The Necessity of Information Security Management in the Vulnerable Pharmaceutical Industry

Shawn J. Roberts

East Carolina University

July 13, 2014

Author Note

This paper was prepared for ICTN 6823: Information Security Management, taught by Dr. Phil Lunsford.

Abstract

The pharmaceutical industry produces billions of dollars in sales each year. The industry is evolving and relying on using technology more and more to conduct day-to-day business. The pharmaceutical industry generates enormous amounts of sensitive and private information such as medical records, employee information, financial data and research data. This makes the pharmaceutical industry vulnerable to cybercrime. The pharmaceutical industry has a big responsibility to stakeholders, patients, employees and customers all over the world to ensure this information is secure. It is imperative for organizations to budget adequate amounts of money and resources to have effective Information Security Management. Information Security Management is critical in the pharmaceutical industry and the alternative of not having it would be devastating to a pharmaceutical company. Cyber criminals can tarnish company reputations and the effects can take years to overcome. This paper will describe the vulnerabilities of the pharmaceutical industry and illustrate why information security is necessary in the pharmaceutical industry.

Keywords: information security, pharmaceutical industry, health information security

The Necessity of Information Security Management in the Vulnerable Pharmaceutical Industry

Information security is the act of protecting data from unapproved access, use, exposure, interruption, change, assessment, recording or destruction. It is a general term that could be utilized paying little respect to the structure the information may take (electronic, physical, etc.). Information accessed without authorization is called a data breach. Data breaches can be intentional or unintentional. When a data breach is intentional and involves the Internet, computer system or computer technology it is called a cybercrime. Some examples of cybercrime are identity theft, account takeover, and phishing. Cybercrime is increasing every year as 0rganizations and consumers are relying more and more on computers and technology.

Cybercrime costs organizations and consumers billions of dollars each year. According to the Identity Theft Resource Center (2014), as of July 3, medical/healthcare breaches comprised 46 percent of reported data breaches in the United States in 2014 as shown in Figure 1. This is a percentage based on reported breaches.

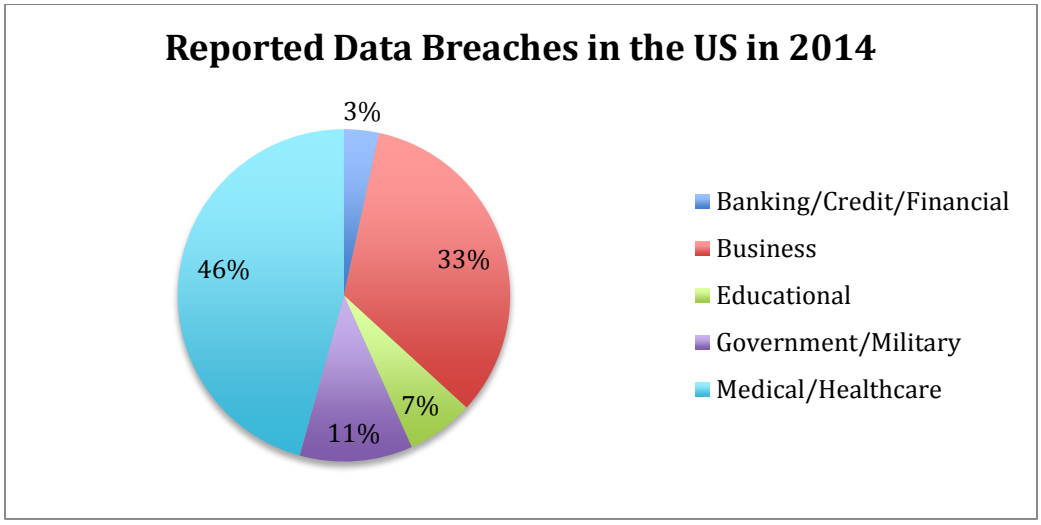

Figure 1. Reported Data Breaches in the US in 2014. This figure shows reported data breaches as of July 3.

