NADA NATIONAL AUTOMOBILE DEALERS ASSOCIATION

Hacking in the Automotive Industry

Michael Overly

Partner

Foley & Lardner LLP

Los Angeles, California

213.972.4533

moverly@foley.com

The views and opinions presented in this educational program and any accompanying handout material are those of the speakers, and do not necessarily represent the views or opinions of NADA. The speakers are not NADA representatives, and their presence on the program is not a NADA endorsement or sponsorship of the speaker or the speaker's company, product, or services.

Nothing that is presented during this educational program is intended as legal advice, and this program may not address all federal, state, or local regulatory or other legal issues raised by the subject matter it addresses. The purpose of the program is to help dealers improve the effectiveness of their business practices. The information presented is also not intended to urge or suggest that dealers adopt any specific practices or policies for their dealerships, nor is it intended to encourage concerted action among competitors or any other action on the part of dealers that would in any manner fix or stabilize the price or any element of the price of any good or service.

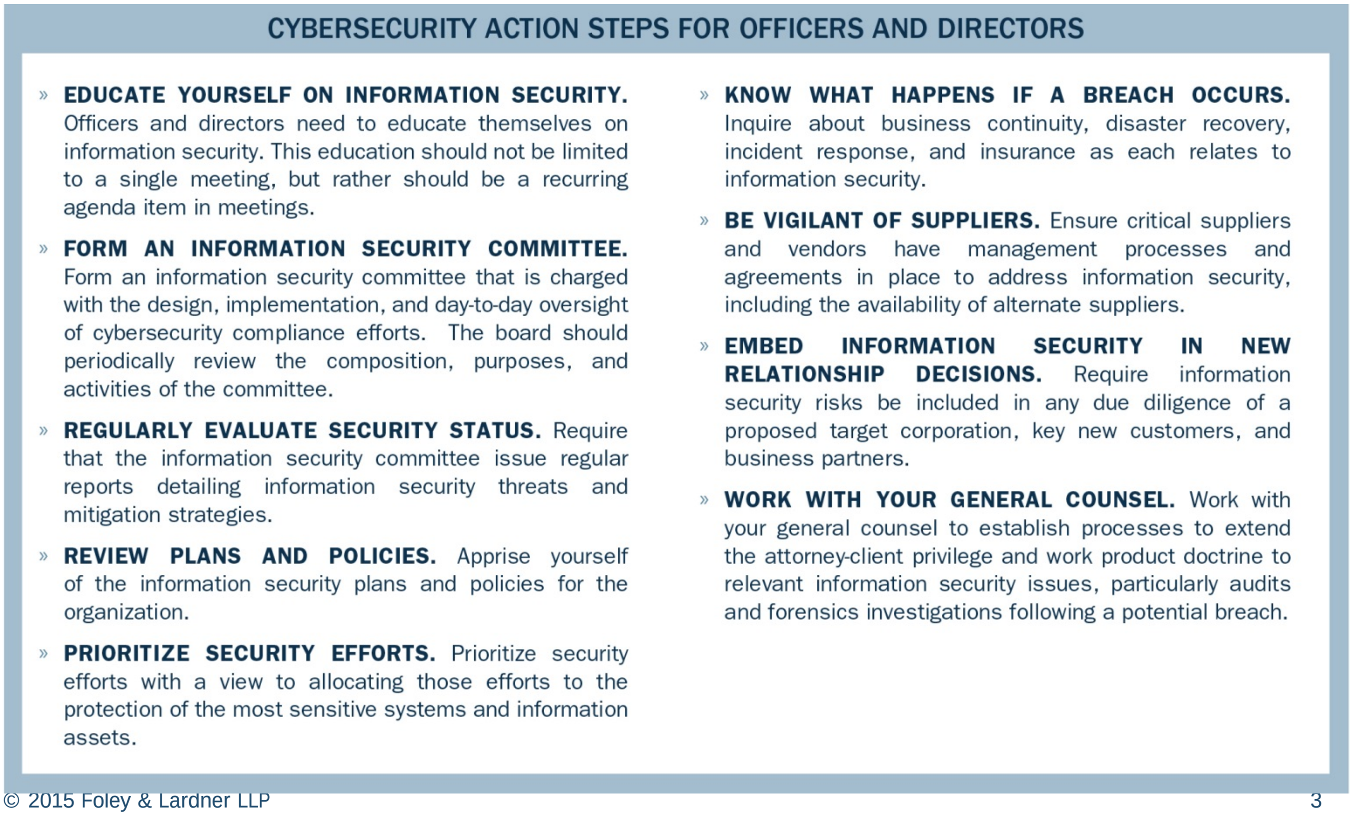
INTRODUCTION

Sony, Target, Westinghouse, Home Depot, U.S. Steel, Neiman Marcus, and the National Security Agency (NSA). The security breaches suffered by these and many other organizations, including most recently the consolidated attacks on banks around the world, combined with an 80 percent increase in attacks in just the last 12 months, have catapulted cybersecurity to the top of the list of priorities and responsibilities for senior executives and board members.

The devastating effects that a security breach can have on an enterprise, coupled with the bright global spotlight on the issue, have forever removed responsibility for data security from the sole province of the IT department and CIO. While most in leadership positions today recognize the elevated importance of data security risks in their organization, few understand what action should be taken to address these risks. This white paper explains and demystifies cybersecurity for senior management and directors by identifying the steps enterprises must take to address, mitigate, and respond to the risks associated with data security.

