Cyber Security: Threats, Targeting Methods and Best Practices

EWA Information & Infrastructure Technologies, Inc.

13873 Park Center Road – Suite 200
Herndon, VA 20171
703-478-7600
www.ewa-iit.com

Copyright © 2004-2013
# Table of Contents

Cyber Security: Threats, Targeting Methods and Best Practices ........................................ 1-15

Cyber Security: Legislation and Regulations .................................................................... 16-20

Executive Summary of Cyber Legislation ......................................................................... 21

Executive Order .................................................................................................................. 25

State Data Security/Breach Notification Laws .................................................................... 33

Articles .................................................................................................................................. 45
Cyber Security:
Threats, Targeting Methods and Best Practices
Cyber Security:
Threats, Targeting Methods and Best Practices

Information and Infrastructure Technologies, Inc.

- Top secret clearances: personnel and facilities
- IIT operates throughout U.S. and internationally
- EWA operates in 17 U.S. and foreign offices (e.g., Canada, Korea)

- Clients
  - Military: Department of Defense, National Guard
  - Intelligence Agencies: Department of Homeland Security
  - Government/Intelligence Agencies: Departments of State, Department of Homeland Security, USAID, Health and Human Services
  - Commercial: Passenger/freight railroads, major telecom equipment providers, financial, law firms

  - 2011 National Cyber Security Innovation Award
  - 2009 NSA Rowlatt Award for Organizational Achievement
  - Operate 3.24/7 Information Sharing & Analysis Centers
**Terminology**

- BotNet - a large number of compromised computers working together for malicious purposes
- Denial of Service Attack – targeting of a system or network causing a degradation or denial of access
- Malware – "malicious software" created to damage or illegally access a computer or network.
- Social Engineering - Manipulating people into performing actions or divulging confidential information
- Spoofing - email, instant message, or website address purporting to be something other than the true source
- Zero-Day - An attack that takes place immediately after a security vulnerability is announced
- Phishing – Malicious Email or Instant Messages
- Spearphishing – specifically tailored to an individual or company
- Whaling – Spearphishing that targets corporate senior executives
- Clone Phishing – Use of previously legitimate emails and attachments
- Drive-by Malware – Legitimate Website unknowingly infected
- Watering Hole – Targeted / themed drive-by attack

**Common Acronyms**

- Commercial-off-the-shelf (COTS)
- Department of Homeland Security (DHS)
- Distributed Denial-of-Service (DDoS)
- Fear, Uncertainty, Doubt or Death (FUD)
- Information Sharing and Analysis Center (ISAC)
- Internet Protocol address (IP)
- Information Technology (IT)
- National Cybersecurity And Communications Integration Center (NCCIC)
- National Institute of Standards and Technology (NIST)
- Operations Security (OPSEC)
- Personal Identifiable Information (PII)
- Tactics, Techniques and Procedures (TTP)
- United States Computer Emergency Readiness Team (US CERT)
Agenda

➤ Threats
  ➤ Target
  ➤ Actors and Goals
  ➤ Case studies

➤ Targeting Methods
  ➤ Phishing and Spear Phishing
  ➤ Drive-by
  ➤ Watering-Hole attacks
  ➤ Social Networking Sites
  ➤ Alternate vectors

➤ Best Practices
  ➤ User
  ➤ Organization

---

Target

YOU

➤ According to Help Net Security, 80 major law firms were hacked in 2011

➤ FBI's Mary Galligan, (SA Cyber Operations), states, “We have hundreds of law firms that we see increasingly being targeted by hackers.” LegalTech, February 2013, New York City

➤ “By targeting large law firms, hackers can obtain information about hundreds or thousands of companies by breaching a single network…to some extent, it’s a one-stop shop for the attackers.” Shane McGee – Mandiant

➤ “The hackers going after law firms often target companies that are negotiating a major international deal — anything from seeking a patent on a sensitive new technology to opening a plant in another country. The best documents to steal are in the law firm that represents that company.” Alan Paller, Director, SANS Institute via Associated Press Nov 2009

➤ “The list of those hacked in recent years includes law firms, think tanks, news organizations, human rights groups, contractors, congressional offices, embassies and federal agencies.” Washington Post – February 2013
Threat Actors and Goals

- Nation States
  - China, Russia
  - Cyber Espionage
  - Intelligence gathering/reconnaissance
  - Sabotage

- Criminals
  - Deny computer/network access for financial gain (ransomware, critical operations held hostage)
  - Theft of personal identity information, bank accounts

*Hackers see attorneys as a back door to the valuable data of their corporate clients.*

- "China-Based Hackers Target Law Firms to Get Secret Legal Data." Bloomberg News (January 2012)

Threat Actors and Goals

- Enthusiasts / Hacktivists
  - Bring network down (Degradation)
  - Defacement (Propaganda)
  - Denial of Service attacks
  - Sabotage

- Insider Threats
  - Disgruntled employee/retribution
  - Espionage
  - Financial gain

*"Law firms, think tanks, newspapers - if there's something of interest, you should assume you've been penetrated."*

- James A. Lewis, Center for Strategic and International Studies, Washington Post - February 2013
Nation States Case Studies

- September 2010: Seven Canadian law firms were targeted in a spear phishing campaign that was specifically designed to gather sensitive information regarding the acquisition of Potash Corp. of Saskatchewan Inc., a large supplier of crop fertilizer, by Australian based BHP Billiton Ltd. Both China and Russia vocally opposed the BHP bid.

- In 2010, Gibson Hoffman & Pancione received emails—ostensibly from members of the firm—designed to implant malware on their network most likely to steal data from their computers. The firm was representing a software company, CyberSitter, in a $2.2 billion lawsuit against the Chinese government and computer manufacturers.

  "Forensics investigators at Mandiant are working on twice as many targeted attacks by so-called advanced persistent threat (APT) adversaries against law firms than in years past, of the commercial victims Mandiant investigated during the past 18 months or so, 10 percent were law firms. And those are only the cases Mandiant sees. Its executives say many more go unnoticed by the victim organizations."
  - Dan Fanning, April 2013

Criminal Case Studies

- Law Firm's Trust Account Hacked: More Than Six Figures Stolen

  December 2012 – A Toronto-area law firm lost “a large six figure” over the holidays after malware planted on the firm’s accountants computer from a successful spear phishing campaign. They used the Trojan Banker virus that copied bank account passwords as the accountant typed them.

  "Lawyers, known to have large amounts of money in their trust accounts, are often targets of such scams."
  - Law Times, January 7, 2013
Criminal Case Studies

CardersMarket

*** USA 100% Approved Track2 Dumps ***

Selling USA 100% APPROVED TRACK2 DUMPS

Prices for approved dumps:
- 66 Visa Classic (debit)
- 67 Visa Classic (credit)
- 68 Visa Gold/Premium (debit)
- 69 Visa Gold/Premium (credit)
- 70 Visa Platinum
- 71 Visa Signature
- 72 Visa Business
- 73 American Express
- 74 MasterCard
- 75 MasterCard Gold
- 76 MasterCard Platinum

Each dump is sent in track2 format. Track1 and track3 isn't included.

Payment option: WBZ (websites) only!

Policy/Info:
- Minimum order is 10 dumps.
- Orders are filled within 24 hours after payment has been received.
- All dumps are checked for validity before sending. No replacements or refunds will be given.
- Dumps are hacked, not from skimming.

Contact:
- Tel: 897505
- Email: ntr@nolhes.org

Enthusiasts / Hacktivists

Case Studies

- STRATFOR: 4 Stage Attack by Anonymous
  - 5 million emails and subscriber financial data stolen
  - Distributed Denial of Service Attack
  - Spear phishing campaign targeting the subscribers
  - The public release of STRATFOR emails to WikiLeaks

- February 6, 2012 - The website belonging to Puckett & Faraj was defaced by the hackers to display a message from Anonymous, 2 gigabytes of confidential emails were stolen and posted on Internet sites. The website was later taken down for over a week. The law firm defended a U.S. Marine accused of civilian casualties in Iraq.

