FOLEY
FOLEY & LARDNER LLP

CYBERSECURITY UPDATE

July 2015

AN INDIVIDUAL'S INFORMATION SECURITY CHECKLIST

by Michael Overly

Employees are the front line of your information security defense. While technological protections are essential (for example, anti-virus software, firewalls, spam filters, etc.), none are as effective as a vigilant end user. We have created these checklists of measures of which every user should be aware. By sharing them with individuals within your organization, you can dramatically increase not only the security of your systems and data, but the user's own personal computers and data. All too frequently, the security of one can impact the other.

KNOW YOUR DATA AND WHERE IT RESIDES

- ☐ Know what data you have and where it is located: Ask people to show you how they create, access, and destroy data.
- ☐ For your personal home accounts, understand where your information is stored. For example, will your data be automatically backed up to online services (e.g., DropBox, iCloud, Microsoft OneDrive, Google Drive, SugarSync, etc.)? Do you use online document services like MicroSoft Office 365, Google Docs, and others? If you use any of these services, understand how your data is protected. In many instances, your data, documents, pictures, voicemail, etc. will not be stored in encrypted form. In still other cases, the terms of use for those services may grant the provider an unqualified right to use — and even sell — your data to others. "Free" services come at a price: your privacy.
- ☐ All confidential, proprietary, and sensitive information should be encrypted or otherwise secured.
- ☐ Determine whether removable media is allowable. If not, disable ports and file sharing. If allowed, require information be encrypted and secured. When done with the information/device, ensure information is securely erased. Beware: If not properly done, erased or deleted information can be readily retrieved using free tools from the Internet.
- ☐ Never transfer sensitive company information to a mobile storage device (e.g., a CD, USB drive, etc.) unless expressly permitted by our security policies and procedures.
- ☐ Consider purchasing credit monitoring protection for your personal information. Among other things, these services will continuously monitor the Internet — particularly known hacking sites — for evidence of your personal information (e.g., social security number, credit card numbers, phone number, etc.).

Keeping informed on all aspects of cybersecurity can help ensure your organization's safety. Watch **here** to discover three important misconceptions about cybersecurity that you should recognize. Then watch your inbox for periodic emails, including videos, focused on cybersecurity-related issues and trends. All videos can also be viewed on our **YouTube Cybersecurity Playlist**.

INSIDE THIS ISSUE

MONITOR

- ☐ Monitor activity within the network and your systems.
- ☐ Review abnormal behavior (e.g., a user that normally always works days, logging in during the middle of the night).
- ☐ Encourage users to report concerns and to ask questions.

VENDORS, SERVICE PROVIDERS, CONSULTANTS, AND OTHER THIRD PARTIES

- ☐ Never allow a third party to use a workstation or otherwise access or use your systems and data without supervision and appropriate contractual protections.
- ☐ Conduct diligence of all service providers and ensure they are compliant with applicable law and our corporate security requirements.
- ☐ For your personal home devices (e.g., laptops, tablets, smart phones, etc.), consider removing sensitive unencrypted data before having a third party service the device. There have been many instances where individuals have brought their laptops and other devices to a local computer repair shop for service only to find out the operator of the store secretly stole their data. Use care when granting a computer or warranty vendor access to your computer for tech support. In many instances, once access is granted, they will have access to the entire content of the hard drive, and in some cases the network, if the computer is connected to the network.
- ☐ If you sell or otherwise dispose of a personal device, make sure your data is securely removed/deleted from the device. Simply deleting files is not sufficient. They can be easily recovered. There are readily available programs on the Internet to securely delete data. In addition, doing a full reset to "factory condition" on a smartphone will erase all data.

ONLY AUTHORIZED SOFTWARE

- ☐ Do not download or install unauthorized or unapproved software or applications from the Internet.
- ☐ In particular, never install encryption software, remote access, backup, or other similar software without the express approval of our information security personnel.
- ☐ Always be certain of the source of downloaded software (i.e., you are actually getting the software from its true creator). It is common for hackers to create fake websites and even "hijack" visitors from official websites, where applications can be downloaded. In some instances, the top search results for software on Google and other search engines point to disguised hacker websites, where your personal information may be stolen and viruses propagated.
- ☐ For your personal computers, make sure you have anti-virus and firewall software installed. There are many inexpensive, complete security packages available for home systems. Also, always promptly install security and other updates to your personal computer and mobile device operating systems.