OFFICERS AND DIRECTORS ARE UNDER A LEGAL OBLIGATION TO INVOLVE THEMSELVES IN INFORMATION SECURITY

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 active role in establishing correct governance, management, and culture for addressing security in their organizations.

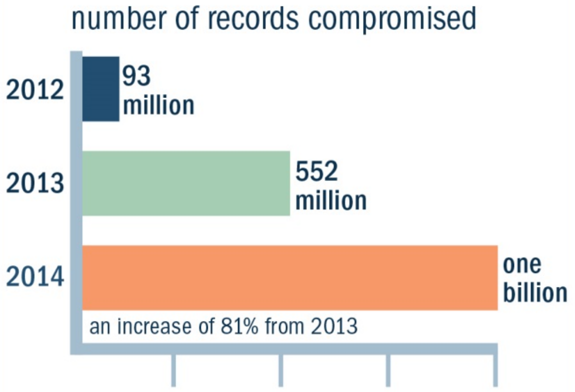


CYBERSECURITY ACTION STEPS FOR OFFICERS AND DIRECTORS

- **EDUCATE YOURSELF ON INFORMATION SECURITY.** Officers and directors need to educate themselves on information security. This education should not be limited to a single meeting, but rather should be a recurring agenda item in meetings.
- **FORM AN INFORMATION SECURITY COMMITTEE.** Form an information security committee that is charged with the design, implementation, and day-to-day oversight of cybersecurity compliance efforts. The board should periodically review the composition, purposes, and activities of the committee.
- **REGULARLY EVALUATE SECURITY STATUS.** Require that the information security committee issue regular reports detailing information security threats and mitigation strategies.
- **REVIEW PLANS AND POLICIES.** Apprise yourself of the information security plans and policies for the organization.
- **PRIORITIZE SECURITY EFFORTS.** Prioritize security efforts with a view to allocating those efforts to the protection of the most sensitive systems and information assets.
- **KNOW WHAT HAPPENS IF A BREACH OCCURS.** Inquire about business continuity, disaster recovery, incident response, and insurance as each relates to information security.
- **BE VIGILANT OF SUPPLIERS.** Ensure critical suppliers and vendors have management processes and agreements in place to address information security, including the availability of alternate suppliers.
- **EMBED INFORMATION SECURITY IN NEW RELATIONSHIP DECISIONS.** Require information security risks be included in any due diligence of a proposed target corporation, key new customers, and business partners.
- **WORK WITH YOUR GENERAL COUNSEL.** Work with your general counsel to establish processes to extend the attorney-client privilege and work product doctrine to relevant information security issues, particularly audits and forensics investigations following a potential breach.

CYBERSECURITY BY THE NUMBERS

DATA BREACHES GROWING EXPONENTIALLY[1]



IMPACT OF THEFT OF INTELLECTUAL PROPERTY[2]

in the U.S.

estimated annual cost

$200-250 billion

and 200,000 jobs

estimated annual cost up to

$538 billion

GLOBALLY

DISTRIBUTED DENIAL OF SERVICES ATTACKS[3]

average cost

$100,000 every hour

AGGREGATE DATA BREACH COSTS[4]

total cost to the global economy

$400 billion

(approximately 15-20% of the revenue due to the Internet lost)

average cost of a breach in the U.S.

$5.85 million

cost for each record compromised

$201

average decrease in net earnings in 4 quarters following breach

22%

13%

average reduction in analysts' earnings forecasts in 90 day period after breach compared to 90 day period prior to breach

[1] Steve Ragan, *Nearly a Billion Records Were Compromised in 2014*, CSO (Nov. 17, 2014) http://www.csoonline.com/article/2847269/business-continuity/nearly-a-billion-records-were-compromised-in-2014.html.

Internet Security Threat Report 2014 (2013 Trends, Volume 19) Symantec Corporation (2014) https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

[2] *Net Losses: Estimating the Global Cost of CyberCrime*, McAfee Center for Strategic and International Studies (2014) http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[3] Whitepaper, *DDoS Imposes $1M Hit on Website and e-Commerce Performance*, Neustar Market Pulse (2014) http://resources.idgenterprise.com/original/AST-0105410_NeustarMarketpulse.pdf.

[4] Research Report, *2014 Cost of Data Breach Study: Global Analysis*, Ponemon Institute (2014).

