities have already become effective channels for information exchange. Other entities have not yet reached a critical mass of participation by all members.

There are many challenges to creating information-sharing mechanisms. Participation is often hindered by a lack of resources. As well, the confidential nature of the information makes it tough to share. Organizations have good reasons not to want others to know how they are being targeted by cyber adversaries. Enterprises are restricted by legal issues, competitive considerations, and fears of reputation loss. Government agencies are restricted by classification requirements and national-security concerns.

Designing a way to deliver cyber-attack indicators is also enormously difficult. How does one create a system to distribute data that needs to be tightly held, yet shared with the broadest amount of people in the shortest amount of time in a form that they can immediately consume?

The good news is that, especially in the past couple of years, more organizations have started to participate and extend their contributions to information-sharing initiatives. It has often been individual companies which lead the way – deciding to make the "leap of faith" by being among the first to provide data and expecting others to follow, which spurs participation.

Groups such as the U.S. National Council of ISACs are also working to increase the number of organizations that participate, expand sector coverage, and improve cross-sector sharing. Governments in some parts of the world are actually starting to mandate participation including provisions for legal protections. For example, the government of India recently mandated participation in information exchange for the banking and critical-infrastructure sectors. There are also efforts underway to facilitate sharing mass amounts of data. Several information exchanges have pilot or production programs for providing data in machine-readable formats.

As information-sharing groups have gained experience, a set of criteria has emerged as the key ingredients for a successful exchange entity including:

- Trust among the participants
- Formalized structure (charter, board members, leadership, and professional staff)
- Adequate funding through government and/or membership fees
- Established protocol and clear rules for information sharing (what is to be shared with whom)
- Legal framework in which to share confidential information (NDA, government safe harbor)
- Standardized and reliable procedures for de-identifying confidential information to be distributed
- Streamlined mechanisms for submitting and distributing information (secure portal, encrypted email, and/or digitally signed machine-readable data)
- Genuine participation (through committed representatives and actual data contribution)

Trust and timeliness are essential components for information sharing. Within existing information-sharing groups, trust is still largely rooted in personal relationships, which does not create a sustainable system. Timeliness of information sharing continues to be a struggle as reliance is on particular individuals to post information in secure portals or securely email information. Automated data-exchange systems need to be established to remove the dependency on specific people. In addition, harmonized standards for representing attack information in machine-readable format, delivering it securely, and consuming it in real time would help to enable automation.

As cyber attacks continue to threaten enterprises and governments, more organizations will likely be motivated to invest in information sharing. An important factor paving the way is that organizations have the people, processes, and technologies in place to effectively participate in intelligence exchange.

6 Conclusion

The era of advanced threats calls for a new approach to information security. When dedicated cyber adversaries have the means and methods to elude commonly used defenses, such as signature-based detection, it is clear that conventional approaches are no longer sufficient. An intelligence-driven approach to information security can deliver comprehensive situational awareness, enabling organizations to more effectively detect and mitigate cyber attacks.

Developing a cyber-risk intelligence capability will take investments in people, process, and technology. It will challenge the information-security team to grow beyond the current skill set and to commit to a change in mind-set. And it will require not only the steadfast efforts of the security team but also broad organizational support.

The value proposition for a cyber-risk intelligence program includes improved security *and* cost-effectiveness. Defensive strategies can be precisely aimed at addressing the most significant threats and protecting the most critical assets. The security team will have the knowledge it needs to make informed risk decisions and invest in the right security controls.

Organizations must begin to recognize that having a cyber-risk intelligence capability is not just for the defense establishment and national-security agencies anymore. Government entities and corporate enterprises in many sectors must start to develop this capability in order to protect against growing threats to their operations and intellectual property.

Although many corporations have developed capabilities in competitive and market intelligence to understand their competitors and customers, most have not developed a cyber-risk intelligence program. Given that most business processes and transactions are now conducted in cyber space, activities such as fraud, espionage, and sabotage have also moved online. Cyber-risk intelligence has become a required competency to understand the online risks.

The guidance provided in this report is intended to help point the way forward. By harnessing the power of information, organizations can develop the knowledge they need to get ahead of advanced threats.

