Cybersecurity Programs – A Guide

By: Linda Lerner, Maida Lerner, Harvey Rishikof, and Jenny E. Cieplak
June 2016

Cybersecurity has been identified as the issue that most keeps corporate management and their IT, legal and compliance teams, as well as many government regulators, up at night. The time for considering whether to have a cybersecurity plan in place is long over; those plans should be in place and reviewed at least annually for their adequacy in light of current developments in federal and state governmental regulation, technology and in the types of cyberattacks being perpetrated. Companies with inadequate cybersecurity protections risk:

- Reputational harm.
- Monetary sanctions for exposing personal identifying information (PII) and personal health information (PHI) of their clients (whether retail customers or patients) and employees/applicants.
- Exposing confidential enterprise operational and business information of the company and/or its customers.
- Bringing the company's operations to a halt when ransomware infections have enabled hackers to hold the systems hostage or other types of attacks, such as Distributed Denial of Service (DDOS), impede operations. This has been particularly troublesome in the healthcare industry, where patient care may be compromised.

In addition to federal law protections and regulatory and self-regulatory rules, applicable state laws require the protection of PII and PHI. EU privacy laws govern PII transferred into the United States. Finally, a company's cybersecurity insurer may impose procedural and testing requirements as a prerequisite to underwriting that insurance.

It is critical for entities that utilize automated systems for any functionality to have a program of risk analysis and oversight for those systems to identify and minimize sources of operational risk and data loss. Companies should conduct regular, periodic and objective testing and review of automated systems to ensure their reliability, secure nature and scalability and should adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer and corporate records and information.

What Does a Robust Cybersecurity Program Include?

Risk Assessment

The company should form a Risk Analysis Committee to perform this task. Factors to be considered by the Committee include:

- Inventory of hardware with data connectivity, data transmission or data storage capability.
- Inventory of critical software and version in use.
- Policies and procedures that ensure prompt installation of software patches and upgrades.
- Inventory of types of data collected, maintained and/or disseminated, who controls it, who has access to it, and how is it transmitted and to whom.

- Internal and external threats and vulnerabilities to at-risk data, including customer and counterparty PII, corporate records and financial information.
- Threats and vulnerability of electronic infrastructure, including systems used to initiate, authorize, record, process and report financial transactions, strategic plans, key corporate documents, and risk management.
- Threats posed by third party vendors and awareness of the devices connected to their networks and network structure; threats posed by fourth party vendors (a third party vendor's vendors) are equally important.
- Understanding of the nature of the threats, including: data loss (including data at rest and interception and compromise of data in transit); loss, destruction or theft of hardware containing at-risk data; and insertion of viruses, spyware and other malware. Threats may include natural disasters, human errors and malicious attacks.
- Prioritization of threats as to possible severity, vulnerability level and past incidents. Threats identified by the firm's outside vendors (or their vendors) should also be considered.
- Deployment of protective measures.
- Physical access restrictions.
- User authentication (complex, frequently changing passwords, multiple authentication modes).
- Systems access controls (least necessary).
- Use of network segmentation.
- Use of secure development practices for internally developed software.
- Selection of storage media.
- Use of and timely patching of anti-virus and firewall technology and other software.
- Use of approved software; prohibition against using unsupported software (whitelists and blacklists).
- Web filtering to block access to inappropriate or malicious websites.
- Testing, including: controls testing; enterprise technology risk assessment; vulnerability testing; penetration testing; security incident response plan testing; and enterprise risk technology testing.
- Regular system and data backup for disaster recovery.
- Documentation of threat detection measures, such as network monitoring software, monitoring for physical intrusions.
- Secure disposal of data and hardware on which data is stored.
- Due diligence on vendors and employees.
- Joining organizations to share threat information, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), the US Computer Emergency Readiness Team, Department of Homeland Security's Cyber Information Sharing and Collaboration Program, FBI's Infraguard, and the Department of Energy's Cybersecurity Risk Information Sharing Program.
- Encryption of data at rest and in transit.
- Ensuring that mobile devices are equally protected.
- Establishing relations with law enforcement and government officials.