THE EVOLVING STANDARD OF CARE FOR INFORMATION SECURITY

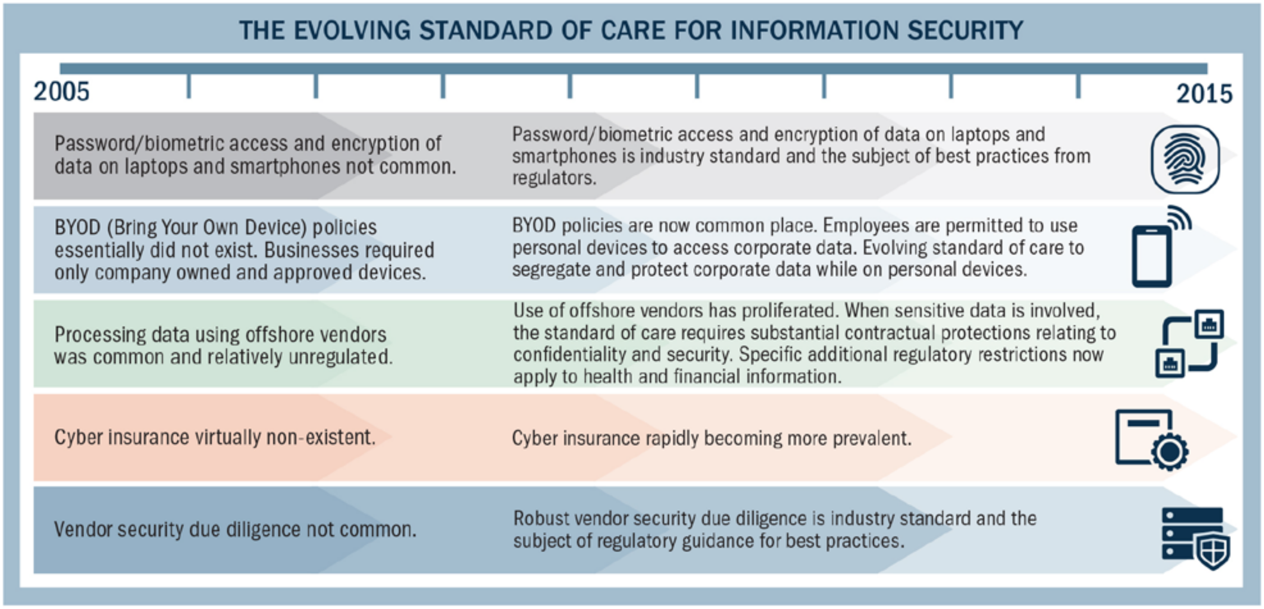
Every organization is exposed to information security threats daily.

It is essential for your organization to have an information security protection program that is properly designed, documented, executed, and updated to minimize exposure to information loss, disruption of operations, and liability to third parties and regulators.

> An overview of key information security concepts that every officer and director should be familiar with is attached as an appendix to this white paper.

The standard of reasonableness against which your information security program will be measured is not static — rather it is evolving to keep pace with the latest security threats and risks. The legal determination of whether your organization has conducted its information security program in conformance with the applicable standard of care will include an examination of the elements of your program to determine whether your organization has committed appropriate financial, technical, and human resources to its program, as both various new risks and protective strategies develop. Information security cannot be addressed as a one-time effort to develop and implement a comprehensive program, as well as supporting policies, that are then shelved; ongoing execution, monitoring, and reassessment are required. Third-party auditor reports (e.g., SOC 2® audit made under the AICPA Guide: *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*) can be valuable tools in assessing the security level of your own organization, as well as that of relevant business partners and vendors.

For example, an information security program implemented prior to 2011 that did not include a well-designed and executed vendor security due diligence approach may have met the applicable standard of care; but, subsequent to the many recent data breach events, that same approach may not be found to conform with the evolved standard of care resulting from those events.