> *"If you know your attackers and what they might be capable of exploiting within your environment, you can demonstrate to your executive management that you're spending money on the right controls."*

DAVE CULLINANE,
Chief Information Security Officer and Vice President, Global Fraud, Risk & Security, eBay

7 Appendices

B *About the Security for Business Innovation Council Initiative*

Business innovation has reached the top of the agenda at most enterprises, as the C-suite strives to harness the power of globalization and technology to create new value and efficiencies. Yet there is still a missing link. Though business innovation is powered by information and IT systems, protecting information and IT systems is typically not considered strategic – even as enterprises face mounting regulatory pressures and escalating threats. In fact, information security is often an afterthought, tacked on at the end of a project or – even worse – not addressed at all. But without the right security strategy, business innovation could easily be stifled or put the organization at great risk.

AT RSA, WE BELIEVE THAT IF SECURITY TEAMS are true partners in the business-innovation process, they can help their organizations achieve unprecedented results. The time is ripe for a new approach; security must graduate from a technical specialty to a business strategy. While most security teams have recognized the need to better align security with business, many still struggle to translate this understanding into concrete plans of action. They know where they need to go, but are unsure how to get there. This is why RSA is working with some of the top security leaders in the world to drive an industry conversation to identify a way forward.

RSA HAS CONVENED A GROUP OF HIGHLY successful security executives from Global 1000 enterprises in a variety of industries which we call the "Security for Business Innovation Council." We are conducting a series of in-depth interviews with the Council, publishing their ideas in a series of reports, and sponsoring independent research that explores this topic. RSA invites you to join the conversation. Go to **www.rsa.com/securityforinnovation** to view the reports or access the research. Provide comments on the reports and contribute your own ideas. Together we can accelerate this critical industry transformation.

Security for Business Innovation Report Series

THE TIME IS NOW: Making Information Security Strategic to Business Innovation

MASTERING THE RISK/REWARD EQUATION: Optimizing Information Risks to Maximize Business Innovation Rewards

DRIVING FAST AND FORWARD: Managing Information Security for Strategic Advantage in a Tough Economy

CHARTING THE PATH: Enabling the "Hyper-Extended" Enterprise in the Face of Unprecedented Risk

BRIDGING THE CISO-CEO DIVIDE

THE RISE OF USER-DRIVEN IT: Re-calibrating Information Security for Choice Computing

THE NEW ERA OF COMPLIANCE: Raising the Bar for Organizations Worldwide

WHEN ADVANCED PERSISTENT THREATS GO MAINSTREAM: Building Information-Security Strategies to Combat Escalating Threats

BUSINESS INNOVATION DEFINED

Enterprise strategies to enter new markets, launch new products or services, create new business models, establish new channels or partnerships, or transform operations

Contributors

Top information-security leaders from Global 1000 enterprises

MARENE N. ALLISON,
Worldwide Vice President of Information Security, **JOHNSON & JOHNSON**

Prior to joining Johnson & Johnson, Marene was a senior security executive at Medco, Avaya, and the Great Atlantic and Pacific Tea Company. She served in the United States Army as a military police officer and as a special agent in the FBI. Marene is on the board of directors of the American Society of Industrial Security International (ASIS) and the Domestic Security Alliance Council (DSAC) and is President of West Point Women. She is a graduate of the U.S. Military Academy.

ANISH BHIMANI, CISSP, Chief Information Risk Officer, **JPMORGAN CHASE**

Anish has global responsibility for ensuring the security and resiliency of JPMorgan Chase's IT infrastructure and supports the firm's Corporate Risk Management program. Previously, he held senior roles at Booz Allen Hamilton, Global Integrity Corporation, and Predictive Systems. Anish was selected "Information Security Executive of the Year for 2008" by the Executive Alliance and named to Bank Technology News' "Top Innovators of 2008" list. He authored "Internet Security for Business" and is a graduate of Brown and Carnegie-Mellon Universities.