- September 2010: #Operation Payback Hacktivists operating under the Anonymous moniker targeted the lawyers of the "US Copyright Group" with Distributed Denial of Service (DDoS) Attacks. #Operation Payback hit ACS Law a second time, knocking out the site and stealing a 350MB archive of ACS Law confidential e-mails, posting them on Internet sites such as The Pirate Bay and Pastebin.
Insider Threat Case Studies

- June 2012 – A fired employee of a Pittsburgh law firm, 24-year-old Alyson Cunningham, with two accomplices, hacked into the firm’s servers and installed password stealing software on the network.

- June 2012, Matthew Kluger, a lawyer for several New York based law firms, was sentenced to twelve years in prison for stealing corporate merger information from four law firms over a 17 year period. Kluger stole the information from cases he was not involved with from the computer networks. The information was used to identify companies in merger negotiations and a large quantity of stock prior to the trade. Along with two other co conspirators, the trio netted $37 million in illicit profits.

- July 2008 – Terry Childs, a disgruntled computer engineer for the City of San Francisco Department of Technology, denied administrative access to the city’s Wide Area Network, where records such as officials’ e-mails, city payroll files, confidential law enforcement documents and jail inmates’ bookings are stored, by changing the passwords.

Targeting Methods

YOU

- Gmail
- LinkedIn
- Facebook
- Yahoo Mail
- Dropbox
Targeting Methods

- Phishing / Spear Phishing
- Drive-by malware
- Watering hole attack
- Social networking sites
- Alternate vectors

Phishing

From: Account Information <bankofamerica@yahoo.com>
Date: Sep 25, 2007 9:05 AM
Subject: Security Notice

Warning: This message may not be from whom it claims to be. Be aware of following any links in or of providing the sender with any personal information.

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons. We now need you to re-confirm your account information to us.

If this is not completed by September 27, 2007, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this matter.

To confirm your Online Banking records click on the following link:
http://192.168.1.100/secure/online_secure/

Thank you for your patience in this matter.

Bank of America Customer Service

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered.

© 2007 Bank of America Corporation. All rights reserved
Spear Phishing

- Number one targeting method
  - Highly researched content
  - Specifically tailored to deceive recipient
  - Malicious links and attachments

- Installation of malicious code
  - Monitor user activity
  - Keystroke loggers
  - Steal documents

*"The FBI assesses with high confidence that hackers are using spear phishing e-mails with malicious payloads to exploit U.S. law firms and public relations firms. During the course of ongoing investigations, the FBI identified noticeable increases in computer exploitation attempts against these entities."
- Dark Reading November 2009
Website Based Attacks

- Drive-By Attacks
  - Victim browses to a legitimate Web site that has been infected
  - Unknowingly downloads malware – with or without user interaction
  - iFrame injection: most commonly used infection vector
    - Used to embed content into Web pages
    - Naked to the eye
    - Zero by zero pixel

- Watering Hole Attack
  - Same exploit approach as Drive-By Attack
  - Targets specific user groups with like interests
  - The compromised website is now “waiting” to infect the profiled victim like a lion awaiting prey at the waterhole

Social Networking Sites

- Ripe Targeting Environment
- Facebook, for example:
  - Large, expanding user base
    - Over 1 billion users and growing
- LinkedIn
  - World’s largest professional network with 200 million members in 200 countries and territories around the globe
- Attractive environment for malicious activity
  - Perception of trusted environment
  - Networks assist in filtering targets
Social Networking Sites

- "Robin Sage"
  - Joined numerous social networking sites
  - 28 days later, hundreds of friends including people from NSA, DoD, and military intelligence
  - Received job offers and speaking invitations
  - Some information “friends” provided was sensitive
  - The purpose of social engineering is to gain trust and then gain access
  - Security researcher created fake profile - This person is not real
- Age 25
- PhD from MIT
- 10 years work experience with military intelligence
Alternate Vectors

- Personal e-mail
- Home computer
- Mobile devices (i.e. BlackBerry, iPhone)
- Gifts from strangers (i.e. USB drives)
- Hotel room intrusions

Personal E-Mail

- Gmail, Hotmail, Yahoo!, Outlook.com
  - 400% annual growth
- E-mail work to/from home
  - Creates security problems
  - Never auto-forward
  - Out of office reply
- Chat programs
  - Facebook, AOL, Gchat
Home Computers

- Protect your home computer
  - Antivirus

- Common Threats
  - Banking Trojans
  - Fake antivirus
  - Ransom Ware

Mobile Devices

- Apple/RIM/Android
- Voice and SMS - not encrypted
- Physical security
  - Maintain possession
- Password protection
- Wi-Fi hotspots
Electronic Gifts and Travel

- Strangers bearing gifts
  - Be cautious of receiving electronic devices [MP3 players, iPod] or media [DVD, CD]
  - USB Drives make popular gifts – also known to contain malware

- Finding electronic devices or media
  - Using found devices or media is not advised

- Hotel Room Security
  - Avoid leaving electronic devices behind
  - Safes are typically not “safe”
  - Encrypt devices such as laptops

User Best Practices

- Be alert for spear phishing

- Use strong and unique passwords

- Avoid using the same password for multiple logons

- Minimize online personal information

- Use only approved hardware and software on company owned systems

- Protect home computers
  - Anti-Virus
  - Personal E-mail accounts
  - Social networking sites

- Physical protection of mobile devices

*Cyber Security is the responsibility of everyone in your organization.*
Organization Best Practices

- User Awareness
  - An uneducated user is typically the weakest link
- Strong Password Policy
- Identify Core Assets "Crown Jewels"
- System Security Patches
  - IT Staff: Test and deploy patches in a timely manner
- Defense In-Depth
  - Anti-Virus, Firewall, Intrusion Detection System, Remote Intrusion Monitoring
- Email Filtering
  - Block attachments known to carry malware
  - Block email address spoofing attempts
- Web Filtering
  - Block undesired websites / content

- Access Controls
  - Normal User, Administrator
- Vulnerability Assessment / Penetration Testing
  - Initial and recurring
- Virtual Private Networks
- Encrypted Email services
  - ZIMMail
  - PGP
- Encrypt Hard Drives
  - Bitlocker
  - TrueCrypt
- Determine Constraints of Best Practices
  - Cost
  - Conducive to work environment
  - Stakeholder buy-in

Contact Information

- Eric Lindquist
  Director of Litigation Support Services
  elindquist@ewa.com
  703-478-7690

Cyber Security:
Legislation and Regulations
Cyber Security Legislation

“Businesses that do not define themselves as critical infrastructure may nevertheless be impacted by the executive order if their customers or affiliates include critical infrastructure.” - Holland & Knight Partners Law Firm

Do you have clients that fall under the definition of Critical Infrastructure and Key Resources (CIKR)?

- Food and Agriculture
- Commercial Facilities
- Dams
- Energy
- Information Technology
- Postal and Shipping
- Banking and Finance
- Communications
- Defense Industrial Base
- Government Facilities
- National Monuments and Icons
- Transportation Systems
- Chemical
- Critical Manufacturing
- Emergency Services
- Healthcare and Public Health
- Nuclear
- Water

Then the following legislation and executive orders concerning cyber security could impact you directly or indirectly if you fall victim to a cyber intrusion:

- White House Executive Order signed February 12, 2013
- H.R. 624 - The Cyber Intelligence Sharing and Protection Act (CISPA) Reintroduced February 12, 2013 – in Committee
- Individual State Data Breach Notification Legislation
White House Executive Order

White House Executive Order: “Improving Critical Infrastructure Cybersecurity,” signed on February 12, 2013:

- Directs the National Institute of Standards and Technology (NIST), in concert with DHS, to develop a voluntary cybersecurity framework, defining standards, methodologies, procedures, and processes for a prioritized, flexible, performance-based, and cost-effective approach to “help” critical infrastructure owners and operators to identify, assess, and manage cyber risk.
- The framework is required to be established within one year and must be updated “as necessary.”
- The framework “shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks” and “incorporate[s] voluntary consensus standards and industry best practices to the fullest extent possible.”
- Directs the Department of Justice, Department of Homeland Security (DHS), and Office of the Director of National Intelligence to establish programs and processes to expand the volume and enhance the quality of information shared on cyber threats, to expand sharing of security clearances to employees of critical infrastructure owners and operators,
- Directs DHS to identify critical infrastructure at “greatest risk” from a cybersecurity incident; to provide notification to private sector entities with assets and systems identified on the list; and to review the list for updating annually.