THE EVOLVING STANDARD OF CARE FOR INFORMATION SECURITY

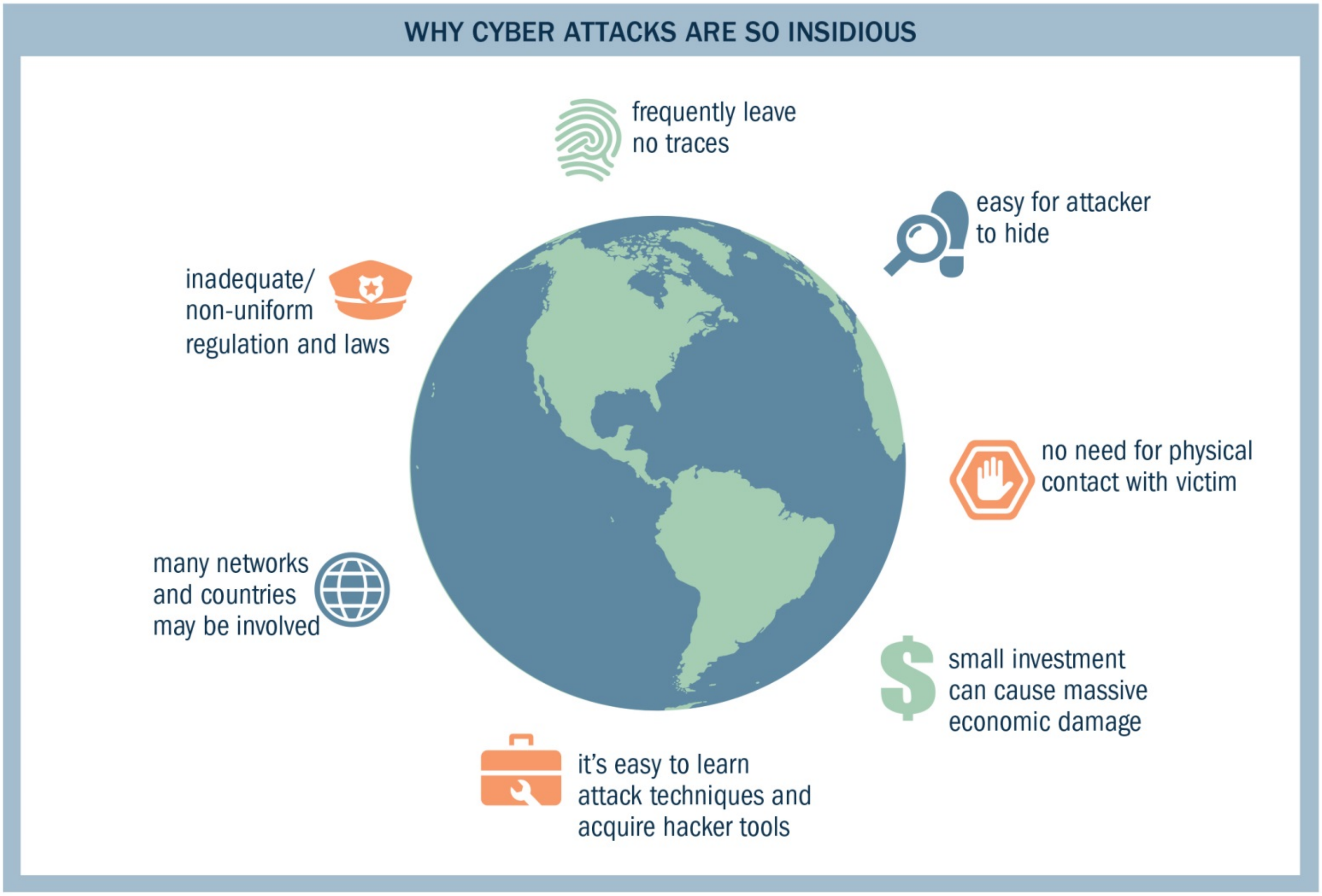
2005	2015
Password/biometric access and encryption of data on laptops and smartphones not common.	Password/biometric access and encryption of data on laptops and smartphones is industry standard and the subject of best practices from regulators.
BYOD (Bring Your Own Device) policies essentially did not exist. Businesses required only company owned and approved devices.	BYOD policies are now common place. Employees are permitted to use personal devices to access corporate data. Evolving standard of care to segregate and protect corporate data while on personal devices.
Processing data using offshore vendors was common and relatively unregulated.	Use of offshore vendors has proliferated. When sensitive data is involved, the standard of care requires substantial contractual protections relating to confidentiality and security. Specific additional regulatory restrictions now apply to health and financial information.
Cyber insurance virtually non-existent.	Cyber insurance rapidly becoming more prevalent.
Vendor security due diligence not common.	Robust vendor security due diligence is industry standard and the subject of regulatory guidance for best practices.

WHY ARE CYBER ATTACKS SO INSIDIOUS?

The risks presented by cyber-attacks are unlike any other that businesses typically encounter.

Anyone with a laptop, an Internet connection, and rudimentary hacking skills can reach out from anywhere in the world and cause dramatic harm to your business by disrupting operations, compromising your most sensitive data, or causing you to lose the confidence of your customers and business partners. To add insult to the injury, any one of the above can subject your business to regulatory scrutiny, fines, and sanctions.

Moreover, the attacker knows it will be almost impossible to identify him or her. Even if the attacker could be identified, he or she may reside in one of the many jurisdictions in which there are no specific cyber-crime laws. In any event, it is also highly probable that the attacker (unless a foreign government or competitor) has no assets to satisfy any judgment, even if one could be obtained. The high impact of cyber attacks and low risks to the attacker fuel the growth in attacks we are witnessing. The bottom line: If attacked, the likelihood that a business will have any real remedy against the culprit is very low.


WHY CYBER ATTACKS ARE SO INSIDIOUS

frequently leave no traces
easy for attacker to hide
inadequate/ non-uniform regulation and laws
no need for physical contact with victim
many networks and countries may be involved
small investment can cause massive economic damage
it's easy to learn attack techniques and acquire hacker tools

COMMON SECURITY MYTHS

One of the greatest challenges for organizations attempting to address cybersecurity risks is the number of fundamental myths that exist about security. Those myths cause organizations to incorrectly assess threats, misallocate resources, and set inappropriate goals. Dispelling those myths is key to developing a sophisticated, appropriate approach to information security.

MYTH #1: "IT'S ALL ABOUT THE DATA."

All too frequently, "security" is thought of as ensuring data cannot be accessed or used for unauthorized purposes or by unauthorized users. While this is certainly a key concern, the systems and networks on which the data reside must also be protected against attack. For example, a denial of services attack (DOS attack) is not aimed at gaining access to a business' sensitive data, but at preventing others, such as customers and business partners, from accessing and using that data.

MYTH #2: "IT'S ALL ABOUT PRIVACY."

Another common misconception is that security relates only to the protection of personally identifiable information. While the protection of personal information is clearly of critical importance, other types of information assets must also be protected. Additional information assets include trade secrets and other intellectual property (such as source code for a company's software products), competitive information (such as customer and supplier lists), pricing and marketing data, company financial information, and more.

MYTH #3: "IT'S ALL ABOUT CONFIDENTIALITY."

When talking about security, the tendency is to focus on the most obvious element: ensuring data is held in confidence (i.e., the data is not used by unauthorized individuals or for unauthorized purposes). For data to be truly secure, it must be confidential, the integrity of the data must be maintained, and it must be available when needed. These are the three prongs of the well-known information security acronym "CIA."