WILLIAM BONI, CISM, CPP, CISA, Corporate Information Security Officer (CISO), VP Enterprise Information Security, **T-MOBILE U.S.A.**

An information-protection specialist for 30 years, Bill joined T-Mobile in 2009. Previously, he was Corporate Security Officer of Motorola Asset Protection Services. Throughout his career, Bill has helped organizations design and implement cost-effective programs to protect both tangible and intangible assets. He pioneered the application of computer forensics and intrusion detection to deal with incidents directed against electronic business systems. Bill was awarded CSO Magazine's "Compass Award" and "Information Security Executive of the Year – Central" in 2007.

ROLAND CLOUTIER,
Vice President, Chief Security Officer, **AUTOMATIC DATA PROCESSING, INC.**

Roland has functional and operational responsibility for ADP's information, risk, crisis-management, and investigative-security operations worldwide. Previously, he was CSO at EMC and held executive positions with consulting and managed-services firms. He has significant experience in government and law-enforcement, having served in the U.S. Air Force during the Gulf War and later in federal law-enforcement agencies. Roland is a member of the High Tech Crime Investigations Association, the State Department Partnership for Critical Infrastructure Security, and Infragard.

DAVID KENT,
Vice President, Global Risk and Business Resources, **GENZYME**

David is responsible for the design and management of Genzyme's business-aligned global security program, which provides Physical, Information, IT, and Product Security along with Business Continuity and Crisis Management. Previously, he was with Bolt Beranek and Newman Inc. David has 25 years of experience aligning security with business goals. He received CSO Magazine's 2006 "Compass Award" for visionary leadership in the Security Field. David holds a Master's degree in Management and a Bachelor of Science in Criminal Justice.

PETRI KUIVALA,
Chief Information Security Officer, **NOKIA**

Petri has been CISO at Nokia since 2009. Previously, he led Corporate Security operations globally and prior to that in China. Since joining Nokia in 2001, he has also worked for Nokia's IT Application Development organization and on the Nokia Siemens Networks merger project. Before Nokia, Petri worked with the Helsinki Police department beginning in 1992 and was a founding member of the Helsinki Criminal Police IT- investigation department. He holds a degree in Master's of Law.

DAVE MARTIN, CISSP, Chief Security Officer, **EMC CORPORATION**

Dave is responsible for managing EMC's industry-leading Global Security Organization (GSO) focused on protecting the company's multibillion-dollar assets and revenue. Previously, he led EMC's Office of Information Security, responsible for protecting the global digital enterprise. Prior to joining EMC in 2004, Dave built and led security-consulting organizations focused on critical infrastructure, technology, banking, and healthcare verticals. He holds a B.S. in Manufacturing Systems Engineering from the University of Hertfordshire in the UK.

TIM McKNIGHT,
CISSP, Vice President and Chief Information Security Officer, **NORTHROP GRUMMAN**

Tim is responsible for Northrop Grumman's cyber-security strategy and vision, defining company-wide policies and delivering security to support the company. Tim received the Information Security Executive of the Year Mid-Atlantic Award and Information Security Magazine Security 7 Award in 2007. Tim has held management roles with BAE and Cisco Systems and served with the FBI. He has a Bachelor's degree and completed Executive Leadership training at the Wharton School. Tim also served as adjunct faculty at Georgetown University.

GUEST CONTRIBUTOR

WILLIAM PELGRIN, ESQ. President & CEO, Center for Internet Security (CIS); Chair, Multi-State Information Sharing and Analysis Center (MS-ISAC); and Immediate Past Chair, National Council of ISACs (NCI)

As President & CEO of CIS, Will provides leadership in establishing, implementing, and overseeing CIS's mission, goals, policies, and core principles. He is founder and Chair of MS-ISAC, which is the focal point for cyber-threat prevention, protection, response, and recovery for U.S. state, local, territorial, and tribal governments. He just finished serving his third term as chair of NCI, which works to advance the physical and cyber security of critical infrastructure and includes representation from major national industry sectors.

DAVE CULLINANE,
Chief Information Security Officer and Vice President, Global Fraud, Risk & Security, **eBay**

Dave has more than 30 years of security experience. Prior to joining eBay, Dave was the CISO for Washington Mutual and held leadership positions in security at nCipher, Sun Life, and Digital Equipment Corporation. Dave is involved with many industry associations including as current Past International President of ISSA. He has numerous awards including SC Magazine's Global Award as CSO of the Year for 2005 and CSO Magazine's 2006 Compass Award as a "Visionary Leader of the Security Profession."