WEBSITES, SOCIAL MEDIA, AND PUBLIC EMAIL

- ☐ Always proceed with the understanding that no public email or messaging service (e.g., services provided by online services such as Google, Yahoo!, Microsoft, Skype, and others) is secure, and that all communications will be stored and, potentially, viewed by others.
- ☐ Avoid sending highly sensitive information through unsecured email, texts, or other communications (e.g., Gmail, Yahoo! mail, text apps on smartphones, etc.).
- ☐ Do not forward internal email, documents, or other information to a personal email address or download to personal devices for access outside of our systems. We cannot protect the information once it has been removed or shared outside of our systems.
- ☐ When submitting personal or other sensitive information via a website, make sure you see the site's address begin with "https," as opposed to "http." Think "s" stands for secure. "Https" uses encryption to send information across the Internet, thus, reducing the risk that the information will be improperly accessed.
- ☐ Think before you submit. Once submitted to a website or transmitted through an online communication service, the information is public. You never know where the information will show up. There is no such thing as deleting information from the Internet. The Internet is forever.
- ☐ Exercise caution using services and devices that record your communications (e.g., Google Voice, Siri, Microsoft Cortana, Skype™, VoIP applications, mobile app-based texting, etc.).
- ☐ Before posting pictures and videos online, remember they may contain GPS data showing where the picture was taken.
- ☐ Be mindful of backup applications running on personal devices (e.g., DropBox, iCloud, Carbonite™, etc.), making copies of sensitive company information, and storing them online.
- ☐ Do not get hooked on someone's fishing line. Do not reply to or click on links in emails, pop-ups, or websites that ask for personal information, financial information, or health information. Never click on links or open files in an email from someone you do not know or were not expecting.
- ☐ Think before you open. If you do not know the sender, are unsure of why the attachment was sent, or if it looks suspicious, do not open the attachment. Better to verify with the sender than infect your computer, or worse, the network.
- ☐ PDF files are a very popular way of distributing viruses. Before opening a PDF, be sure you know where it came from.
- ☐ When installing apps on your smartphone, be cautious of requests to access your calendar, contacts, texts, GPS, and other data. In many, if not most, instances, there is no reason for these apps to have access to your data and, in almost all instances, whatever you choose to share will likely be analyzed and sold to others.

CYBER INSURANCE: IS YOUR BUSINESS PREPARED?

by Ethan Lenz

Part of any company's contingency plan for financing losses that might arise from cyber threats should include a review of its current insurance coverage and an assessment of the costs and benefits of obtaining cyber-specific insurance coverage.

Questions that should initially be addressed, and items to consider in this regard, include:

1 Are we protected under our Commercial General Liability insurance coverage?

There are likely significant limitations on the protection provided by such coverage due to limitations of the coverage to losses arising from damage to "tangible" property (as opposed to intangible data losses) and specific exclusions of coverage for damage to electronic data.

2 Are our directors and officers adequately protected from suits by shareholders and regulatory agencies?

Increasingly, D&O insurers are taking much harder looks at companies' information technology safety and security, and are considering including exclusions or limitations on the protection they provide under their policies.

3 Is the company itself protected from claims by customers, regulatory agencies and other third parties under our D&O policy?

For publicly traded companies, in particular, the answer is likely "no" because of limitation of the coverage to securities-related claims.