"Confidentiality" means the data is protected from unauthorized access and disclosure. "Integrity" means the data can be relied upon as accurate, and that it has not been subject to unauthorized alteration. Finally, "availability" means the data is available for access and use when required. It does no good to have data that is confidential and the integrity maintained, but the data is not actually available when a user requires it. To achieve this last requirement, the systems on which the data resides must have specific service levels for availability, response time, and more. This is particularly important when a third-party vendor may be hosting the data for the benefit of the business.

MYTH #4: "TO BE A HACKER, YOU MUST BE A TECHNOLOGICAL GENIUS."

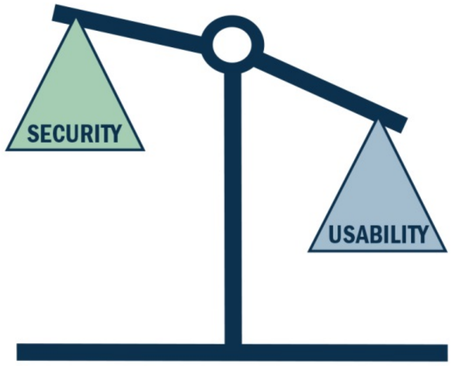
It is a common error for businesses to focus their security measures on the professional hacker. That is, your security measures are designed to protect against individuals or entities that are highly skilled in programming and technology. Such skills are, however, no longer a pre-requisite to hacking activities. Today, someone with little or no knowledge of technology can find online, easy-to-use hacking tools capable of causing substantial harm to a business. These individuals are sometimes referred to in the hacking community as "script kiddies" because they require no real hacking knowledge. There are also a wide range of readily available books that can quickly educate even technological neophytes regarding hacking.

Finally, one of the most effective means of hacking in use today — social engineering — requires no technological skills whatsoever. Rather, to be an effective social engineer, all that is required is self-assurance and a knowledge of human nature. One prevalent form of social engineering is phishing — a hacker sending fake emails soliciting sensitive information or including attachments that install malware that can infect a company's network. Phishing attacks and other social engineering techniques were used recently to conduct a concerted attack on banking institutions worldwide, causing losses of $300 million — or possibly as high as $1 billion.

MYTH #5: "I CAN ACHIEVE 100 PERCENT SECURITY."

Finally, one of the most common misconceptions about security is that complete security can be achieved or that complete security is required by law or industry practice. Neither is correct. Both laws and industry practices require businesses to do what is "reasonable." Complete security is not required or even a realistic goal. Studies show that it would require businesses to increase their overall security budgets nine-fold to address just 95 percent of the threats. That increase would, in most cases, exceed the overall budget for the entire business. In addition, there is a fundamental paradox with regard to security efforts: As security protections are increased, usability of the secured systems decreases. That is, the greater the security, the less useful the thing secured will be.

BALANCING SECURITY AND USABILITY



As security protections are increased, usability of the secured systems decreases and vice-versa.

KEY ELEMENTS TO A CYBERSECURITY COMPLIANCE AND RISK MANAGEMENT PROGRAM

An effective cybersecurity risk management program requires an effective governance structure based on the organization's risk appetite — just like the company would create for any other material risk.

A key success factor to your program will include engaging management with security risk, and producing information risk management policies and procedures. While the components of a cybersecurity risk management program may vary from organization to organization, certain key elements are generally common to all effective programs. The following is a list of the 10 key elements and a set of checklists of important considerations as to each element.

10 KEY ELEMENTS OF A CYBERSECURITY RISK MANAGEMENT PROGRAM

1 INCIDENT MANAGEMENT

2 USER EDUCATION AND AWARENESS

3 MANAGING USER PRIVILEGES

4 HOME AND MOBILE WORKING

5 REMOVABLE MEDIA CONTROLS

6 MALWARE PROTECTION

7 MONITORING

8 SECURE CONFIGURATION

9 NETWORK SECURITY

10 CYBERSECURITY INSURANCE

1 INCIDENT MANAGEMENT CHECKLIST

"Incident Management" refers to people, processes, and technologies triggered by a security breach to resolve the breach and mitigate risk.

☐Does your company have an established multi-disciplinary incident response team, comprised of personnel from information security, compliance, legal, corporate communications, and relevant managers?

☐Does your company have an established incident response policy describing the actions to be taken, by whom, and in what order in the event of a breach?

☐Does your company have pre-established relationships with potentially key outside vendors, who may be required to assist in investigating and resolving a security incident, for example, information security consultants and computer forensics experts?

☐Does your company include language in its vendor agreements, requiring the vendor to promptly report potential incidents, cooperate in investigating the incident, preserve relevant evidence, and so forth?

☐Does your company have backup/disaster recovery/business continuity plans in place to minimize the impact of an incident causing a system outage or data loss?

☐Does your company periodically (at least once a year) test its incident response, backup, and disaster recovery policies and procedures?

☐Are procedures in place, coordinated with general counsel or outside counsel, to ensure relevant investigative activities are subject to the attorney-client privilege or work-product doctrine?

2 USER EDUCATION AND AWARENESS CHECKLIST

□Are company security policies and procedures written in plain English, capable of being understood by all relevant employees? Consider developing summaries of all policies for easier review and understanding by employees.