Sets the groundwork for future regulation:

- first, within 90 days of publication of the preliminary version of the Cybersecurity Framework (which is to occur within 240 days after issuance of the Executive Order), Federal security agencies are to report to the President on the status of their regulatory authorities to establish requirements based on the Framework; and
- if current regulatory requirements relating to cybersecurity are deemed insufficient, then within 90 days of issuance of the final Cybersecurity Framework (which is to occur within 1 year of issuance of the Executive Order), Federal agencies are to propose regulations to mandate cybersecurity and.

Proposed Congressional Legislation


- More than 50 statutes address various aspects of cybersecurity either directly or indirectly, but there is no overarching framework legislation in place.
- No major cybersecurity legislation has been enacted since 2002.
- Recent legislative proposals, including many bills introduced in the 111th and 112th Congresses, have focused largely on issues in 10 broad areas (Shown in Table 1)
Proposed Congressional Legislation

H.R. 624 - The Cyber Intelligence Sharing and Protection Act (CISPA) –
Reintroduced February 13, 2013; sponsored by Representatives Mike Rogers (R-MI) and C.A. “Dutch”
Ruppersberger (D-MD). Status: Referred to the House Committee on intelligence (Permanent Select). This
bill is scheduled for a closed session markup in the House Intelligence Committee on April 10,2013.

This legislation proposes the following:
- Establishes direct sharing of cyber security information from intelligence community to certified private
  entities that possess appropriate clearances.
- Inspector General oversight and report annually on type and use of information. Government liable for
  violating restrictions on FOIA, regulatory use, proprietary information, etc.
- Authorizes a cybersecurity provider (a non-governmental entity that provides goods or services intended
  to be used for cybersecurity purposes), with the express consent of a protected entity (an entity that
  contracts with a cybersecurity provider), to:
  - use cybersecurity systems to identify and obtain cyber threat information in order to protect the
    rights and property of the protected entity, and
  - share cyber threat information with any other entity designated by the protected entity, including the
    federal government.
- Cyber security information shared with the government will be protected from FOIA and regulatory use.
  Proprietary information also protected.

Proposed Congressional Legislation

[M1-13][introduced 3/13/2013] Referred to the House Committee on the Judiciary.

This legislation proposes the following:
- Amends the federal criminal code to provide criminal penalties for intentional failures to provide
  required notices of a security breach involving sensitive personally identifiable information.
- Defines “security breach” as a compromise of the security, confidentiality, or integrity of
  computerized data that there is reason to believe has resulted in improper access to sensitive
  personally identifiable information.
- Requires a person who owns or possesses data in electronic form containing a means of
  identification and who has knowledge of a major security breach of the system containing such
  data maintained by such person to provide prompt notice to the U.S. Secret Service or Federal
  Bureau of Investigation (FBI).
- Defines “major security breach” as any security breach involving: (1) means of identification
  pertaining to at least 10,000 individuals reasonably believed to have been acquired, (2) databases
  owned by the federal government, or (3) means of identification of federal employees or
  contractors involved in national security matters or law enforcement.
- Authorizes the Attorney General (DOJ) and any state attorney general to bring civil actions and
  obtain injunctive relief for violations of federal laws relating to data security.
Proposed Congressional Legislation

S.21 - "Cybersecurity and American Cyber Competitiveness Act of 2013 Introduced January 23, 2013 — Senate Commerce Committee Chairman Jay Rockefeller (D-WV), Senate Intelligence Committee Chairman Dianne Feinstein (D-CA), and Senate Homeland Security Committee Chairman Tom Carper (D-DE)"

This legislation proposes the following:
- enhancing the security and resiliency of public and private communications and information networks against cyber attack by nation-states, terrorists, and cyber criminals;
- establishing mechanisms for sharing cyber threat and vulnerability information between the government and the private sector;
- enhancing the security and resiliency of public and private communications and information networks against cyber attack by nation-states, terrorists, and cyber criminals; developing a coherent public/private system to improve the capability of the United States to assess cyber risk and prevent, detect, and robustly respond to cyber attacks against United States critical infrastructure;
- preventing and mitigating identity theft and guarding against abuses or breaches of personally identifiable information;
- preventing and mitigating identity theft and guarding against abuses or breaches of personally identifiable information enhancing United States diplomatic capacity and public-private international cooperation to respond to emerging cyber threats;
- expanding tools and resources for investigating and prosecuting cyber crimes in a manner that respects privacy rights and civil liberties and promotes United States innovation;
- maintaining robust protections of the privacy of United States citizens and their online activities and communications.

State Legislation

California Senate Bill 24 (SB-24)amends Cal. Civ. Code §§ 1798.29 and 1798.80 —

As of January 1, 2012, - owner or licensor of computerized data that includes personal information belonging to a California resident to notify that California resident in the event that his or her personal information is, or is reasonably believed to be, acquired by an unauthorized person.

Subject to very limited exceptions, any entity in possession of a California resident’s personal information that it does not own must, upon discovering a breach of the security of such personal information, notify the owner so that it may notify affected California residents.

48 states and the District of Columbia, Puerto Rico and the U.S. Virgin Islands enacted data privacy and breach notification laws that uses the California Civ. Code §§ 1798.29 and 1798.80 as a model.

- Alabama, Kentucky, New Mexico, and South Dakota do not have security breach notification laws.
State Legislation

Texas – As of September 2012, the amended Texas breach notification law went into effect, breach notification obligations will exist in all states since the Texas law will require entities doing business within the state to provide notification of data breaches to residents of states that have not enacted their own breach notification law.

Many states include an element of harm as a trigger for notification rather than simply unauthorized acquisition.

Penalties greatly vary in each state including:
- a civil penalty of up to $500, but not to exceed $50,000 for each state resident who was not notified;
- a civil penalty not to exceed $10,000 per breach;
- assessment of appropriate penalties and damages;
- $1,000 per day per breach, then up to $50,000 for each 30-day period up to 180 days not to exceed $500,000;
- $2,500 per violation and for any actual damages;

Contact Information

• Eric Lindquist
  Director of Litigation Support Services
  elindquist@ewa.com
  703-478-7690
Executive Summary of Cyber Legislation

White House Executive Order: “Improving Critical Infrastructure Cybersecurity,” signed on February 12, 2013:

- Defines critical infrastructure as systems or assets -- virtual and physical -- whose incapacity or destruction would have a debilitating effect on security, national economic security, or public health and safety.
- Directs the Department of Justice, Department of Homeland Security (DHS), and Office of the Director of National Intelligence to establish programs and processes to expand the volume and enhance the quality of information shared on cyber threats; to expedite granting of security clearances to employees of critical infrastructure owners and operators; and to integrate private sector subject matter experts into Federal service on a temporary basis to advise on the type of cyber threat information most useful to critical infrastructure owners and operators.
- Directs DHS to establish a consultative process to facilitate improvements to cybersecurity, with specific reference to the use of Sector Coordinating Councils (SCC) and the Critical Infrastructure Protection Advisory Council (CIPAC) process.
- Directs the National Institute of Standards and Technology (NIST), in concert with DHS, to develop a voluntary Cybersecurity Framework, defining standards, methodologies, procedures, and processes for a prioritized, flexible, performance-based, and cost effective approach to "help" critical infrastructure owners and operators to identify, assess, and manage cyber risk.
- Directs DHS to work with the Federal Sector Specific Agencies to support adoption of the Cybersecurity Framework by private sector entities; to incentivize participation in the program; and to report annually on the extent of private sector participation.
- Directs DHS to identify critical infrastructure at "greatest risk" from a cybersecurity incident; to provide notification to private sector entities with assets and systems identified on the list; and to review the list for updating annually.