DR. MARTIJN DEKKER,
Senior Vice President, Chief Information Security Officer, **ABN AMRO**

Martijn was appointed Chief Information Security Officer of ABN Amro in early 2010. Previously he held several positions in information security and IT including Head of Information Security and Head of Technology Risk Management in the Netherlands. Other positions included IT Architect, Program/Portfolio Manager, and IT Outsourcing/ Offshoring Specialist. Martijn joined ABN Amro in 1997 after completing his Ph.D. in Mathematics at the University of Amsterdam and a Master's of Mathematics at the University of Utrecht.

PROFESSOR PAUL DOREY,
Founder and Director, CSO Confidential and Former Chief Information Security Officer, **BP**

Paul is engaged in consultancy, training, and research to help vendors, end-user companies, and governments in developing their security strategies. Before founding CSO Confidential, Paul was responsible for IT Security and Information and Records Management at BP. Previously, he ran security and risk management at Morgan Grenfell and Barclays Bank. Paul was a founder of the Jericho Forum, is Chairman of the Institute of Information Security Professionals, and a Visiting Professor at Royal Holloway College, University of London.

RENEE GUTTMANN,
Chief Information Security Officer, **THE COCA-COLA COMPANY**

Renee is responsible for the information-risk-management program at The Coca-Cola Company. Previously, she was VP of Information Security and Privacy at Time Warner and Senior Director of Information Security at Time Inc. She has also held information-security roles at Capital One and Glaxo Wellcome and has been a security analyst at Gartner. Renee received the 2008 Compass Award from CSO Magazine and in 2007 was named a "Woman of Influence" by the Executive Women's Forum.

FELIX MOHAN,
Senior Vice President and Chief Information Security Officer, **AIRTEL**

At Airtel, Felix ensures that information security and IT align with changes to the risk environment and business needs. Previously, he was CEO at a security-consulting firm, an advisor with a Big-4 consulting firm, and head of IT and security in the Indian Navy. He was a member of India's National Task Force on Information Security, Co-chair of the Indo-U.S. Cybersecurity Forum, and awarded the Vishisht Seva Medal by the President of India for innovative work in Information Security.