□Are employees trained regarding corporate information security policies and practices? Training should be conducted on initial hire; when an employee's position or duties change so as to alter their access to sensitive systems and data; on an ongoing basis to reinforce key obligations and address significant changes in policies or procedures; and on termination to ensure all information assets are returned to the company and to emphasize the employee's continuing obligations to hold information assets in confidence.

□Does your company conduct activities to heighten employee awareness of significant ongoing threats, such as viruses contained in email attachments, and any newly identified threats, including new forms of social engineering? Previously, phishing was used by a large group of hackers stealing a total of $300 million to $1 billion from numerous banks around the world.

3 MANAGING USER PRIVILEGES CHECKLIST

"User privileges" refers to the rights users are granted in accessing systems and data. The well-known security principle of "least privilege" requires that users be granted only the level of access necessary for them to conduct their jobs, but nothing more. For example, a worker in the mailroom would not be granted computer access to payroll records.

□Do your company security policies and procedures include the principle of least privilege in granting user access rights?

□Are accounts with broad access rights limited to individuals that truly require them?

□Are audits and reviews performed on a periodic basis to re-assess the rights and privileges granted users? All too often, a user's duties may change, and they no longer require access to data previously granted to them. In those cases, the user's access rights should be altered to prevent further access to that data.

□Do you require your employees to sign confidentiality agreements or otherwise acknowledge their confidentiality obligations to the company?

□Do your company security policies and procedures ensure user access rights are limited, suspended, or terminated when a user is the subject of investigation for wrongdoing or is notified their employment may be terminated?

□Does your company conduct appropriate background screening for employees and contractors with access to sensitive information and systems?

□Do you conduct appropriate data security due diligence for vendors that will have access to company confidential information or personal information?

□Do you have appropriate contractual protections in place in agreements with vendors that will have access to company confidential information or personal information?

4 HOME AND MOBILE WORKING CHECKLIST

☐Has the appropriateness of having a home or mobile working program (sometimes called a "Bring Your Own Device" or "BYOD" program) for your organization been assessed?

☐Have all stakeholders within the company been consulted in creating the policy, including human resources, compliance, information security, legal, relevant managers?

☐Have any regulatory obligations been identified that would impact implementation of a BYOD program, such as regulatory guidance limiting use of removable media with personal information stored on them?

☐Has the company developed a clear and detailed BYOD policy regarding its expectations and the obligations of participating employees?

☐Have employees been properly trained regarding the BYOD policy and their obligations to uphold your company's security standards in using home and mobile devices?

☐Does your company require encryption of company data on laptops, smartphones, tablets and other mobile devices, as well as backups of data stored off-site?

5 REMOVABLE MEDIA CONTROLS CHECKLIST

"Removable media" refers to USB (thumb) drives, memory cards (e.g., secure digital (SD) cards), recordable DVDs, CD ROMs, removable hard disks, the use of smartphones and tablets on to which company information may be transferred, and so forth. This media may be capable of storing dozens, even hundreds, of gigabytes of information, such as hundreds of thousands of pages of information. Since this type of media is generally small and easily transportable, there is a constant risk the media may be lost, not properly erased after use, or used by a malicious employee to misappropriate company proprietary information.

☐Is your company a regulated entity, such as a financial services company, subject to regulatory guidance against use of removable media?

☐Does your company have specific policies about use of removable media? Common areas addressed in these policies include:

- ☐Has your company considered disabling USB and other connections on desktop and laptop computers to prevent use of unauthorized removable media?
- ☐Does your company address removable media controls in vendor contracts in which a vendor will have access to highly sensitive company data?
- ☐Does your company have a policy for securely destroying removable media that is no longer in service?

6 MALWARE PROTECTION CHECKLIST

□Does your company have industry standard anti-virus/malware software installed on its systems? Is that software continuously updated to reflect the latest virus databases, signatures, and more?

□Has your company trained users to avoid high-risk activities that may give rise to virus transmission, including clicking on attachments or hyperlinks in email from unknown third parties, installing software from vendors the company has not specifically approved, or connecting non-company supplied removable media to company systems?

□Do company security policies address anti-virus/malware, including use of appropriate protections in BYOD programs?

7 MONITORING CHECKLIST

□Does your company have an established policy and associated procedures to monitor access to and use of its systems and data?

□Has your company deployed technologies (e.g., intrusion detection systems) to effectuate those policies?

□Does your company ensure that the log files created by monitoring technologies are not subject to modification? For example, the log files must be protected to prevent a hacker from erasing his tracks.

□Are the log files and other information generated by the monitoring procedures reviewed, either by individuals or other technologies, to identify potential threats?

8 SECURE CONFIGURATION CHECKLIST

□Does your company have a current inventory of all key information assets, systems, networks, and related technologies?

□Does your company subscribe to and monitor notifications to the United States Computer Emergency Readiness Team (US-CERT) or similar service, vendor notifications, and other recognized sources of information for critical patches to software?

□Does your company have an encryption policy addressing encryption of sensitive data as required by law or otherwise dictated by industry standards and risk assessments?

□Does your company have a process to fix or patch identified security problems in an adequate and timely manner?

□Do company security policies address secure configuration activities, such as changing default passwords in software and hardware, removal of outdated and insecure technologies, and the other areas described in this section?

□Does your company dispose of computers, laptops, hard drives, removable media and other storage media in a secure manner, so as to avoid unauthorized access to data on hardware no longer used by the company?