This is not a true representation of the number of breaches that have occurred because many organizations do not report a breach and sometimes organizations are not aware a breach has occurred. “Cyber security for the healthcare and pharmaceutical sectors of the S&P 500 index worsened at a faster rate in the past year than for the other sectors tracked by Bitsight, one of the few companies that try to measure how vulnerable companies and industries are to cyber attacks” (Kuchler, 2014, para. 2). So why is the pharmaceutical industry so vulnerable to cybercrime? This paper will explain some of the threats that exist in the pharmaceutical industry, why it is so enticing to cyber criminals and why it is important for this industry to have effective Information Security Management.

Threat of Insiders

One of the biggest threats to the pharmaceutical industry is not from a hacker, but from someone inside the organization such as an employee or contractor. Insiders are a problem because they are trusted to handle information within the company and based on their position, they could have access to sensitive information. Dealing with malicious, disgruntled or ignorant insiders is much more difficult than outsiders. According to the National Research Council (1997), the following are the levels of threat to information in health care organizations;

Threat 1: Insiders who make “innocent” mistakes and cause accidental disclosures.

Threat 2: Insiders who abuse their record access privileges.

Threat 3: Insiders who knowingly access information for spite or profit.

Threat 4: The unauthorized physical intruder.

Threat 5: Vengeful employees and outsiders, such as vindictive patients or intruders, who mount attacks to access unauthorized information, damage systems, and disrupt operations.

"Companies can be doing more to increase employees' awareness of the danger to protect valuable information from those inside the firewall and to keep track of what insiders do when they're using corporate computer systems" (Totty, 2006, para. 3). The following are some of the recommendations from security experts and others for dealing with the security challenges from troublesome insiders.

- Know your risks – Understand exactly where and how information might be vulnerable to misdeeds or mistakes by employees.
- Know your insiders – Perform background checks when hiring for sensitive positions.
- Teach security – Most problems with insiders are unintentional such as putting sensitive information in an email or writing down passwords and placing it under their keyboards. Remind employees that they hold a privileged position and that it is their responsibility to protect the sensitive information they work with.
- Classify your data – Keep it simple; have three to five classes of data each with different levels of access and comes with different layers of control.
- Limit access – Limit access to information strictly on a need to know basis.
- Use encryption – Scrambling data so that it can't be read if someone can get access to it
- Monitor, filter and block – Obtain software that monitors, filters or blocks employee email, web browsing and other computer activities.
- Hold employees accountable – Make sure employees and other insiders know the rules and are held accountable for failure to follow them (Totty, 2006).

An example of an insider malicious act happened to Shionogi, a Japanese pharmaceutical company. Jason Cornish, a former employee of Shionogi, used passwords he had obtained while employed at Shionogi to delete contents of fifteen virtual hosts. The attacks were so severe that they crippled Shionogi's operations for a few days. The company was not able to ship products, cut checks or even send emails. The damages caused by Cornish were estimated at $800,000. On August 16, 2011, Jason Cornish, pleaded guilty to charges of computer intrusion, which has a maximum sentence of ten years in prison (Homeland Security News Wire, 2011).

Valuable Patient Information

Patient data is abundant in the pharmaceutical industry. Patient data is collected from employees, clinical patients and donors. Patient health information is so valuable because the records tell a person's entire life history as well as transactional history. This type of breach is typically hard to detect and these records contain so much personal information such as social security numbers, insurance records, birth dates, family details, billing information, and medical history. Most naïve people ask, what would cyber criminals possibly want with patient data of people they didn't even know? Little do they know that cyber criminals sell this information at a premium price in the black market! According to Horan (2014), a stolen credit card number sells on the black market for $1, but a stolen medical ID number and record sells on the black market for $50.

The following are three types of overarching risks involved in healthcare breaches and medical identify theft:

1. Health risk - There are serious health risks involved when a medical record is polluted or merged with someone else's medical prescriptions or lab procedures. This could cause life-threatening complications or even death to a patient.
2. Financial risk - Medical files and billing and insurance records are the most likely patient data to be stolen during a data breach. However, there is a risk of financial identity theft since healthcare organizations hold credit cards and bank records. There are also issues of "denial of service" or "denial of claim" often associated with medical theft. This is when a person uses someone else's medical record to obtain or bill for medical goods or services.
3. Reputational risk – A person's health information or medical records contain private information that we often don't want in the public domain. Consider mental health, depression, alcohol or substance abuse. This type of information still has a huge stigma in our society and can cause reputational harm. This type information can come up in an employment background check. Imagine in a health record was polluted by someone else's medical history; patients would be wrongfully penalized based on false information (Horan, 2013).