SETS THE FOUNDATION FOR REGULATION: By calling upon Federal agencies with security responsibilities to take two categories of actions, essentially concurrently with development of the voluntary Cybersecurity Framework:

- first, within 90 days of publication of the preliminary version of the Cybersecurity Framework (which is to occur within 240 days after issuance of the Executive Order), Federal security agencies are to report to the President on the status of their regulatory authority to establish requirements based on the Framework; and
- if current regulatory requirements relating to cyber security are deemed insufficient, then within 90 days of issuance of the final Cybersecurity Framework (which is to occur within 1 year of issuance of the Executive Order), these same Federal agencies are to propose regulations to reduce cybersecurity risk.
House of Representatives and Senate Pending Legislation

H.R.624: Cyber Intelligence Sharing and Protection Act
Sponsor: Rep Rogers, Mike J. [MI-8] (introduced 2/13/2013)

Latest Major Action: 2/13/2013 Referred to House committee. Status: Referred to the House Committee on Intelligence (Permanent Select). This bill is scheduled for a closed session mark up in the House Intelligence Committee on April 10, 2013.

This legislation proposes the following:

- Defines "cyber threat intelligence" as intelligence in the possession of an element of the intelligence community directly pertaining to:
  - a vulnerability of a system or network of a government or private entity;
  - a threat to the integrity, confidentiality, or availability of such a system or network or any information stored on, processed on, or transiting such a system or network;
  - efforts to deny access to or degrade, disrupt, or destroy such a system or network; or
  - efforts to gain unauthorized access to such a system or network, including for the purpose of exfiltrating information.

- Requires the procedures established to ensure that such intelligence is only:
  - shared with certified entities or a person with an appropriate security clearance,
  - shared consistent with the need to protect U.S. national security, and
  - used in a manner that protects such intelligence from unauthorized disclosure.

- Authorizes a cybersecurity provider (a non-governmental entity that provides goods or services intended to be used for cybersecurity purposes), with the express consent of a protected entity (an entity that contracts with a cybersecurity provider), to:
  - use cybersecurity systems to identify and obtain cyber threat information in order to protect the rights and property of the protected entity; and
  - share cyber threat information with any other entity designated by the protected entity, including the federal government.

H.R.1121: Cyber Privacy Fortification Act of 2013

Latest Major Action: 3/13/2013 Referred to House committee. Status: Referred to the House Committee on the Judiciary.

- Amends the federal criminal code to provide criminal penalties for intentional failures to provide required notices of a security breach involving sensitive personally identifiable information. Defines "sensitive personally identifiable information" to mean specified electronic or digital information.
- Defines "security breach" as a compromise of the security, confidentiality, or integrity of computerized data that there is reason to believe has resulted in improper access to sensitive personally identifiable information.
• Requires a person who owns or possesses data in electronic form containing a means of identification and who has knowledge of a major security breach of the system containing such data maintained by such person to provide prompt notice to the U.S. Secret Service or Federal Bureau of Investigation.
• Defines "major security breach" as any security breach involving: (1) means of identification pertaining to at least 10,000 individuals reasonably believed to have been acquired, (2) databases owned by the federal government, or (3) means of identification of federal employees or contractors involved in national security matters or law enforcement.
• Authorizes the Attorney General (DOJ) and any state attorney general to bring civil actions and obtain injunctive relief for violations of federal laws relating to data security.
• Requires federal agencies as part of their rulemaking process to prepare and make available to the public privacy impact assessments that describe the impact of certain proposed and final agency rules on the privacy of individuals.
• Sets forth authority for agencies to waive or delay certain privacy impact assessment requirements for emergencies and national security reasons.
• Directs federal agencies to periodically review promulgated rules that have a significant privacy impact on individuals or a privacy impact on a substantial number of individuals. Requires agencies to consider whether each such rule can be amended or rescinded in a manner that minimizes any such impact while remaining in accordance with applicable statutes.
• Provides access to judicial review to individuals adversely affected or aggrieved by final agency action on any such rule.

S.21 : Cybersecurity and American Cyber Competitiveness Act of 2013
Sponsor: Sen Rockefeller, John D., IV [WV] (introduced 1/22/2013)
Latest Major Action: 1/22/2013 Referred to Senate committee. Status: Read twice and referred to the Committee on Homeland Security and Governmental Affairs.

• Calls for the enactment of bipartisan legislation to improve communication and collaboration between the private sector and the federal government to secure the United States against cyber attack, enhance the competitiveness of the United States and create jobs in the information technology industry, and protect the identities and sensitive information of U.S. citizens and businesses by:
  o enhancing the security and resiliency of public and private communications and information networks against cyber attack;
  o establishing mechanisms for sharing cyber threat and vulnerability information between the government and the private sector;
  o developing a public-private system to improve the capability of the United States to assess cyber risk and prevent, detect, and respond to cyber attacks against critical infrastructure such as the electric grid, the financial sector, and telecommunications networks;
  o promoting research and development investments and professional training; (5) preventing and mitigating identity theft;
- enhancing U.S. diplomatic capacity and public-private international cooperation to respond to emerging cyber threats;
- expanding resources for investigating and prosecuting cyber crimes in a manner that respects privacy rights and civil liberties and promotes U.S. innovation; and
- maintaining robust protections of the privacy of U.S. citizens and their online activities and communications.
Executive Order

THE WHITE HOUSE
Office of the Press Secretary

EMBARGOED UNTIL DELIVERY OF THE PRESIDENT'S STATE OF THE UNION ADDRESS February 12, 2013

EXECUTIVE ORDER

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Sec. 3. Policy Coordination. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive-1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of
section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 16, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties
risks of the functions and programs undertaken by DHS as called
for in this order and shall recommend to the Secretary ways to
minimize or mitigate such risks, in a publicly available report,
to be released within 1 year of the date of this order. Senior
agency privacy and civil liberties officials for other agencies
engaged in activities under this order shall conduct assessments
of their agency activities and provide those assessments to DHS
for consideration and inclusion in the report. The report shall
be reviewed on an annual basis and revised as necessary. The
report may contain a classified annex if necessary. Assessments
shall include evaluation of activities against the Fair
Information Practice Principles and other applicable privacy and
civil liberties policies, principles, and frameworks. Agencies
shall consider the assessments and recommendations of the report
in implementing privacy and civil liberties protections
for agency activities.

(b) In producing the report required under subsection (b)
of this section, the Chief Privacy Officer and the Officer for
Civil Rights and Civil Liberties of DHS shall consult with the
Privacy and Civil Liberties Oversight Board and coordinate with
the Office of Management and Budget (OMB).

(c) Information submitted voluntarily in accordance with
6 U.S.C. 133 by private entities under this order shall be
protected from disclosure to the fullest extent permitted by
law.

Sec. 6. Consultative Process. The Secretary shall
establish a consultative process to coordinate improvements to
the cybersecurity of critical infrastructure. As part of the
consultative process, the Secretary shall engage and consider
the advice, on matters set forth in this order, of the Critical
Infrastructure Partnership Advisory Council; Sector Coordinating
Councils; critical infrastructure owners and operators; Sector-
Specific Agencies; other relevant agencies; independent
regulatory agencies; State, local, territorial, and tribal
governments; universities; and outside experts.