9 NETWORK SECURITY CHECKLIST

□Do company security policies and procedures address protection of its networks from both internal and external attack, including use of firewalls and malware detection technology?

□Does your company promptly install all updates and patches to its operating system software and all security-related software?

□Do you regularly (no less than annually) conduct penetration testing to assess the strength of your network protection against external attacks?

□Are corporate wireless networks secured using industry best practices, for example, changing default router passwords, avoidance of insecure encryption protocols like Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA), firewalls, and not broadcasting its Service Set Identifier (SSID)?

□Are network perimeter defenses configured to filter or block suspicious access or activities?

□Are network servers and other network components protected physically through use of secure and locked facilities?

10 CYBERSECURITY INSURANCE CHECKLIST

□Does your company have cybersecurity insurance that protects it against security incidents, including hacking, viruses, data theft, and inadvertent loss of personal information? Most general commercial liability policies either contain express exclusions or will not cover security incidents.

□If you have cybersecurity insurance, are you in full compliance with the requirements of the policy? Some policies require a baseline level of data security to be implemented and maintained within the organization.

□Does your vendor due diligence and contracting process ensure vendors that handle your information assets have adequate cybersecurity insurance?

YOUR INFORMATION SECURITY POLICY LIBRARY

As noted throughout the checklists above, a critical element of your organization's information security program is to have appropriate written policies in place.

The following identifies the most critical policies your company should consider as part of its security compliance program.

1 INFORMATION SECURITY POLICY

Typically, the core policy for the information security program is a detailed information security policy, addressing a number of different security issues and directed primarily to the information security team. These issues may be dealt with in a single policy or divided into smaller sub-policies; but each of these issues should be addressed in a written policy.

» Access control
» Establishing network connection
» Password management
» Encryption
» Viruses, malicious software, and change control
» Perimeter firewall management and protection
» External network connections
» Software updates and patch management
» Disposal of data, devices, storage media, and other hardware containing information
» Network security management
» Log management and monitoring
» Password management
» Physical security
» Remote access to company network
» Wireless network security

2 ACCEPTABLE USE OF ASSETS POLICY

This policy addresses employee use of information systems, networks, email, Internet access, and more.

3 BACKUP, DISASTER RECOVERY, AND BUSINESS CONTINUITY

This policy provides procedures for backing up company data and recovering from an outage, data loss, disaster, or other disruption of information technology services or infrastructure.

4 HOME AND MOBILE COMPUTING

This policy addresses employee use of home computers and mobile devices (employee-owned and company-owned).

5 BRING YOUR OWN DEVICE (BYOD) POLICY

This policy addresses employee use of employee-owned devices used to perform company business.

6 EMPLOYEE EDUCATION AND TRAINING

These policies and procedures address the education and training materials for employees.

7 SECURITY INCIDENT REPORTING AND RESPONSE POLICY

These policies address the procedures for preparing for, recovering from, and responding to a security incident, such as a data security breach, resulting in the misappropriation of company information or consumer personal information.

8 SOCIAL MEDIA ACCEPTABLE USE POLICY

This policy addresses employee use of social media for company business purposes and when using company systems.

9 VENDOR DUE DILIGENCE AND CONTRACTING

This policy addresses procedures for conducting due diligence on and contracting with vendors that will have access to the company's information assets.

CONCLUSION AND KEY TAKEAWAYS

To comply with their fiduciary duties, senior officers and directors must take an active role in the implementation and management of your organization’s information security program.

The evolving standard of care requires continued diligence and attention to data security safeguards and policies utilized by your organization. The steps and action items described above will assist officers and directors in keeping up with this evolving standard of care, including:

- Senior management educating themselves on the fundamentals of information security.
- Establishing an information security committee subject to board oversight and review.
- Senior management keeping informed of the information security plans and policies for your organization.
- Prioritizing security efforts by allocating resources based on the potential likelihood and magnitude of risk of loss, and implementing safeguards for the most sensitive systems and information assets.
- Delegating authority and providing company resources for the implementation of the key elements of the enterprise’s information security program.
- Overseeing the development of written policies and documentation to support the information security program.
- Periodically reassess your company’s cybersecurity program through regular reviews and meetings with decision makers and stakeholders.

APPENDIX – KEY INFORMATION SECURITY CONCEPTS

ENCRYPTION

Encryption is a critical aspect of any data security program. Encryption is the process of scrambling data using a computer algorithm so that the data cannot be read without having the "key" to decipher or unlock the encrypted data. As encryption has become more feasible, affordable, and ubiquitous, it has become both a legal and industry standard for protection of sensitive information. For example, regulatory guidance for the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach Bliley Act (GLBA), Massachusetts state law, and Nevada state law all contain encryption requirements for sensitive information under certain conditions. The Payment Card Industry Data Security Standards (PCI DSS) require encryption of credit card information.

The security afforded by encryption is based on "time." That is, how long would it take using readily available current technology, working 24 hours a day, to crack the encryption. For most strong methods of encryption, this "brute force" method of cracking is measured, at minimum, in terms of years and, more commonly, in terms of decades. The problem is that technology is constantly evolving. The power of the most sophisticated desktop computer of just a few years ago can now be found in a wristwatch. As the power of readily available computers increases, encryption methods thought to be secure are now unsecure. This is why the type and strength of encryption used to protect data must be periodically reviewed and updated.