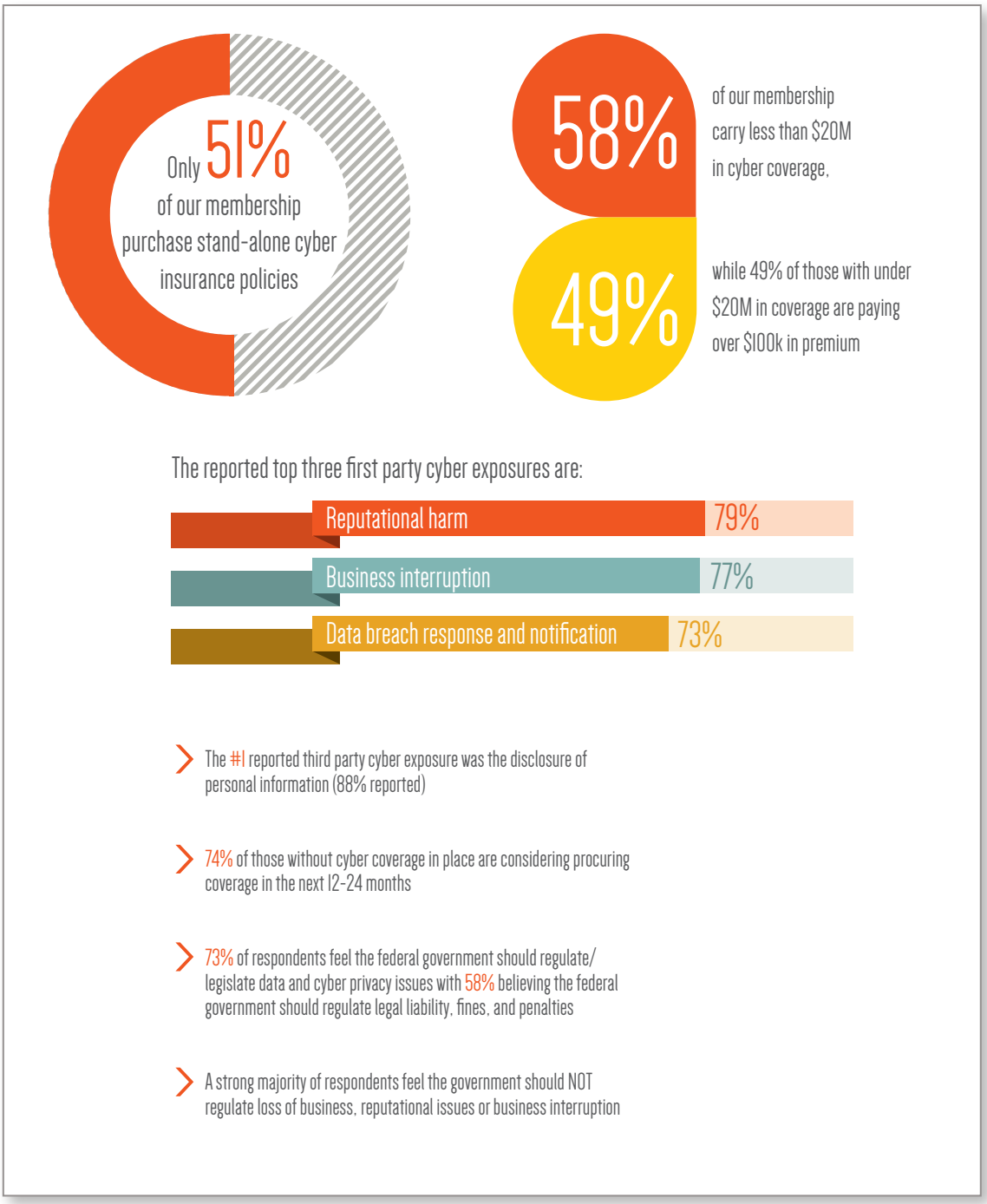
Given these limitations on coverage under the more traditional forms of insurance coverage, insurers are developing new cyber-specific insurance coverage forms. The policy forms are often menu-driven, where a company can pick and choose the particular coverage it wishes to include in the policy. This might include protection for costs associated with the company's direct losses arising from business interruption, extra expenses, and reputation damage resulting from a breach event.

Additionally, a cyber policy may provide protection against third-party claims and associated losses and expenses arising from:

- Failures of network security systems
- Wrongful disclosure of information
- Regulatory investigations arising from privacy and data breaches
- Forensic investigations following breaches
- Customer notification expenses following a breach
- Costs associated with providing credit monitoring and identity protection services to customers following a breach

Given the relative infancy of cyber insurance, there are no standardized policy forms utilized by insurers. Every insurer writes the coverage on its own policy forms, and the scope and breadth of protection can vary widely from one insurer to the next. Seemingly small differences in the wording of the policy forms can lead to significant differences in how the policies will potentially respond in the event of an actual claim. At the same time, however, the terms and conditions of the policy forms are typically highly negotiable and can be tailored to cover the risks posing the greatest threat to any particular client.

So how prepared are today's businesses when it comes to cyber insurance protection? A recent survey by RIMS, the risk management society™, asked their membership of more than 3,500 industrial, service, nonprofit, charitable, and government entities that same question. Here is what they discovered:



The full survey results are available at **www.RIMS.org/Riskknowledge**.

For information on exhibiting or sponsoring at future RIMS events, please contact Matt Whyte at **mwhyte@rims.org**.

INSIGHTS ON RECENT DEVELOPMENTS

by Chanley Howell and Steve Millendorf

LESSONS LEARNED FOR BUSINESS FROM THE OFFICE OF PERSONNEL MANAGEMENT SECURITY BREACH

On July 9, 2015, the Office of Personnel Management (OPM) announced that more than 21 million Social Security numbers were compromised in the recent security breach the agency suffered. This is in addition to the 4.2 million Social Security numbers compromised as reported in June of this year. The two systems breached were the Electronic Official Personnel Folder (eOPF), an electronic personnel file for federal employees (often referred to by federal employees as "Your Federal Birth Certificate") that includes compensation, employment actions, retirement plans, work schedules, and personal identifying information of federal employees, and the EPIC database, which contains sensitive information gathered for government employee and contractor investigations. The EPIC database also includes local law enforcement and emergency personnel who may have contact with federal anti-terror "fusion" centers during their activities. Information regarding CIA personnel may not have been affected because it does not use the EPIC system for background investigations and personnel clearance. Unnamed sources continue to link both intrusions to China. After testifying before Congress about the breaches and under intense pressure from Congress, OPM's Management Director Katherine Archuleta resigned on July 10.

In response to the first attack, the Obama administration ordered a "30-day Cybersecurity Sprint" which requires federal agencies to beef up cybersecurity by conducting penetration tests on their systems, fixing any known vulnerabilities immediately, restrict the number of privileged users who can access privileged information, implement multi-factor authentication procedures, and deploy monitoring systems to detect intrusions. However, many agencies may require more than thirty days to implement one or more of these new practices after years of simply "checking the box" to claim security "compliance" with regulations without really being secure.