Pharma organizations should as of now follow strict security guidelines held in 21 CFR Part 11 for all electronic records made, altered, kept up, filed, recovered, or transmitted as a requirement of the Food and Drug Administration (FDA) or submitted to FDA under the necessities of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act. Electronic records produced as a feature of a clinical trial performed to help a New Drug Application (NDA) or an Abbreviated New Drug Application (ANDA) fall under the extent of 21 CFR Part 11 (IPPC, 2005).

When implemented in electronic data capture (EDC) and other workstation frameworks, the transmission controls held in 21 CFR Part 11 guarantee that transmissions of electronic Protected Health Information (ePHI) from a secured element (trial site) to a pharma supporter will fulfill the Health Insurance Portability and Accountability (HIPAA) Security Rule's specialized shields for transmission. Furthermore, different parts of the specialized protections listed in the HIPAA Security Rule are generally tended to through consistence with 21 CFR Part 11 (IPPC, 2005).

An example of a data breach happened to Pfizer Inc. In 2007, an employee at Pfizer Inc. installed unauthorized file-sharing software on a laptop provided by the company for at-home use. By doing this, she exposed the Social Security numbers and other private information of 17,000 current and former employees of Pfizer Inc. In order to help rectify the matter, Pfizer contracted a protection package with Experian for all the employees that were affected by the breach as well as a $25,000 insurance policy to assist in covering expenses that the employees might incur as a result of the breach (Vijayan, 2007). What happened to Pfizer Inc. is not as uncommon as you may think. Recent breaches that have made the news lately are the breaches that occurred at eBay and Target.

Bensinger and Calia (2014) stated that EBay asked 145 million registered users to change their passwords following a cyber attack that compromised a database containing encrypted passwords. The database also included additional information such as email addresses, physical addresses, phone numbers and dates of birth, but did not include financial data. “The attackers gained access to the corporate network by compromising some employees’ login credentials” (Bensinger & Calia, 2014, para. 4).

The Target incident was a different animal. “Hackers took 40 million credit and debit card numbers, as well as personal account information on 70 million customers from Target Corp” (Bensinger & Calia, 2014, para. 12).

Supply Chain Security

“Protecting and securing the pharmaceutical supply chain requires constant vigilance in cooperation with all partners in the channel: the manufacturer, the distributor and the pharmacy as well as state and federal legislators and regulatory agencies” (Zimmerman, 2006, para. 1). Expanding globalization and store network intricacy has postured dangers to pharmaceutical wellbeing, eventually affecting organizations and, in particular, patients.

Today, up to 40% of the medicines Americans take are produced outside the United States as well as 80% of the active pharmaceutical ingredients in those drugs.

> This rapid expansion of the global market opens companies up to an exponential increase in the number of vulnerability points, coupled with decreased visibility to them, due to insufficient supply chain information. Globalization also leads to a complex system of foreign, federal and state product safety oversight with an incomplete set of enforcement tools. This misalignment of resources leaves the United States drug distribution vulnerable to a host of problems (Hauhn, 2013, para. 8).

At any stage in this long, multi-faceted journey from raw source materials to finished products and then to consumers, products can be contaminated from four primary risks:

- Intentional adulteration – This is due to contamination in the manufacturing, storage, or distribution process or from ingredient substitution for economic gain.

Adulteration can result from a number of sources including foreign and domestic terrorist organizations or activists, economically motivated person or group, or even disgruntled employees.