Sec. 7. Baseline Framework to Reduce Cyber Risk to
Critical Infrastructure. (a) The Secretary of Commerce shall
direct the Director of the National Institute of Standards and
Technology (the "Director") to lead the development of a
framework to reduce cyber risks to critical infrastructure (the
"Cybersecurity Framework"). The Cybersecurity Framework shall
include a set of standards, methodologies, procedures, and
processes that align policy, business, and technological
approaches to address cyber risks. The Cybersecurity Framework
shall incorporate voluntary consensus standards and industry
best practices to the fullest extent possible. The
Cybersecurity Framework shall be consistent with voluntary
international standards when such international standards will
advance the objectives of this order, and shall meet the
requirements of the National Institute of Standards and
Technology Act, as amended (15 U.S.C. 271 et seq.), the National
Technology Transfer and Advancement Act of 1995 (Public Law 104-
113), and OMB Circular A-119, as revised.

(b) The Cybersecurity Framework shall provide a
prioritized, flexible, repeatable, performance-based, and
cost-effective approach, including information security measures
and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the "preliminary Framework"). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the "final Framework").

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").
[b] Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

c. Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

d. The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

e. Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

Sec. 9. Identification of Critical Infrastructure at Greatest Risk. (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant
stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

Sec. 10. Adoption of Framework. (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12666 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 14, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13605 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13605 of May 10, 2012 (Identifying and Reducing Regulatory Burden), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are
encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies, and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. Definitions. (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) "Critical Infrastructure Partnership Advisory Council" means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) "Independent regulatory agency" has the meaning given in 44 U.S.C. 3502(5).

(e) "Sector Coordinating Council" means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) "Sector-Specific Agency" has the meaning given the term in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

Sec. 12. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at
law or in equity by any party against the United States, its
departments, agencies, or entities, its officers, employees, or
agents, or any other person.

BARACK OBAMA

THE WHITE HOUSE,
February 12, 2013.