Companies can learn from the security deficiencies at OPM as part of their continual monitoring and evolution of cybersecurity efforts. In particular, as recently as November, 2014, the Office of Inspector General issued another in a string of audit reports which identified numerous vulnerabilities and security protocols at OPM (the report can be found **here**). Despite these warnings, OPM continued to fail to implement relatively simple cybersecurity measures. The following are some of the deficiencies that were noted in the 2014 audit report:

- OPM had not fully established a risk executive function, and there was no individual accountable for appropriately analyzing and implementing management and/or board approved strategies to minimize the information security risks to the organization.

  Lesson learned:
  In order to achieve appropriate accountability, and consistent with NIST and ISO standards, companies and federal organizations should designate at least one individual accountable to the organization for assessing and addressing information security risks – this individual should report up to the board, information security committee, or other appropriate management on a regular basis or as required during security incidents.

- OPM did not maintain a comprehensive inventory of servers, databases, and network devices. In addition, OIG was unable to independently attest that OPM has a mature vulnerability scanning program.

  Lesson learned:
  In order to properly implement security controls it is essential that businesses inventory and

map all information system components, including the sensitivity of the data stored in and processed by those components.

- Although about 80 percent of OPM's systems had implemented monitoring technologies to detect a security event, the remaining twenty percent of OPM's systems and all systems operated by outside contractors did not include such monitoring as required by the Federal Information Security Management Act (**FISMA**). As a result, OPM was not able to understand the activity on any of its contractor's networks and only had a limited understanding of the scope of activity occurring on its own networks, potentially further exacerbating the damage due to the breach.

  Lesson learned:
  Intrusion detection or other monitoring tools are an important component of an organization's cybersecurity protections to detect abnormal activity, minimize the damage due to the breach, and to understand the extent of a breach.

- Access control mechanisms to highly sensitive information did not require two factor authentication. The Office of Management and Budget mandated the use of Personal Identity Verification (PIV) readers as a form of secondary authentication for access to work stations and applications; however the OIG **reported** that none of OPM's 47 major applications required the use of such authentication.

  Lesson learned:
  To mitigate the chance of a breach from an attacker simply having a password, companies should use two factor authentication methods whenever possible to protect access to its most sensitive information.

- OPM continued to use outdated IT components that contained known security vulnerabilities. For example, it continued use Adobe's ColdFusion and JRun Web server applications. The ColdFusion source code was stolen from Adobe, and Adobe dropped the entire JRun product line in 2013, with support ending in 2014. OPM also continued to operate systems based on Microsoft's Windows XP operating system under a custom support agreement with Microsoft. Some of the core systems used to access some of its most sensitive information have not been updated since they were patched for Y2K.

  Lesson learned:
  If your hardware or software systems are too old to support modern security techniques, have known vulnerabilities, or are no longer officially supported, update the systems. If you cannot afford to update the systems, consider keeping them off the Internet.

The breaches at OPM illustrate that some federal agencies have failed to adopt an approach to security that includes understanding how attackers may exploit systems in unexpected ways, including the use of trusted white-hat hackers to conduct penetration tests that resemble current actual attacks. An important part or every company's cybersecurity program should include monitoring current developments in information security, which includes learning from the security mistakes made by others, and taking steps to avoid making those same mistakes.

TELECOMS' SETTLEMENT WITH FCC HIGHLIGHTS THE IMPORTANCE OF ENCRYPTION AND VENDOR DUE DILIGENCE

On July 9, 2015, the Federal Communications Commission (FCC) announced a $3.5 million settlement with TerraCom, Inc. and YourTel America, Inc., resolving an investigation into whether the companies failed to properly protect the confidentiality of personal information they received from more than 300,000 consumers. The FCC's action and settlement highlight the important roles both encryption and vendor due diligence play in the protection of sensitive personal information,

such as Social Security numbers and driver's license numbers. The case provides useful guidance for all companies – not just those regulated by the FCC.

The FCC's investigation found that the companies' vendor stored consumers' personal information – including names, addresses, Social Security numbers, driver's licenses, and other sensitive information – on unprotected servers that were accessible over the Internet. The FCC asserted that "the Companies' choice to store, or its vendor's choice to

store, files containing the PI of customers in a publicly accessible folder on the Internet, without password protection or encryption, is the practical equivalent of having provided no security at all." This lack of adequate security in turn resulted in a data breach which exposed their customers' personal information to unauthorized individuals. The lack of encryption played a prominent role in the FCC's enforcement action.

The case also demonstrates the importance of vendor due diligence. Had TerraCom and YourTel conducted appropriate due diligence on their vendor, they likely would have discovered the vendor's lax security practices with respect to encryption of sensitive personal information. Learning from this enforcement action: Companies should ensure that their security practices and the security practices of their vendors include the encryption of all sensitive information such as Social Security numbers and driver's license numbers.