- Cargo theft – This is due to the sluggish economy and security measures that rely too heavily on expecting people to consistently follow prescribed procedures. In the United States, cargo theft produces an annual loss of $35 billion.
- Counterfeiting – This is fraudulently mislabeling a product in identity or source. Counterfeiting will be discussed in more detail later on in this paper.
- Diversion – This is when products are diverted from the intended authorized market to another market (Hauhn, 2013).

Businesses can also incur daunting costs, such as revenue loss, recall costs, legal costs for damage to health or life and regulatory fines. Ultimately, complications in any supply chain impact a brand's reputation and require time and investment to rebuild trust among customers, partners and patients (Hauhn, 2013).

An example of cargo theft happened to Eli Lilly & Co. in Enfield, Connecticut. Brazen thieves cut a hole in a warehouse roof, slid down a rope, disabled the interior alarm system and spent hours inside the warehouse. The thieves made off with $75 million in drugs. Some of the drugs that were stored in the warehouse included Prozac, Cymbalta and Zyprexa. There was no disclosure whether those were among the products stolen, but it was said that controlled substances such as painkillers and narcotics were not taken (Efrati & Loftus, 2010).

Counterfeit Pharmaceutical Drugs

The reason counterfeit pharmaceutical drugs is discussed in much more detail than the other three primary risks is because of the growing problem in the world today and the fatal

consequences due to their existence. There are many different definitions for counterfeit drugs. For this paper's purpose, the World Health Organization's definition will suffice. The World Health Organization's definition for counterfeit drugs is as follows:

> A counterfeit medicine is one that is deliberately and fraudulently mislabeled with respect to identity and/or source. Counterfeiting can apply to both branded and generic products and counterfeit products may include products with the correct ingredients or with the wrong ingredients, without active ingredients, with insufficient (inadequate quantities of) active ingredient(s) or with fake packaging (WHO, 2014).

The definition may sound a little drawn out and confusing, but this definition must be all-inclusive to identify all types of counterfeiting.

Counterfeit drugs are everywhere, especially in developing countries. As Mackey and Liang (2011) have stated, counterfeit drugs are a global problem with significant consequences for global health and patient safety, including patient deaths. Identifying counterfeit drugs in the market is a very difficult task. Unlike other types of products that are frequently counterfeited such as purses, watches, and sunglasses, consumers are often under the impression they are buying knock-off products. Consumers generally have no idea that the prescription drugs they purchase are counterfeit.

Mackey and Liang (2011) stated that this multibillion-dollar industry does not regard geopolitical borders and debilitates the wellbeing of both rich and poor nations.

> The United States of America, although more insulated from the dangers of counterfeit medicines introduced into the domestic drug supply chain, has also reported patient safety issues and deaths related to counterfeit medicines. As the world's largest market for pharmaceutical sales, it is natural that counterfeit manufacturers and seller have

> targeted the United States of America as its most lucrative market (Mackey & Liang, 2011).

Some counterfeit drugs include Lipitor, Viagra, Zyprexa, and Epogen. Other counterfeit drugs that the FDA has discovered are Generic Tamiflu and counterfeit Alli being sold over the Internet (Mackey & Liang, 2011). Securing the pharmaceutical industry supply chain is a way to help decrease the presence of counterfeit drugs in the United States, protect consumers and reduce the costs to organizations and consumers.

Serialization

The current test is to better gather, track, and trace products and data that pass through pharmaceutical supply chains. Makers are continually vigilant for new advances that have the most exact and advanced track-and-trace abilities to help them react rapidly to climbing issues. Serialization is the response for some and has been recognized by the U.S. Food & Drug Administration (FDA) as the best solution accessible to keep counterfeiting under control and minimize recalls (Kerper, 2013).

According to the FDA (2014), President Obama signed the Drug Quality and Security Act (DQSA) into law on November 27, 2013.

> Title II of the Drug Quality and Security Act outlines critical steps to build an electronic, interoperable system to identify and trace certain prescription drugs as they are distributed in the United States. Drug manufacturers, wholesale drug distributors, repackagers, and many dispensers (primarily pharmacies and hospitals) will be called on to work in cooperation with FDA to develop the new system over the next ten years (United States Food and Drug Administration, 2013).