Incident Response Plan

Every company can expect to experience a cybersecurity incident. When that incident arises, a response plan should already be in place; the time of the incident is not the time to plan the response. The incident response plan should cover, at a minimum, roles and responsibilities for individuals tasked with responding to and mitigating the incident, the restoration of software and hardware, paths of communication with stakeholders and regulatory authorities, and a review of the cybersecurity plan in light of the incident. The details are critical – who will restore software and hardware, are alternates available, does the company have an alternate, independent warm or hot site, how long will it take to get up and running in various scenarios, which attorney to call and should outside counsel be engaged, should an independent forensic consultant be engaged, should an outside PR firm be engaged, and in each case, that entity and its contact person and information identified. All of these issues should be decided in advance and reviewed periodically. Tabletop exercises are especially helpful in ensuring that the responsible individuals understand the escalation process and that processes set out in an incident response plan flow smoothly.

Employee Training and Background Checks

Employee training is a key component of an adequate cybersecurity plan. Some in the field believe that a substantial cause of incidents is due to human carelessness – whether it is opening a phishing email, neglecting to immediately terminate system access of a terminated employee, failure to install a patch or many other simple human errors. Vendors with effective, user friendly educational tools attend or sponsor many cybersecurity conferences.

Cyber incidents may be caused not by employee error but by employees acting with malicious intent. Thus, it is important to conduct background checks where permitted, to ensure that access is terminated when an employee no longer needs such access, and that two-factor authentication is used so that employees cannot share login credentials.

Contractual Relations With Vendors

Cybersecurity requirements for vendors should be set forth in each contract with any vendor that will be providing information systems or that will otherwise have access to sensitive information. Those contracts should include a provision requiring the third party vendor to impose the same requirements on its service providers that the company imposes on its third party vendor. A firm's cybersecurity implementation procedures should provide a way to verify compliance by third and fourth party vendors, whether through access to testing results or audit rights.

Stakeholders to Be Involved in Developing and Reviewing the Cybersecurity Plan

Senior management must be involved in and approve each aspect of the company's cybersecurity plan so that cybersecurity is recognized company-wide as a priority governance issue and because management ultimately must approve the budget for what can become a significant expense. A company should designate a knowledgeable individual as the Chief Information Security Officer (CISO), senior management should be included in the initial meeting and in at least the final meeting to approve the overall cybersecurity plan. Other parties that are critical to this process are IT, the affected business units, back office, risk management, internal audit, HR, compliance and legal. Finally, the involvement of the company's board of directors is very important; a lack of board involvement may be viewed as a breach of the board's fiduciary duty. As a best practice, the firm's management (whether a designated Risk Management Committee or group that has been delegated this task) should report to the board no less than annually, and preferably quarterly.

Independent Testing

It is important to conduct independent testing so that the company's board and executive management, as well as the Chief Information Security Officer, the head of IT and/or any other staff managing the process may receive independent perspectives. Vulnerability testing, external and internal penetration testing, controls testing, incident response plan testing and enterprise technology risk assessment should be conducted by persons who are not responsible for development or operation of the systems or capabilities being tested, but that person may be internal or external, depending on the severity of the risk, applicable regulatory requirements and industry best practices. The frequency of such testing should be guided by those same factors. The board of directors and senior management should receive and review reports setting forth the results of all testing and assessment.

Resources

- The National Institute of Standards and Technology (NIST) has published a Framework for Improving Critical Infrastructure Cybersecurity. The Framework recommends testing detection processes and procedures as well as response and recovery plans.
- The Financial Industry Regulatory Authority (FINRA), which regulates securities broker-dealers, published a Report on Cybersecurity Practices in February 2015. It contains a robust framework for drafting procedures and has a list of standards and best practices reference materials.
- On May 23, 2016, FINRA published a Checklist for Cybersecurity based on the NIST Framework that is a very useful tool for ensuring that necessary areas are covered.
- The Federal Information Security Management Act (FISMA) requires governmental agencies to evaluate and test systems annually.
- The Council for Cybersecurity's Critical Security Controls for Effective Cyber Defense recommends tabletop exercises and penetration testing, as well as continuous scanning for vulnerabilities.
- The Federal Financial Institutions Examination Council (FFIEC) stresses the importance of independent testing—i.e., testing independent of the person controlling the function being tested.
- Most of these resources are also reviewed in a recent CFTC Rule Proposal published in the Federal Register on December 23, 2015 (Vol. 80, No. 246 at page 80114).
- SANS Institute's Critical Security Controls for Effective Cyber Defense and an Effective IT Security Plan: http://www.sans.org.
- Open Web Application Security Project's guidance: http://www.owasp.org.
- ISACA Control Objectives for Information and Related Technology: http://www.isaca.org.
- The FCC's Small Biz Cyber Planning Guide is broad-ranging and very useful.