INTERNATIONAL SPOTLIGHT: CHINA'S NEW NATIONAL SECURITY LAW AND PROPOSED CYBERSECURITY LAW AIMS TO STRENGTHEN GOVERNMENT'S POWERS

On July 1, 2015, the Chinese government announced that it had enacted a new national security law. The law is a general pronouncement of the importance of national security to the Communist Party, and stresses that security must be maintained in all fields, including culture, education, international waters and cyberspace. The cybersecurity measure is intended to make the Internet, information technologies, infrastructure, and data in key sectors "secure and controllable."

The law will give the government more power to crack down on actual and perceived security threats, both internal and external. While it remains to be seen exactly how the law will be implemented, it is a signal to western companies that the Chinese government is taking security – including cybersecurity – very seriously, potentially making it even harder for companies to do business in China.

Following quickly on the heels of the national security law, on July 6, 2015, Chinese lawmakers released a draft of a cybersecurity law that would require Internet service providers to retain user data and cooperate with authorities. A translation of the proposed law can be found **here**.

Among other things, the law would elevate the authority given to the Chinese government to crack down on Internet content. In the past, China has frequently taking action to prohibit and limit many types of online content, such as pornography and political discussions. Foreign sites have been blocked, and domestic sites use automated censorship mechanisms as well as staff members to remove posts on forbidden topics. The proposal also includes the ability of the government to restrict Internet access in a particular region to

> The law would also strengthen the government's power to oversee data collection and to block private messages that disseminate information prohibited under Chinese law

"safeguard the national security, social stability or handle a sudden major incident of concern for social safety."

Under the proposed law, Internet service providers must store data collected within China inside Chinese territory. Data stored overseas for business purposes must be government-approved. Network equipment must also be approved under testing standards issued by China's cabinet.

The law would also strengthen the government's power to oversee data collection and to block private messages that disseminate information prohibited under Chinese law, including those deemed "to promote terrorism, extremism, incitement to subvert state power and overthrow the socialist system."

As with the national security law, the proposed cybersecurity law is short on details, and it remains to be seen how the law will be implemented and enforced. One aspect of the law, for example, requires the development of safeguards on "critical information infrastructure." The manner in which this is implemented could have a significant impact on companies looking to do business in China.

Companies looking to do business in China should keep a close eye on how the national security law and the proposed cybersecurity law (upon its likely passage) are implemented and enforced, as both laws will have a significant impact business dealings in China.

NEGLIGENCE ACTIONS HIT UCLA, SONY, AND HOME DEPOT BOARDS

by James Kalyvas and Michael Chung

In the most recent in a string of cases highlighting the trend of claims of negligence against boards and officers in the face of security breaches, on July 20, 2015, a class action complaint was filed against the UCLA Health Systems Auxiliary and the Regents of the University of California. The plaintiff alleges, among other claims, a "failure to adequately secure the private, personal financial information of Plaintiff and all other persons similarly situated." The complaint was filed in the Central District (Los Angeles) of the United States District Court. In Plaintiff's negligence claim, he alleges:

> "Defendants had a foreseeable duty to Plaintiff and Class members to exercise reasonable care to secure Plaintiff's and Class members' nonpublic personal and financial health information from being accessed by unauthorized persons. This duty included creating, maintaining, testing, and securing any databases containing Defendants' customers' nonpublic personal and financial information, to ensure that Plaintiff's and Class members' nonpublic personal and financial information was secured from cyber attack, and other things. This duty also included, at the minimum, that Plaintiff's and Class members' nonpublic personal, financial and health information be encrypted."

On June 15, 2015, in a class action lawsuit arising out of Sony Pictures' 2014 data breach, the Federal District Court for the Central District of California ruled on Sony's motion to dismiss the complaint filed by Sony employees, allowing certain of the plaintiffs' claims for damages to proceed, including a claim that Sony's failure to maintain adequate data security measures was negligent. The court also held that the plaintiffs had established standing by alleging that their personally identifiable information had been made available to potential identity thieves and that the information had been used to send emails threatening physical harm. The court determined that the allegations demonstrated "a credible threat of real and immediate harm, or certainly impending injury."

Sony argued that plaintiffs' negligence claim should be dismissed because the plaintiffs suffered only purely economic losses, and such losses were not recoverable under the economic loss doctrine. Though decisions have been mixed in barring negligence claims arising out of data breaches, here, the court noted that even if the plaintiffs had only suffered purely economic losses, a negligence claim could still proceed in California if a special relationship existed between the parties. The court determined that plaintiffs' employment with Sony was sufficient to establish such a special relationship, and thus the plaintiffs' negligence claim could proceed despite having suffered only purely economic losses.

Also in June, a complaint was filed in Delaware Court of Chancery, arising out of Home Depot's 2014 data breach which had resulted in the widespread exposure of consumer information.