ROBERT RODGER,
Group Head of Infrastructure Security, **HSBC HOLDINGS plc**

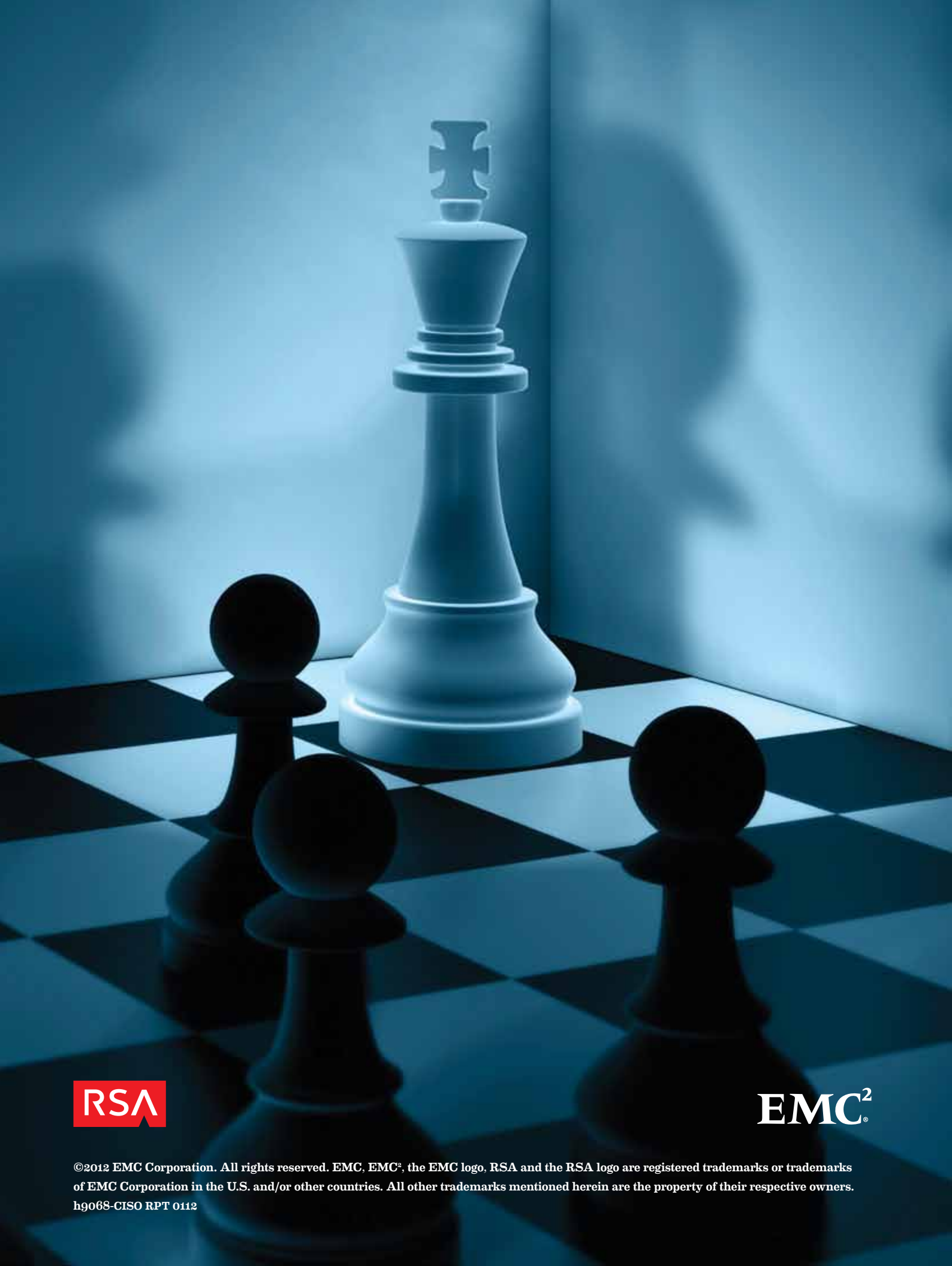
Bob has been with HSBC Bank since 2004. He is responsible for Infrastructure (IT) Security and IT Security Architecture for the Group. Previously, Bob was Head of IT Security at Bank of Bermuda and worked for the Bank of Scotland Group in IT Security consulting roles. He has over 16 years' experience in banking IT security, designing and implementing end-to-end security solutions for internal and external-facing applications. He holds a B.Sc.(Hons) in Information Technology with applied Risk Management.

RALPH SALOMON,
Vice President, IT Security & Risk Office, Global IT, **SAP AG**

Ralph is responsible for developing and maintaining the global IT security strategy and operational IT security at SAP worldwide. His many accomplishments include integration of Security, Quality, and Risk Management and improvements in IT Service and Business Continuity Management, which led SAP to achieve ISO 27001 certification and to become the first German company to be BS25999 certified. Prior to SAP, Ralph worked at KPMG as an IT Security, Quality, and Risk Management advisor and auditor.

VISHAL SALVI, CISM,
Chief Information Security Officer and Senior Vice President, **HDFC BANK LIMITED**

Vishal is responsible for driving the Information-Security strategy and its implementation across HDFC Bank and its subsidiaries. Prior to HDFC, he headed Global Operational Information Security for Standard Chartered Bank (SCB) where he also worked in IT Service Delivery, Governance, and Risk Management. Previously, Vishal worked at Crompton Greaves, Development Credit Bank, and Global Trust Bank. He holds a Bachelor's of Engineering degree in Computers and a Master's in Business Administration in Finance from NMIMS University.



h9068-CISO RPT 0112

MULTI-STATE Information Sharing & Analysis Center™

MS-ISAC Security Primer
Emergency Preparedness for Cyber Infrastructure

September 07, 2016, SP2016-0844

Overview: Disaster preparation should include protecting cyber assets. The Center for Internet Security (CIS) is providing the following recommendations to aid entities in protecting their cyber assets from physical harm during a natural disaster. Entities should give special attention to ensuring these special precautions are in place in advance of a predicted natural disaster such as a hurricane or blizzard.