###
# State Data Security/Breach Notification Laws

*(As of December 2011)*

<table>
<thead>
<tr>
<th>State</th>
<th>Legislative Reference</th>
<th>Statute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Effective Date</strong></td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>No data security/breach notification law.</td>
<td></td>
</tr>
<tr>
<td>Alaska</td>
<td>HB 6</td>
<td>Alaska Stat. §45.48.010</td>
</tr>
<tr>
<td><strong>Effective Date</strong></td>
<td>7/1/2009</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Relating to breaches of security involving personal information (&quot;PI&quot;).</td>
<td></td>
</tr>
<tr>
<td><strong>Effective Date</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Requires businesses to provide consumer notification of data breaches.</td>
<td></td>
</tr>
<tr>
<td><strong>Effective Date</strong></td>
<td>3/31/2005</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Encourage those that acquire, own, or license PI to provide reasonable security for the info.</td>
<td></td>
</tr>
<tr>
<td>California</td>
<td>1) AB 700 SB 1386 (amended by SB 24) 2) AB 2886</td>
<td>1) Cal. Civ. Code §§1798.29 (agency) and 82 (person or business) 2) Cal. Penal Code §§530.5 and 530.55</td>
</tr>
<tr>
<td><strong>Effective Dates</strong></td>
<td>1) 1/1/2012 2) 1/1/2007</td>
<td></td>
</tr>
<tr>
<td><strong>Descriptions</strong></td>
<td>Protect against unauthorized access of computerized data compromising the security, integrity, or confidentiality of PI. 2) Increases penalties for identity theft crimes.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Legislative Reference</td>
<td>Statute</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Colorado</td>
<td>HB 1119</td>
<td>Col. Rev. Stat. §6-1-716</td>
</tr>
<tr>
<td>Effective Date</td>
<td>9/1/2006</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Requires businesses to provide consumer notification of data breaches.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) HB 5658</td>
<td>(Public Act No. 05-14)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Public Act No. 08-167)</td>
</tr>
<tr>
<td>Effective Dates</td>
<td>1) 1/1/2006</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) 10/1/2008</td>
<td></td>
</tr>
<tr>
<td>Descriptions</td>
<td>1) A business must disclose security breach involving PI to affected consumers, without unreasonable delay.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) Protects against intentional failure to safeguard PI.</td>
<td></td>
</tr>
<tr>
<td>Delaware</td>
<td>HB 116</td>
<td>Del. Code Ann. tit. 6, §§12B-101 to 104</td>
</tr>
<tr>
<td>Effective Date</td>
<td>6/28/2005</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Protects PI by encouraging data brokers to provide reasonable security for PI.</td>
<td></td>
</tr>
<tr>
<td>Florida</td>
<td>HB 481</td>
<td>Fla. Stat. ch. 817.5681</td>
</tr>
<tr>
<td>Effective Date</td>
<td>7/1/2005</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Businesses maintaining computerized data including PI must provide notice of security system breach in certain circumstances.</td>
<td></td>
</tr>
<tr>
<td>Effective Date</td>
<td>5/5/2005</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Requires expeditious notification of unauthorized acquisition and possible misuse of PI.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Legislative Reference</td>
<td>Statute</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Hawaii</td>
<td>SB 2290</td>
<td>Haw. Rev. Stat. §487N-1 to 487N-7</td>
</tr>
<tr>
<td><strong>Effective Dates</strong></td>
<td></td>
<td>7/1/2008 (HRS §487N-1, 5-7) 4/17/2008 (§487N-2) 1/1/2007 (§487N-3, 4)</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td>Alleviate identity theft by requiring businesses to notify an individual, whenever the individual's PI has been compromised by unauthorized disclosure.</td>
</tr>
</tbody>
</table>
| Idaho  | 1) SB 1374  
2) HB 566 | 1) Idaho Code §§28-51-104 to 107  
2) Idaho Code §§28-51-105 |
| **Effective Dates** | | 1) 7/1/2006  
2) 7/1/2010 |
| **Descriptions** | | 1) To provide for disclosure of breach of security of computerized PI by an agency, individual or a commercial entity.  
2) Requires notification of state attorney general of data breach. |
<p>| Illinois | HB 1633 (amended by HB 3025) | 815 Ill. Comp. Stat. §§530/1 to 530/30 |
| <strong>Effective Date</strong> | | 1/1/2012 |
| <strong>Description</strong> | | Data collector must provide notification of security breach after discovery, even if data has not been accessed by unauthorized person. |</p>
<table>
<thead>
<tr>
<th>State</th>
<th>Legislative Reference</th>
<th>Statute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indiana</td>
<td>1) HB 1101</td>
<td>1) Ind. Code §24-4.9</td>
</tr>
<tr>
<td></td>
<td>2) HB 1197</td>
<td>2) Ind. Code §24-4.9-2-2</td>
</tr>
<tr>
<td></td>
<td>3) HB 1121</td>
<td>3) Ind. Code §24-5-26 et seq.</td>
</tr>
<tr>
<td>Effective Dates</td>
<td>1) 7/1/2006 (revisions effective 7/1/2009)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) 7/1/2008</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3) 7/1/2009</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>1) Requires disclosure of data breach if data base owner knows, should know, or should have known the breach resulted in or could result in ID deception, etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) Revised def. of security breach so that breach occurs if encryption key has been compromised.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3) Provide protection to consumers affected by ID theft.</td>
<td></td>
</tr>
<tr>
<td>Iowa</td>
<td>SF 2308</td>
<td>Iowa Code §§715C.1 et seq.</td>
</tr>
<tr>
<td>Effective Date</td>
<td>7/1/2008</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>A bill for an act relating to ID theft by providing for the notification of a security breach of PI; requesting the establishment of an interim study committee relating to disclosure of PI; and providing penalties.</td>
<td></td>
</tr>
<tr>
<td>Kansas</td>
<td>SB 196</td>
<td>Kan. St. Ann. §50-7a01 to 4</td>
</tr>
<tr>
<td>Effective Date</td>
<td>7/1/2006</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Requires businesses to provide consumer notification of data breaches.</td>
<td></td>
</tr>
<tr>
<td>Kentucky</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Effective Date</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>No data security/breach notification law.</td>
<td></td>
</tr>
<tr>
<td>Effective Date</td>
<td>1/1/2006</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Requires rapid notification of possible misuse of a PI to help minimize and counter costs of ID theft.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Legislative Reference</td>
<td>Statute</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td>--------------------------------------------------</td>
</tr>
</tbody>
</table>
| Maine        | 1) LD 1671 (LD 2017 revises 1671)  
2) Same            |
| Effective Dates | 1) 1/31/2006 (with revisions effective 1/31/2007)  
2) 9/12/2009       |
| Descriptions | 1) A business that owns or licenses electronic data containing PI, must inform those affected by breach following the discovery of the breach.  
2) Same            |
<p>| Maryland     | SB 194                | Md. Code Ann., Commercial Law §§14-3501 to 3508 |
| Effective Date | 1/1/2008               |
| Description  | To require businesses that own, license, or maintain computerized data that includes PI to conduct an investigation and notify persons of a breach of the security of a system. |
| Massachusetts | HB 4144               | Mass. Gen. Laws ch. 93H, §1 to 6                 |
| Effective Date | 10/31/2007             |
| Description  | To safeguard PI of residents and provide safeguards for protection of PI. Requires disclosure of data breach if data base owner knows or has reason to know of a Security Breach. |
| Effective Date | 6/29/2007             |
| Description  | To prohibit certain acts and practices concerning ID theft; to require notification of a security breach of a database that contains certain PI. |
| Minnesota    | HF 2121               | Minn. Stat. §325E.61 and 64                      |
| Effective Date | 1/1/2006              |
| Description  | Requires business possessing PI to notify those whose PI has been disclosed to unauthorized persons. |</p>
<table>
<thead>
<tr>
<th>State</th>
<th>Legislative Reference</th>
<th>Statute</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mississippi</strong></td>
<td>HB 583</td>
<td>Miss. Code Ann. §---</td>
</tr>
<tr>
<td><strong>Effective Date</strong></td>
<td>7/1/2011</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Includes a risk of harm trigger for when businesses must notify state residents of a breach of their unencrypted PI.</td>
<td></td>
</tr>
<tr>
<td><strong>Missouri</strong></td>
<td>HB 62</td>
<td>Mo. Rev. Stat. §407.1500</td>
</tr>
<tr>
<td><strong>Effective Date</strong></td>
<td>8/28/2009</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Requires notification of affected consumers that there has been a security breach following the discovery or notification of the breach.</td>
<td></td>
</tr>
<tr>
<td><strong>Montana</strong></td>
<td>1) HB 732</td>
<td>1) Mont. Code Ann. §30-14-1701 et seq.</td>
</tr>
<tr>
<td></td>
<td>2) HB 155</td>
<td>2) Mont. Code Ann. §2-6-501 et seq.</td>
</tr>
<tr>
<td><strong>Effective Dates</strong></td>
<td>1) 3/1/2006</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) 10/1/2009</td>
<td></td>
</tr>
<tr>
<td><strong>Descriptions</strong></td>
<td>1) Purpose is to enhance the protection of individual privacy and to impede identity theft.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) Require state agencies to develop procedures to protect personal information.</td>
<td></td>
</tr>
<tr>
<td><strong>Nebraska</strong></td>
<td>LB 876</td>
<td>Neb. Rev. Stat. §§87-801 to 807</td>
</tr>
<tr>
<td><strong>Effective Date</strong></td>
<td>7/14/2006</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enhance the protection of individual privacy and to impede identity theft.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Legislative Reference</td>
<td>Statute</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Nevada**          | 1) SB 347  
2) SB 82    | 1) Nev. Rev. Stat. §§205.461 to 4657 and §§603A.010 to 920  
| **Effective Dates** | 1) 10/1/2005, 1/1/2006, or 1/1/2008, 1/1/2010 depending on provision, 10/1/2011  
2) 7/1/2011    |                                                              |
| **Descriptions**    | 1) Requires data collectors to provide notification concerning any breach of security involving system data and protects personal identifying information.  
2) Requires the Chief of the Office of Info Security of the Department of IT to investigate and resolve matters relating to security breaches of info systems of state agencies and elected officers |
<p>| <strong>Effective Date</strong>  | 1/1/2007              |                                                              |
| <strong>Description</strong>     | Requires a person engaged in business in NH to notify consumers of any security breach that compromises the confidentiality of PI. |
| <strong>Effective Date</strong>  | 1/1/2006 (except for police reports, then effective 9/22/2005) |                                                              |
| <strong>Description</strong>     | Business or public entity compiling/maintaining computerized data with PI must disclose security breach if PI was/is reasonably believed to be acquired by unauthorized person. |
| <strong>New Mexico</strong>      | N/A                   | N/A                                                          |
| <strong>Effective Date</strong>  | N/A                   |                                                              |
| <strong>Description</strong>     | No data security/breach notification law.                     |</p>
<table>
<thead>
<tr>
<th>State</th>
<th>Legislative Reference</th>
<th>Statute</th>
</tr>
</thead>
<tbody>
<tr>
<td>New York</td>
<td>AB 4254</td>
<td>N.Y. St. Tech. Law §208 (apply to state agencies) and N.Y. Gen. Bus. Law, §899-aa (apply to business)</td>
</tr>
<tr>
<td>Effective Date</td>
<td>12/7/2005</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>Guarantees persons the right to know what info was exposed during a breach, so that they can take the necessary steps to both prevent and repair any damage incurred.</td>
</tr>
<tr>
<td>North Carolina</td>
<td>1) SB 1048</td>
<td>1) N.C. Gen. Stat. §14-113.20 and §75-60 to 66</td>
</tr>
<tr>
<td></td>
<td>2) HB 1248</td>
<td>2) N.C. Gen. Stat. §132-1.10</td>
</tr>
<tr>
<td>Effective Dates</td>
<td>1) 12/1/2005</td>
<td>1) 12/1/2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2) 8/1/2006</td>
</tr>
<tr>
<td>Descriptions</td>
<td></td>
<td>1) Enacts protections against ID theft, including consumer report security freezes, security breach notifications, and protections for Social Security numbers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2) Expands NC's security breach provisions to government agencies.</td>
</tr>
<tr>
<td>North Dakota</td>
<td>SB 2251</td>
<td>N.D. Cent. Code §§51-30-01 to 07 and 51-33-01 to 14</td>
</tr>
<tr>
<td>Effective Date</td>
<td>6/1/2005</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>Requires disclosure to consumers of security breach by businesses maintaining PI in electronic form.</td>
</tr>
<tr>
<td>Ohio</td>
<td>1) HB 104</td>
<td>1) Ohio Rev. Code Ann. §1347.12 (for state agency)</td>
</tr>
<tr>
<td></td>
<td>2) HSB 126</td>
<td>2) Ohio Rev. Code Ann. §1349.19 (for private entity)</td>
</tr>
<tr>
<td>Effective Dates</td>
<td>1) 2/17/2006</td>
<td>1) 2/17/2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2) 3/30/2007</td>
</tr>
<tr>
<td>Descriptions</td>
<td></td>
<td>1) Person or state agency must contact individuals of unauthorized acquisition of PI that is reasonably believed to cause a material risk of ID or other fraud.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2) Same</td>
</tr>
<tr>
<td>State</td>
<td>Legislative Reference</td>
<td>Statute</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>1) HB 2357</td>
<td>1) Okla. Stat. tit. 74, §3113.1</td>
</tr>
<tr>
<td></td>
<td>2) HB 2245</td>
<td>2) Okla. Stat. tit. 24, §161 et seq.</td>
</tr>
<tr>
<td>Effective Dates</td>
<td>1) 6/8/2006</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) 11/1/2008</td>
<td></td>
</tr>
<tr>
<td>Descriptions</td>
<td>1) Only applies to state agencies.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) Provides guidelines for notice requirements.</td>
<td></td>
</tr>
<tr>
<td>Oregon</td>
<td>SB 583</td>
<td>Or. Rev. Stat. §646A.600 et seq.</td>
</tr>
<tr>
<td>Effective Date</td>
<td>10/1/2007</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Consumer identity theft protection act.</td>
<td></td>
</tr>
<tr>
<td>Effective Date</td>
<td>6/20/2006</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Provides for the notification for those whose PI data was or may have been disclosed due to a security system breach.</td>
<td></td>
</tr>
<tr>
<td>Rhode Island</td>
<td>HB 6191</td>
<td>R.I. Gen. Laws §§11-49.2-1 to 7</td>
</tr>
<tr>
<td>Effective Date</td>
<td>3/1/2006</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Ensures that PI is protected by requiring businesses that own or license PI to provide reasonable security for that info.</td>
<td></td>
</tr>
<tr>
<td>South Carolina</td>
<td>S 453</td>
<td>S.C. Code Ann. §37-20-110 et seq. and §39-1-90</td>
</tr>
<tr>
<td>Effective Date</td>
<td>7/1/2009</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Provide protection to consumers in the event of identity theft.</td>
<td></td>
</tr>
<tr>
<td>South Dakota</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Effective Date</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>No data security/breach notification law.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Legislative Reference</td>
<td>Statute</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------</td>
<td>-----------------------------------</td>
</tr>
</tbody>
</table>
| Tennessee | 1) SB 2220  
2) SB 2793 | 1) Tenn. Code Ann. §§47-18-2101 to 2107  
2) Tenn. Code Ann. §§49-7-2___ |
| Effective Dates | 1) 7/1/2005  
2) 3/22/2010 |                                  |
| Descriptions | 1) Requires parties that discover a breach of info resulting in disclosure of unencrypted PI to unauthorized third parties to provide notice of such disclosure.  
2) Protects the TN Independent Colleges and Universities Assoc. (TICUA) or any of its members from liability under certain situations |                                  |
<p>| Texas     | HB 1262 (amended by HB 300) | Tex. Bus. &amp; Com. Code §§521.001 et seq. (replaced previous code) |
| Effective Date | 9/1/2012 |                                  |
| Description | Purpose is to prevent and punish those who commit ID theft and protect the rights of victims of ID theft. |                                  |
| Utah      | SB 69 | Utah Code Ann. §§13-44-101 to 301 |
| Effective Date | 1/1/2007 |                                  |
| Description | Purpose is to address the integrity of consumer credit databases. |                                  |
| Effective Date | 1/1/2007 |                                  |
| Description | Purpose is to prevent and punish those who commit ID theft and protect the rights of victims of ID theft. |                                  |</p>
<table>
<thead>
<tr>
<th>State</th>
<th>Legislative Reference</th>
<th>Statute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virginia</td>
<td>1) HB 1469/SB 307</td>
<td>1) Va. Code Ann. §18.2-186.6</td>
</tr>
<tr>
<td></td>
<td>2) HB 1039</td>
<td>2) Va. Code Ann. §32.1-127.1:05</td>
</tr>
<tr>
<td>Effective Dates</td>
<td>1) 7/1/2008</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) 1/1/2011</td>
<td></td>
</tr>
<tr>
<td>Descriptions</td>
<td>1) Purpose is identity theft prevention and creation of notice of breach of information system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) Requires notification for breach of medical or insurance information.</td>
<td></td>
</tr>
<tr>
<td>Effective Dates</td>
<td>1) 7/24/2005</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) 7/1/2010</td>
<td></td>
</tr>
<tr>
<td>Descriptions</td>
<td>1) Party that owns or licenses computerized data that includes PI must disclose breach to those whose unencrypted PI is reasonably believed to be acquired.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) Expands WA's security breach laws.</td>
<td></td>
</tr>
<tr>
<td>Effective Date</td>
<td>6/8/2008</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Provides for the notification for those whose PI data was or may have been disclosed due to a security system breach.</td>
<td></td>
</tr>
<tr>
<td>Wisconsin</td>
<td>SB 164</td>
<td>Wis. Stat. §134.98</td>
</tr>
<tr>
<td>Effective Date</td>
<td>3/31/2006</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Requires reasonable effort to notify those affected by security breach of unauthorized access.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Legislative Reference</td>
<td>Statute</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Effective Date</td>
<td>7/1/2007</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Providing for notice to consumers affected by breaches of consumer information databases as specified.</td>
<td></td>
</tr>
<tr>
<td>Washington, DC</td>
<td>B16-810</td>
<td>D.C. Code Ann. §28-3851 to 3864</td>
</tr>
<tr>
<td>Effective Date</td>
<td>3/8/2007</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>To ensure that consumers are notified when electronically-stored PI is compromised in a way that increases the risk of ID theft.</td>
<td></td>
</tr>
</tbody>
</table>
Most major U.S. law firms have been victims of security breaches, and the unwelcome threats likely operated covertly for 8 to 9 months before they were discovered. For many firms, the first whiff of insidious action comes from a knock on the firm’s door by the FBI. In 2011, the U.S. government labeled New York City’s 200 largest law firms “the soft underbelly” of hundreds of corporate clients, two experts warned at an ABA Techshow session on data security for lawyers. Even midsize, boutique and solo firms are at risk, warned presenters Sharon Nelson, president of Sensei Enterprises, an information and digital technology firm, and Ben Schorr, CEO of IT consulting firm Roland, Schorr & Tower. And untrained lawyers and office personnel are often the No. 1 chink in a law firm’s defense, the duo said.