The complaint was filed by a Home Depot stockholder pursuant to 8 Del C. § 220 to compel the production of records at Home Depot related to the data breach. The court noted that the allegations of "lax cyber security at the company, the pending government investigations, together with numerous lawsuits claiming misconduct at Home Depot, provide a credible basis from which mismanagement at the Company can be inferred," and that the inspection of records was necessary to "take appropriate action in the event the members of the Company's management and certain directors did not properly discharge their fiduciary duties."

The corporate laws of every state impose fiduciary obligations on all officers and directors. Courts will not second-guess decisions by officers and directors made in good faith with reasonable care and inquiry. To fulfill that obligation, officers and directors must assume an appropriate role in establishing the correct policies and procedures to address data security in their organizations and ensuring the policies and procedures are followed.

PLAN AND TRAIN FOR SECURITY INCIDENTS NOW

by Aaron Tantleff, Jonathan Halpern, and Matthew Karlyn

In order to minimize potential damage to company assets, employees, and customers, it is critical that companies take quick and effective action upon the discovery of any suspected or actual cyber incident (e.g., any unauthorized access, use, or disclosure of data or other information security breach). To achieve an effective response to an incident, you need an incident response plan in place and employees who are trained to execute it before the need arises. The incident response plan should address, at a minimum:

- Preparation
- Detection and analysis
- Containment
- Eradication
- Recovery
- Follow-up capabilities

Each of the above elements is discussed briefly below.

PREPARATION

- **Have a plan — now.** Establish and maintain an incident response plan that keeps pace with the rapidly evolving threats to data and use of technology in your company (e.g., automobile manufacturers must now adjust their response plans to address threats to vehicles).
- **Incident response testing and exercises.** Companies that develop and implement a trial run of their incident response plan at least once a year are in a significantly better position to identify vulnerabilities and address them before a real attack strikes. The feedback and lessons learned from executed trial runs should be reviewed and incorporated into existing incident response plans to make them more effective.
- **Incident response training.** Detailed, practical, up-to-date training is critical. Everyone with any responsibility under the incident response plan should know their role in the plan and how to execute it. Training must be focused and contextual for each participant, rather than generic.
- **Resources.** Set aside appropriate resources (including all applicable hardware and software) that are available and accessible to execute the plan.
- **Protect your communications.** Engage legal counsel — with knowledge in information management and security — to advise and assist in the implementation of appropriate preventive measures in compliance with the evolving standard of care. This will increase both the assurance that your plan will be viewed as reasonable, if questioned, and the likelihood of protecting communications with and actions directed by counsel under applicable attorney/client privilege and work product doctrines.

DETECTION AND ANALYSIS

- **Detection.** Detection capabilities that automatically scan, monitor, and search for incidents, along with manual scanning and monitoring (where automated processes are not feasible), routinely form part of effective incident response plans. Regularly reviewing reports on new vulnerabilities and access logs are a couple of examples of manual monitoring. Incidents should be reported immediately to the appropriate individuals upon discovery of an incident.
- **Incident analysis.** A response to a suspected or actual incident starts with an analysis to determine the scope, nature, and origin of the incident, as well as the people, software, and hardware involved in the incident. The analysis should identify affected systems and data, the origin of the incident, any malware implicated, any remote servers that received data, a list of affected individuals, and any additional impact on company networks, systems, and information infrastructure.

- **Incident documentation**. To ensure that incidents are resolved in a timely manner and that the company complies with its own policies and applicable legal requirements, it is critical that any suspected or actual incident be properly documented, and that, to the extent that it is practical, documentation and communication be under the direction of a company attorney to maximize the protection of the communications. Identifying, collecting, and maintaining records regarding the company's response to incidents should be standard operating procedure.

  The documentation should include: a status report and a summary of all related incidents and responsive actions taken by the company; an impact assessment; contact information for every individual and entity involved; a comprehensive list of the collected evidence; and a summary of incident prioritization, notification, containment, eradication, recovery, reporting, and follow-up actions to resolve the incident and prevent future recurrences. Depending on the nature of the incident, companies may consider additional steps such as:

  - Arranging for a "forensic image" of the affected computer systems
  - Locating backups and checking for any unauthorized changes to network
  - Using uncompromised media to store copies of retrieved and stored data — and safeguarding media from being compromised
  - Preserving logs, ongoing notes, records and data — to be preserved, if possible, by a single designated custodian
  - Recording any continuing activity for ongoing incidents and, subject to legal limitations, employment agreements, privacy policies, and pre-clearance from legal counsel, considering monitoring and recording communications between intruder and targeted server in order to protect the entity's property or rights or with advance documented consent of system users
- **Incident prioritization**. Multiple incidents occurring simultaneously or in a short time period can wreak havoc on company systems and employee morale. If more than one incident adversely affects a company, it may be necessary, depending on a company's resources and the nature of the incidents, to prioritize the response to account for each incident's overall impact.
- **Incident notification**. In many cases, incidents (and even suspected incidents) may require notification of state and federal agencies and others. Depending on the resources available to the company, identifying a point-of-contact and at least one backup contact to address incidents with the media, law enforcement, incident reporting organizations, and other third parties will help ensure consistent and accurate responses. Training a designated company manager to communicate effectively about the incidents and the company's compliance before any security incident occurs is an essential part of an effective response plan.