TECHNICAL RECOMMENDATIONS:

- Run a full backup on all servers and test installing backups on a clean machine to ensure that reinstallation can occur. Store copies of all items necessary to perform fresh installations, such as backups, configuration files, cabling, media, serial numbers, and license keys at a secure, off-site location. If possible, store spare equipment at an off-site location.
- Test all emergency operations plans, especially plans that include equipment failure and relocation. Ensure that information technology staff are included in emergency preparations and are available for immediate response; do not assume that staff will have remote access capabilities. Ensure that all remote staff are informed of network changes during preparation.
- Know what cyber infrastructure is required for key tasks and where it is physically located. Cyber infrastructure may include communications infrastructure provided by a third party, and key databases and software for first responders, incident coordinators, and emergency managers.
- Consider the possible results of damage to structures, such as flooding and broken windows. If equipment can be moved permanently or in advance of a predicted event, do so; ideally sensitive equipment should be in an interior room, above ground level, away from windows, and off the floor.
- Ensure redundant infrastructure, including alternative power sources, is tested and operational. When possible, have surplus and back-up equipment, including power cords, cables, and fans for cooling a server room, stored in locations where they are easily accessible. If it is common to lose power, consider supplementing battery power with extended-life chargers and/or solar chargers.
- If there are single points-of-failure, such as communication towers/antennas or fiber paths along bridges/tunnels, consider response plans for repairing those crucial protection/recovery points.
- Review access control measures and restrictions to ensure that essential employees can still gain access to critical locations in the event of a power failure or if computer networks are offline.
- Have contingency plans in place in case of infrastructure failures and train users in how to complete essential tasks without telephones, Internet connectivity, and computers.
- Where possible, ensure all battery operated electronic devices are charged and unplugged.
- Encrypt or password protect all electronic devices in case of evacuation.
- If appropriate, have pre-established agreements with vendors to ensure replacement equipment and software is available on a priority basis, and through a line of credit, if needed.
- Ensure that up-to-date equipment insurance policies provide sufficient coverage.

Keep a hardcopy list of critical information, including:

- Emergency contacts and information for essential equipment/software/vendors and department employees, including special escalation procedures for natural disasters. Test the list regularly.
- Additional items necessary for a support call, such as contract numbers, support numbers, license keys and serial numbers, and exact configuration settings (hardware requirements, drive letters and sizes, patches, hot fixes, etc.) and restoration instructions.

TLP: WHITE *For more information regarding this cyber threat actor please contact the Multi-State Information Sharing and Analysis Center (MS-ISAC), 31 Tech Valley Drive, East Greenbush, NY 12064, 866-787-4722, SOC@cisecurity.org, www.cisecurity.org.*

Links to materials for further reading

State of Michigan: Cyber Disruption Response Plan
October 2015
https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf

State of Iowa: Cybersecurity Strategy
July 2016
https://ocio.iowa.gov/sites/default/files/documents/2016/08/2016_cybersec_document_web_version_2_final_0.pdf

State of the States on Cybersecurity
November 2015
http://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf

National Governors Association Issue Brief: Enhancing the Role of Fusion Centers in Cybersecurity
July 2015
https://www.nga.org/files/live/sites/NGA/files/pdf/2015/1507EnhancingTheRoleOfFusionCenters.pdf

National Association of Chief Information Officers of the States:
Cyber Disruption Response Planning Guide
April 2016
http://www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_CyberDisruption_072016.pdf

US Department of Homeland Security
Strategic Principles for Securing the Internet of Things
November 2016
https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

To access the information below, please double-click the PDF icon.

The CIS Critical Security Controls for Effective Cyber Defense August 2016

CSC-MASTER-VER61
-FINAL[1].pdf

Privacy Implications Guide for the CIS Critical Security Controls

Privacy Implications
Guide for the CIS Cr