“The biggest threat to law firms’ data are its own users who aren’t trying to do damage,” Schorr said, who shared an anecdote of a law firm that unwittingly allowed its receptionist access to read, edit and delete client documents on the firm’s server. At another firm, an associate with Internet connection issues in his office used his own unprotected Wi-Fi router to work on client matters, rendering the firm’s security measures useless. Updated ethics rules require lawyers to make reasonable efforts to make sure client data is secure. The new rules also require lawyers to be competent with technology or to hire someone who is. Judges will no longer buy arguments that tech and its threats are evolving too quickly for lawyers to keep up, Nelson said. Some of the other security tips offered by the panelists include regularly updating firewalls and security programs. “You can’t set it and forget it,” Schorr said, because new security threats are constantly evolving. And always use your own encryption devices in addition to the encryption offered by popular cloud platforms like Dropbox. This double-safety effort keeps lawyers in ultimate control instead of solely relying on the cloud platform’s security measures.

For those lawyers who use smartphones, which is nearly everyone, 36 percent of us have lost them—many in a taxi or left charging at an airport terminal. And 46 percent of those lost were not protected by a password of any kind. Nelson recommends an alphanumeric passcode of at least 12 characters, as 8 has proven too easy for hackers to foil, and for lawyers to enable phones to be wiped of all data after 10 incorrect log-in attempts. For those of us who have trouble remembering all of various our passwords, the duo recommend the apps eWallet and LastPass to help manage our memories.

Copyright 2013 American Bar Association. All rights reserved.

www.abajournal.com/news/article/as_more_hackers_target_lawyers_heres_how_to_protect_client_data/
China-based hackers looking to derail the $40 billion acquisition of the world’s largest potash producer by an Australian mining giant zeroed in on offices on Toronto’s Bay Street, home of the Canadian law firms handling the deal.

Over a few months beginning in September 2010, the hackers rifled one secure computer network after the next, eventually hitting seven different law firms as well as Canada’s Finance Ministry and the Treasury Board, according to Daniel Tobok, president of Toronto-based Digital Wyzdom. His cyber security company was hired by the law firms to assist in the probe.