CONTAINMENT, ERADICATION AND RECOVERY

- **Incident containment**. Upon discovery, containment is critical —stop the breach, contain the damage, secure the information, and recover compromised information. Incidents encompass a wide range of issues, including severity, information type, causes, and risk. Be sure to assess how various incidents may affect the particular operations and assets of your company, prioritize them and take extra measures to safeguard the most valuable from attack. A detailed containment strategy may include the following:
  - A range of measures, from blocking access to monitoring activity to identifying the source or scope of the incident
  - Re-routing network traffic
  - Filtering or blocking a distributed denial-of-service attack
  - Isolating some or all of compromised network

  - » Restoring the network to prior uncompromised state if back-up copy of important data has been preserved
  - » Preserving records of mitigation/response measures and related costs
- **Incident eradication**. Response, resolution, and containment may not be sufficient. The lingering effects of an incident can harm a company immediately or long after an incident occurs. After an incident has occurred and the company has carried out its containment strategy, an eradication process may be necessary to eliminate any harmful remnants. A supplemental action plan may be called for: delete malware, disable breached user accounts, and rebuild systems.

POST-INCIDENT ACTIVITY

- Each incident can help educate companies to become smarter, draft more sophisticated and comprehensive security response plans, and improve their execution capabilities to detect, prevent, and respond to incidents. Taking full advantage of lessons learned is critical — doing so will enhance a company's detection and response capabilities, make them stronger, and render managers better equipped to safeguard the operations and assets of their companies.
- Consider implementing new and improved technology and ensuring that lessons learned are incorporated into the company's information and security training programs, policies and protocols. After an incident, conduct meetings and training sessions with all involved parties to address the incident in its entirety: from detection, investigation, and diligence to containment and eradication. As part of the post-incident recovery phase, a thorough review of the company's incident policy should be conducted and modifications made to incorporate the lessons learned.

ACTIONS TO AVOID

- Don't ignore the incident. Your response actions may have more impact on the operational and reputational damage and liability incurred than the incident itself.
- Suspend use of the compromised system or run suitable antivirus programs. Failing to do so may spoil, alter, or destroy evidence.
- Do not hack back for any purpose, including accessing, damaging, impairing, or preventing another attack or further damage from a system believed to be connected to the intruder. Even with a good motive, such conduct is likely illegal, under U.S. and some foreign laws, and therefore may well result in civil and criminal liability.
- Leave examination of the affected systems to the forensics experts. Non-experts commonly spoil, alter, or destroy evidence.

SOME FINAL THOUGHTS

- Each plan should also be tailored to the company's particular business model and customer base (e.g., an organization that accepts credit cards is required to have an emergency response plan consistent with PCI Data Security Standards).
- In addition to a training program for employees, training for and obtaining cooperation from contractors and others with access to company information is a critical program component.
- Periodic auditing also is necessary to test company performance against plan requirements.
- Finally, company cyber managers should oversee the compliance with applicable laws and the enforcement of the company's policies, either through or via the combination of internal and external resources, including engaging counsel as appropriate.
- Responding to information incidents is an iterative process. Lessons learned as part of an investigation or incident response, as well as any trial run of the plan, will aid the company to better understand what happened, how to be better prepared for future incidents, and how to help avert future incidents.

The action plan incorporates and adapts certain recommendations from the 2015 Best Practices Report, Cybersecurity Unit, Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice.

LAW WATCH: CYBERSECURITY LEGISLATION THAT COULD AFFECT YOUR BUSINESS

by Dennis Cardoza

Cybersecurity issues continue to command a great deal of attention on Capitol Hill.

The recent data breach in the Office of Personnel Management (OPM) disclosed over 4,000,000 sensitive records and other classified information regarding virtually the entire federal workforce. The OPM attack highlights the difficulty of protecting government secrets and personal privacy. Expect Congress to conduct several informational hearings into the cybersecurity challenges that face both government and industry, throughout the summer and fall of 2015.

In 2002 Congress passed the Federal Information Security Management Act (FISMA). This act began the work to establish federal rules and guidelines regarding cyber threats, including a requirement for each federal agency to implement a program providing information security for agency-wide systems. For the next twelve years Congress held hearings and debated further cyber legislation, however there was little in the way of significant new law.