Even when not legally required, encryption provides important liability protections. For example, HIPAA exempts health care organizations from data breach notification obligations in the event that electronically stored health information is encrypted using industry standard techniques. Similarly, state laws that require notification of security breaches to consumers and attorneys general provide an exception if the data is encrypted.

Many people confuse password protection and encryption. For example, while it is possible to require a password to access a device or open a file, it does not necessarily mean the data on the device or in the file is encrypted. Data on a laptop that is password-protected without encryption can be accessed relatively easily, using widely available computer forensics tools. Because the data is not encrypted it can still be read. Thus, in order to protect data on a laptop or other mobile device, it should be encrypted.

The encryption can be at the "file level" or the "disk level." File level means the data is encrypted on a file-by-file basis. Some files may be encrypted, while others are not. Encryption at the disk level means all data on the entire hard drive of the device is encrypted. Disk encryption is the industry standard when encrypting data on a laptop, smartphone, or other mobile device or storage media.

FIREWALLS

A firewall is a software and/or hardware solution that protects a company's network from unauthorized access from outside networks, for example, hacking attempts from the Internet. The firewall is configured to block access from certain sources, such as known bad actors and certain content, including known viruses and malware that can be used to infiltrate a company's network. The firewall software is continuously updated to block known malicious sources and content.

INTRUSION DETECTION SYSTEMS

Similar in function to a firewall, an intrusion detection system monitors network activity within the organization (behind the firewall), while a firewall looks outward to prevent intrusions. For example, an intrusion detection system can be configured to trigger an alarm if certain type of network traffic or activity matches a library of known attacks. It can also trigger an alarm if certain critical files are modified or deleted. Finally, the intrusion detection system can provide an alert if the network activity is not "normal," such as a higher or different type of activity.

ACCESS CONTROLS

Access controls establish limits and restrictions on which employees can access what data and systems. Companies should implement the concept of "least privilege," which is the principle that employees and other individuals should be granted the least amount of privilege — or access rights — necessary for the individual to do his or her job. This mitigates the risks associated with accidents, mistakes, intentional misconduct, and unauthorized use of an individual's access credentials. Although this security principle has been around at least since the 1970s, many organizations do not properly implement restrictions on network access rights.

PENETRATION TESTING

Penetration testing is the practice of hiring an outside consultant to test the strength and vulnerabilities of a company's network with respect to attacks from outside of the network. Systems are constantly changing, meaning a system that is relatively secure one month may not be as secure the next. Periodic penetration is required under the Payment Card Industry Data Security Standards for companies that process credit card information. Penetration testing every six months, or at least annually, is an important step in keeping a company's network secure against outside hacking attacks.

PHISHING/SPEAR PHISHING

"Phishing" refers to a social engineering technique in which a perpetrator sends out communications, typically in the form of email, that appear to be from a reputable source (e.g., a well-known bank, broker-dealer, or department store). Unsuspecting recipients are lured into responding to the communication by disclosing their personal information, account access codes, or other sensitive information. In addition, the communications may contain innocuous looking hyperlinks that are, in fact, means of downloading viruses to the recipient's computer. Phishing generally involves sending the same communication to a large number of recipients with the hope that a subset will be lured into responding. In contrast, "spear phishing" refers to the more sophisticated practice of using publicly available information gleaned from social media, corporate websites, and other sources to specifically tailor communications to target an individual. Spear phishing is more time intensive for the perpetrator, but more likely to bear fruit. Corporate executives are frequent targets of spear phishing. In fact, executives in businesses with more than 2,500 employees stand a 1 in 2.3 chance of receiving a spear phishing attack.[5]

NETWORK SEGMENTATION

Risks to highly sensitive data (for example, credit card information, Social Security numbers, trade secrets, and intellectual property) can be mitigated by separating the data from less secure networks and systems that can be accessed through the Internet. For example, a server that contains sensitive employee information, such as Social Security numbers, can be segregated from servers that can be accessed by the public from the Internet.

VENDOR DUE DILIGENCE

More and more companies are providing outside vendors and business partners with access to company networks for purposes of exchanging data. The vendor's network then, in essence, becomes an extension of the company's network. If the vendor has weak security, the vendor's network can be breached and then used to enter the company's network. The source of the Target security breach originated through a refrigeration, heating, and air conditioning subcontractor that had access to Target's network. Effective vendor due diligence and periodic auditing (or audit reporting requirements) can mitigate these risks.

[5] *Internet Security Threat Report 2014* (2013 Trends, Volume 19), Symantec Corporation (2014) http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

AN INDIVIDUAL'S INFORMATION SECURITY CHECKLIST

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.).

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, SkypeTM, 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, CarboniteTM, 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.

ABOUT THE AUTHOR

Michael Overly
Partner, Foley & Lardner LLP
213.972.4533
moverly@foley.com

Michael Overly is a partner and intellectual property lawyer with Foley & Lardner LLP, where he focuses on drafting and negotiating technology related agreements, software licenses, hardware acquisition, development, disaster recovery, outsourcing agreements, information security agreements, e-commerce agreements, and technology use policies. He counsels clients in the areas of technology acquisition, information security, electronic commerce, and online law. Mr. Overly is a member of the Technology Transactions & Outsourcing and Privacy, Security & Information Management Practices.