Berkleylifesciences
a W. R. Berkley Company

"Am I at-risk for a cyber-security breach?"

This is a question many life science companies have been asking themselves over the past couple of years as more data breaches are in the news. Even the federal government is at risk: in 2012, the United States Food and Drug Administration (FDA) detected a breach of their information systems that resulted in the theft of personal information included by life science companies in their product submissions.[1] The FDA quickly made the necessary adjustments but the submitting life sciences companies were concerned that the cyber criminals were after more than just personal information and were looking for data on clinical trials, intellectual property or more. The FDA defines cyber security as the "process of preventing unauthorized modification, misuse, or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient." [2]

This paper, which will be the first in a series, provides a foundation of why cyber security is important to a life sciences company, what particular security vulnerabilities are important to these companies, and the practices that every life science company should undertake to protect themselves from cyber criminals.

Overview of Life Sciences Industry and Cyber Security

The life sciences industry is attractive to cyber security breaches due to the sensitive digital information that is seen as valuable to cyber criminals. This information can be patients' personal information, intellectual property or more. So, what makes a life sciences company vulnerable to breaches? Some common vulnerability within the life sciences industry are the lack of policies and procedures around information technology, lack of protection around the data stored, and the outsourcing of information technology services. These vulnerabilities can lead to cyber security breaches to the digital information network of the life sciences company. The digital information network can be any of the networks within a company's control that stores their digital information. These vulnerabilities can be exploited by either having an uncontrolled point within the digital network, the evolution of technology and lack of software updates, or through a device that is tied to the digital network.

Cybercriminals come in a variety of different types but there are four main categories:

1. Nuisance cyber criminals who want to interfere with a company's daily business operations.
2. State sponsored cyber criminals that are principally interested in trade secrets and confidential company information as a form of espionage for their country state.
3. 'Hacktivists' who are interested in making a political statement to stop a life science company from conducting a particular activity.
4. Cyber criminals who can be insiders or third party vendors that have access to the information and want to make a profit from the personal information.

As an example of what a cyber-criminal can do is that they can both lock down critical data such as research and clinical data so that it cannot be accessed, or that they could release the data publically which can be detrimental to items such as a regulatory filing.

Understanding the vulnerabilities

Understanding their own cyber vulnerabilities along with cyber criminals' motivations will help a life sciences company create a plan to protect against a cyber-attack. First, a life sciences company needs to understand where their particular vulnerabilities are located. Below are a series of questions about the digital information network that a company can consider to see where these vulnerabilities may be:

1. Does your organization collect, store, or process personally identifiable or other confidential information, such as financial data or intellectual property?

2. Is this information safeguarded through policies and procedures? Are your employees trained on these procedures?
3. Does your organization conduct regular audits of any third-party information security service providers and partners to ensure that they are following the prescribed information security protocol?

What is driving the loss costs for life sciences?

The life sciences industry is being targeted by cyber criminals due to the success that this market has achieved as well as the great amount of sensitive digital information that they have available. Loss from these attacks comes from two areas: internal costs and external claims. Internal costs occur when a cyber-security breach disrupts business operations, and requires notification to clients whose information was taken along with accompanying credit monitoring, loss of intellectual property, reputational damage, regulatory compliance exposure, and legal defense costs. External claims occur when outsiders have lost sensitive information through this breach and want to be compensated.

The costs of a cyber-security breach is often hard to quantify due to the wide variety of data breaches that can happen and the indirect costs for which there is no direct accounting. For instance, the 2015 Verizon Data Breach Investigations Report documents different research that says that a data breach "can cost anywhere from $0.58 to $201 per record." [3] This data is for a 'generic' data breach. For example, if a developmental drug company had the personal data of 2,500 clinical trial participants stolen, this could cost the company somewhere in the range of $200,000 to $300,000 to resolve. This cost analysis helps to show that the preparation and security needed for life science companies is well worth the investment. These figures do not take into effect the damage to the company's reputation, which is hard to quantify and for a growing life science company, may be hard to overcome.

Regulatory Considerations

Before mitigating these vulnerabilities, a life sciences company needs to understand what regulations concerning information security are in place. As with life science companies' primary work of developing products where regulations form the baseline of what these companies can (or cannot) do, the arena of information security is no different. Many federal regulatory agencies are involved in helping companies protect their cyber security via regulation, such as:

- Federal Communications Commission (FCC): The FCC monitors communication practices and provides recommendations to ensure optimal security of communication systems.
- Federal Trade Commission (FTC): The FTC monitors business practices to ensure that the consumers are protected from deceptive or fraudulent practices. FTC's Health Breach Notification Rule provides companies that have had a security breach with specific notification rules. This applies to companies that store or gather any type of personal medical information.
- FDA: The FDA has recently created guidance documents for life science companies for their digital world presence. Of specific concern is information security for medical devices.
- Office of Civil Rights - Health Insurance Portability and Accountability Act (HIPAA): HIPAA is used to "protect the privacy of individually identifiable health information." This regulation is meant to protect health information that could be vulnerable due to network breaches through medical devices at hospitals or due to clinical trial information leaks. This regulation encompasses both the primary user of this information as well as any contractors or subcontractors that may do work involving this protected information. Violations of the HIPAA may involve investigation by a particular state's attorney general.
- Securities and Exchange Commission (SEC): Information security is a known risk factor in SEC filings and cyber-security risks and such incidents must be disclosed by publicly traded companies.
- International: Many international laws regulate information security for life sciences companies, including the European Union's General Data Protection Regulation. This proposed regulation that will be finalized

in 2015/2016 will create a regulation whose scope is to harmonize data protection laws throughout the EU and affecting any data of EU residents used by all companies.

Risk Management Resources to mitigate this exposure to cyber security

To understand where to start in mitigating this exposure, a life sciences company should conduct a risk assessment of its information security policies and procedures to better understand its exposure and where to focus their new strategy. The following practices can help a company reduce these exposures to cyber security:

1. Technical
   The first place to start to prevent exposure to cyber criminals at a life sciences company is to look at the technical set up of your network. There are multiple steps that a company can take to protect these systems.
   a. Update Computer software: Ensuring that the computer software that is used on the digital network is up to date.
   b. Install malware detection services: These detection services will help scan the networks to find any malware that has infiltrated these systems.
   c. Security audits: Conducting regular security audits of the network systems will ensure that the system is as robust as it should be. There are many ways that the audits can be conducted, so it is up to individual life science companies to establish a baseline of what must be covered in an audit. Topics may include:
      i. Review of security checkpoints and firewall access
      ii. Performing a penetration test to check for vulnerabilities
      iii. Review threat sources and their potential to become vulnerabilities
2. Administrative
   Administrative practices help to create the foundation for a secure information network. This foundation includes updated security policies and procedures, a disaster recovery plan, a review of who is involved with the digital world at the company and a financial review of how to prepare for a cyber-attack.
   a. Security policies and procedures: These policies and procedures help the company understand what to be aware of concerning information security. These policies should include:
      i. Management's goal for information security
      ii. Roles and Responsibilities
      iii. Description of technical parameters to control access to electronic information
      iv. Workflows for handling of secure information
      v. Management of outsourced information security vendors
      vi. Mobile device and social media usage guidelines
   b. Training: Once these policies have been created, employees need to be trained on them to understand what is expected of them. Part of this training should include a description of how cyber-criminals will try to get information from the employees. For example, social engineering may be used, such as where the cyber-criminal manipulates an unsuspecting employee to give their information allowing the cyber-criminal to gain access to the company's network.
   c. Disaster Recovery Plan: A disaster recovery plan should be created specific to information security. Preparing this plan helps to anticipate the type of cyber-attacks to which a life sciences company can be exposed and outline an appropriate response. The evaluated impacts of such attacks should include not only the company itself, but also how it affects a company's customers, vendors or others. Once the plan is created, it should be reviewed, and if necessary updated, annually.
   d. Data management: Data that is collected can be anything from individual patient information to the company's intellectual property. Determining whether all the information that is collected is actually needed to conduct business could help to lower the exposure by elimination of unneeded data.

3. Financial Protection:
   Once a company understands the impact that a cyber-attack can have, a life sciences company needs to see how best to financially protect it. One way to do this is to purchase data breach insurance. Various coverage types may cover investigative costs, legal defense costs, notification costs, and third party liability claims just to name a few. Insurance comes in many forms and it is best to work with your insurance broker to see what best fits your company's needs.

---

1 "Drugmakers urge FDA security audit after cyber breach" from http://uk.reuters.com/article/2013/12/18/us-cyberattack-fda-drugmakers-idUKBRE9BH01C20131218
2 "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff", available at http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.
3 Verizon 2015 Data Breach Investigation Report from http://www.verizonenterprise.com/DBIR/2015/

Sonia Weiss, ARM, CIH, MBA, MPH, has over 10 years of experience working in the environmental, health and safety ("EHS") professions, specializing in providing EHS services and advice to the academia, manufacturing, and biotechnology sectors. At Berkley Life Sciences, her focus is on helping her life science clients understand and manage their overall risk, with a particular focus on cyber security risk. Prior to joining Berkley Life Sciences in 2013, Ms. Weiss was the Safety Health and Environmental (SHE) Manager for Genencor, where she was responsible for workplace safety, regulatory compliance, risk assessments, and industrial hygiene. Ms. Weiss has a Bachelor of Arts degree in Biochemistry and Environmental Sciences from Northwestern University, a Master in Public Health in Environmental Health Sciences from the University of California, Berkeley and a Master in Business Administration from Presidio Graduate School.