IN DECEMBER OF 2014 CONGRESS PASSED FIVE BILLS:

- **PL 113-246 Cybersecurity Workforce Assessment Act**
- **PL 113-274 Cybersecurity Enhancement Act of 2014**
- **PL 113-277 Border Patrol Agent Pay Reform Act of 2014**
- **PL 113-282 National Cybersecurity and Communications Integration Center Act of 2014**
- **PL 113-283 Federal Information Security Modernization Act of 2014**

While these measures generally cover only federal agency management and best practices in the "government" cybersecurity space, business and industry should be aware of the protocols these measures will establish. These protocols will likely inform the national standard of care by which data security management practices are judged, even in the private sector.

More recent legislative efforts have focused on information sharing, data-breach notification and cybercrime laws. Over 30 bills to address these areas were introduced at the beginning of the 114th Congress. Two bills HR 1560 and HR 1731 were combined and HR 1560 passed

the House of Representatives in late April, 2015. This measure is currently awaiting consideration in the Senate and is the most likely candidate to actually become law. HR 1560 contains measures that outline federal government conduct in data sharing communication between government and private institutions. HR 1560 further provides safe harbor provisions that protect private entities that share information on data breaches, limiting claims arising from the sharing of information in all cases except where willful misconduct can be demonstrated.

IN SUMMARY:

In 2015, over 30 bills to address information sharing, data-breach notification, and cybercrime laws were introduced to Congress.

Expect more Congressional hearings into cybersecurity challenges to government and industry throughout the remainder of 2015.

INFORMATION SECURITY AUDITS: PRECAUTIONS AND CONSIDERATIONS

by Michael Overly

Various forms of information security audits are used by organizations seeking to identify and remediate security vulnerabilities before, or as part of the recovery from, a cyber-attack. Penetration testing (or ethical hacking) is an important element of security audits. Below are important precautions and considerations for your organization before you start with a security audit:

- Consider whether to have the consultant engaged by legal counsel to maximize your ability to protect the audit and its results with the attorney-client privilege and under the attorney work product doctrine. Ask to review the report in draft form to make any changes before it is placed in final.
- Treat the audit agreement as any other professional services engagement. Ensure the work is clearly detailed in a well drafted statement of work and that all costs and fees are identified and appropriate cost controls are used. Beware of "scope creep" as the project progresses as new services may be added that significantly increase overall cost.
- Think carefully before permitting unannounced penetration tests. At least some coordination should be done to ensure the operation of critical systems is not disrupted during key operating hours or during month end processing.
- Don't permit the audit agreement to create more risk than it is intended to resolve. This means ensuring the auditor assumes an appropriate level of responsibility for confidentiality and information security. All too often, audit agreements include little to no language regarding obligations of the vendor with regard to information security and only trivial language regarding confidentiality. The vendor will have access to very sensitive business data and the exact details of how the business secures its systems. That information must be protected. That means strong security and confidentiality obligations, plus a level of liability that ensures the vendor will comply with those obligations. Beware of vendors that are unwilling to provide reasonable protection for this highly sensitive information.
- Review very carefully language in the agreement that permits the vendor to remove data from the customer's systems for offsite review. If such activity is permitted, the agreement should make clear the data cannot be made available outside the country (unless specific controls are employed), that the vendor cannot remove personally identifiable data that may be subject to specific laws or regulations without first committing to be bound by those laws and regulations (it is far better, however, to prohibit the vendor from removing such data in the first place, given its sensitivity), be wary of vendors that request possession of credit cardholder information (unless there is an express need for possession and the vendor is fully compliant with the Payment Card Industry Data Security Standard (PCI DSS).

ABOUT FOLEY

Foley & Lardner LLP provides award-winning business and legal insight to clients across the country and around the world. Our exceptional client service, value, and innovative technology are continually recognized by our clients and the legal industry. Foley has been recognized in a survey of *Fortune* 1000 corporate counsel as an elite BTI Client Service 30 — one of only seven law firms to hold this distinction for more than 12 years (2015 BTI Client Service A-Team survey, The BTI Consulting Group, Wellesley, MA). In addition, Foley received 27 national Tier 1 rankings in the 2015 edition of U.S. News – Best Lawyers® "Best Law Firms," and was named to the *InformationWeek* 500 list for seven of the past eight years for technological innovation that enhances business value. At Foley, we strive to create legal strategies that help you meet your needs today — and anticipate your challenges tomorrow.

TAKING CONTROL OF CYBERSECURITY: A PRACTICAL GUIDE FOR OFFICERS AND DIRECTORS

Get the white paper that has become a blueprint for managing information security and complying with today's evolving standard of care.

Download your complimentary copy at **Foley.com/TakingControl**.

EDITORS

Chanley T. Howell
Partner
Jacksonville, Florida
904.359.8745
chowell@foley.com

Michael R. Overly
Partner
Los Angeles, California
213.972.4533
moverly@foley.com

James R. Kalyvas
Partner
Los Angeles, California
213.972.4542
jkalyvas@foley.com