The investigation linked the intrusions to a Chinese effort to scuttle the takeover of Potash Corp. of Saskatchewan Inc. by BHP Billiton Ltd. as part of the global competition for natural resources, Tobok said. Such stolen data can be worth tens of millions of dollars and give the party who possesses it an unfair advantage in deal negotiations, he said. Though the deal eventually fell apart for unrelated reasons, the incident illustrates the vulnerability of law firms. They are increasingly threatened with a loss of client business if they can’t show improved security as such attacks continue to escalate.

Stephen Surdu, vice president of professional services at Mandiant Corp., a cybersecurity firm that tracks industrial espionage, compared the risk of hacking in the mergers and acquisition arena to gambling. “You’re playing poker, and there’s a mirror over the other guy’s shoulder,” Surdu said.

“As financial institutions in New York City and the world become stronger, a hacker can hit a law firm and it’s a much, much easier quarry,” said Mary Galligan, head of the cyber division in the New York City office of the U.S. Federal Bureau of Investigation. Galligan’s unit convened a meeting with the top 200 law firms in New York City last November to deal with the rising number of law firm intrusions. Over snacks in a large meeting room, the FBI issued a warning to the lawyers: Hackers see attorneys as a back door to the valuable data of their corporate clients. “We told them they need a diagram of their network; they need to know how computer logs are kept,” Galligan said of the meeting. “Some were really well prepared; others didn’t know what we were talking about.”

The ability to keep client information confidential is a key principle of how law firms function. The attacks have created what Tony Cordeiro, chief information officer at White & Case LLP, termed a “healthy paranoia.”

Mandiant, which is based in Alexandria, Virginia, said it estimates that 80 major U.S. law firms were hacked last year. More than a dozen law firms contacted about the New
York City meeting, including Wilson Sonsini Goodrich & Rosati PC and Cadwalader Wickersham & Taft LLP, didn’t return telephone calls and e-mails seeking comment. Jennifer Becker, a spokeswoman for Skadden Arps Slate Meagher & Flom LLP and Kevin Blasko, a spokesman for Baker & McKenzie LLP, declined to comment. Mark Hendrick, director of information technology for Baker Botts LLP, declined to comment beyond confirming the firm’s attendance at the November forum. “Given the sensitive nature of the topics discussed, including possible threats to the safety of our IT network, I can only state that at Baker Botts we work diligently every day at maintaining the integrity of our systems,” Hendrick said in an e-mailed statement.

‘Up at Night’
Cordeiro said “protecting ourselves against threats keeps me up at night.” Hackers could gain access to a firm’s networks through phishing or its use of cloud storage programs, which might allow information to be compromised during a seemingly routine transfer or sync, Cordeiro said. “It’s a people door,” Cordeiro said. “It’s like having the door and allowing someone to walk through without having a key.”

To enhance New York-based White & Case’s data security, he said he requires the use of encrypted connections and restricts the use by attorneys of vulnerable file-hosting programs like Drop Box, a cloud-based system that allows users to save files including photos, documents and videos. White & Case is one of a handful of firms to receive an accreditation for information protection, which some law firms are now using as a selling point to clients.

Dedicated Terminal
Edward Stroz, a partner in the data security firm Stroz Friedberg LLC, said many more law firms have knocked on his door within the last 12 months than previously. They are driven there in many cases by clients, who are demanding greater protection of their confidential information, he said. In some sensitive cases, Stroz has required lawyers to access highly sensitive client data directly in a secure location, banning e-mail or the digital transfer of documents.

“They have to go on site at the client company, use a dedicated terminal and review the data there so that the client knows it never left the building,” Stroz said. The level of skill and seriousness of the attacks differs widely. Attackers include hackers looking for information they can sell quickly. Law firms representing celebrities, for example, are top targets, said Don Jackson, a researcher with Atlanta-based Dell SecureWorks, a cybersecurity firm.

The Canada case involving Potash Corp. of Saskatchewan Inc. by BHP Billiton Ltd. (BHP) shows just how serious the threat can be. The intruders were professionals potentially linked to the interests of a nation-state, with all its resources, said Anup Ghosh, chief scientist at the Fairfax, Virginia-based cyber security firm Invincea Inc.
New Spy Game
“This is the new way the spy game is played,” Ghosh said. Chinese government officials have denied any involvement. Calls to the Chinese embassy in Ottawa weren’t immediately returned. Bill Johnson, a spokesman for Potash Corp., and Ruban Yogarajah, a spokesman for BHP, declined to comment. At the time of the attacks, China was on the hunt for new sources of agrochemicals. Potash is a common name for compounds containing potassium used in the manufacture of fertilizer. Sinochem Group, China’s formerly state-owned chemical giant, hired Deutsche Bank AG and Citigroup Inc. in September 2010 to evaluate moves to disrupt BHP’s bid for Potash Corp., a hostile tactic approved directly by the Chinese government, according to a report at the time by the Financial Times.

Tobok said a law firm involved in the deal detected signs of the intrusion the same month, including network disruptions. Analyzing the attack, investigators found that the spyware designed to capture confidential documents -- and sent via spoofed e-mails -- was compiled on a Chinese-language keyboard and China-based servers were involved in the attack, he said.

Aboriginal Ruse
Technical similarities connected those attacks with counterfeit e-mails sent to Finance Ministry officials supposedly from an aboriginal group opposed to the deal, according to Tobok. The e-mails directed the officials to a website which stealthily downloaded spyware through a vulnerability in web browsers onto state-owned computers, according to a Canadian government report cited by the Ottawa Citizen in October. “It sounds like something out of Mission Impossible, but this is the sophistication of the stuff out there,” Tobok said.

Successful Attacks
It’s not known how successful the attacks were or how any data stolen was used by the intruders, investigators have said. The government report said the attack on the federal ministries was successful in stealing some data. According to a person familiar with the case who asked not to be identified because of the criminal investigation, the hackers’ victims included Toronto-based law firms Blake, Cassels & Graydon LLP, which represented BHP, a company with primary offices in Melbourne, Australia, Singapore and London. Also hit, the person said, was Stikeman Elliott LLP, which represented Saskatoon, Canada-based Potash Corp.

The law firms would have had detailed knowledge of the deal’s negotiations, including potential weak points, the person said. Diana Lawrence, a spokeswoman for Stikeman Elliott, said there was no evidence client information was compromised or that the firm’s networks were breached. Robert Granatstein, managing partner of Blake Cassels, said that the firm wasn’t aware that any client data was compromised.
Takeover Stopped
The Canadian government later killed the BHP takeover using federal powers to declare it wasn’t in the nation’s interest. Similarities between the Canadian attack and other recent intrusions at U.S. law firms suggest that cyber attacks on attorneys are now part of the hacking playbook for gathering sensitive information on corporate clients, according to Ghosh. In one recent case, a corporation was negotiating to open a major plant in China when the law firm helping with the deal was hacked, Surdu said. “They were looking for what the company was willing to pay for that land, what were they willing to pay to bring roads to the facility,” he said. “This was a major deal with lots of zeros on the end.”

Other recent law firm hacks involved efforts to steal secret details about a merger and documents relating to an opponent’s strategy in a major litigation, Ghosh and Surdu said. Galligan, the FBI agent, said that the culture of law firms and the significant sway of partners often make them a soft target.

‘It’s Trendy’
“Everybody wants network administrator rights,” Galligan said. “It’s trendy.” She said partners insist on mobility -- including the flexibility to review case documents at weekend homes or on the road -- which means highly sensitive documents are routinely transferred by e-mail.

At the November meeting, the FBI urged firms to review their mobility policies, including the security of e-mail linkups and mobile phones, Galligan said. “If clients start thinking they can’t give private information to their lawyers because it might get out, it’s a huge problem for the profession,” said Richard Goldberg, a former software programmer and lawyer in Washington involved in the data security issue. “The whole system will start to fail.”


To contact the reporters on this story:
Michael A. Riley in Washington at michaelriley@bloomberg.net;
Sophia Pearson in Wilmington, Delaware, at spearson3@bloomberg.net
To contact the editor responsible for this story:
Michael Hytha at mhytha@bloomberg.net