Among key provisions implemented over the next ten years are requirements for:

1. Product identification – Manufacturers and repackagers to put a unique identifier on certain prescription drug packages, for example, using a barcode that can be easily read electronically.
2. Product tracing – Manufacturers, wholesaler drug distributors, repackagers, and many dispensers in the drug supply chain to provide information about a drug and who handled it each time it is sold in the United States market.
3. Product verification – Manufacturers, wholesaler drug distributors, repackagers and many dispensers to establish systems and processes to be able to verify the product identifier on certain prescription drug packages.
4. Detection and response – Manufacturers, wholesaler drug distributors, repackagers, and many dispensers to quarantine and promptly investigate a drug that has been identified as suspect, meaning that it may be counterfeit, unapproved, or potentially dangerous.
5. Notification – Manufacturers, wholesalers drug distributors, repackagers, and many dispensers to establish systems and processes to notify FDA and other stakeholders if an illegitimate drug is found.
6. Wholesaler licensing – Wholesale drug distributors to report their licensing status and contact information to FDA. This information will then be made available in a public database.
7. Third-party logistics provider licensing – Third party logistic providers, those who provide storage and logistical operations related to drug distribution, to obtain a state or federal license (United States Food and Drug Administration, 2013).

The FDA (2013) also stated that the law requires the FDA to develop standards, guidance documents and pilot programs and to conduct public meetings, in addition to other efforts necessary to support efficient and effective implementation.

Conclusion

With the Drug Quality and Security Act in place, the United States is well on its way in making the pharmaceutical industries supply chain more secure. Ten years seems like a long time, but to get all the key players on the same page will take a lot of effort, time, money and resources. Strict security requirements of 21 CFR Part 11 and HIPPA are ensuring the pharmaceutical industry is doing its due diligence in protecting patients, customers, stakeholders and employees from cybercrime. No security in place is 100% and that is why Information Security Management is so important in the pharmaceutical industry. It is important to have the resources in place so that proper education and training is available to the average employee who does not have an information security background. It is also important to have employees in place with an Information Security background to identify possible attacks. Keeping these employees training and updated on future risks and security strategies is another way to improve security. If you are keeping up with today's escalating risks, then you are not prepared to manage future risks. Not if, but when a security breach takes place, it is imperative that it is caught immediately so the damage can be controlled and contained. The pharmaceutical industry can improve on these aspects of information security by holding employees accountable for their actions and providing the education and training needed to bring awareness to all employees and avoid cyber attacks.

References

*Bensinger, G. & Calia, M. (2014). Corporate news: EBay is latest victim of cyberattack. *Wall Street Journal*, May 22. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1526643698?accountid=10639

Data Breach Category Summary. (2014). Retrieved July 6, 2014 from http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2014.pdf

*Efrati, A., & Loftus, P. (2010). Lilly hit in massive pill heist. *Wall Street Journal*, Mar 17. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/399142244?accountid=10639

Hauhn, J. (2013). What the pharmaceutical industry can teach us about supply chain security best practices. Retrieved from http://www.Industryweek.com/supply-chain/what-pharmaceutical-industry-can-teach-us-about-supply-chain-security-best-practices

Homeland Security News Wire. (2011, January 1). Japanese pharmaceutical crippled by insider cyberattack. Retrieved from http://www.homelandsecuritynewswire.com/japanese-pharmaceutical-crippled-insider-cyberattack

Horan, A. (2014). Healthcare records: A hacker's roadmap to your life. Electronic Health Reporter. Retrieved from http://electronichealthreporter.com/healthcare-records-hackers-roadmap-life/

International Pharmaceutical Privacy Consortium (IPPC). (2005). Transmission security practices of pharma sponsors of clinical research. Retrieved from http://www.pharmaprivacy.org/download/Clinical_Research_Transmission_Security.pdf

Kerper, J. (2013). Boosting security in the pharmaceutical supply chain with serialization. Healthcare Packaging: News, trends and analysis of pharmaceuticals, biologics, medical devices, and nutraceuticals. Retrieved from http://www.healthcarepackaging.com/trends-and-issues/traceability-and-authentication/boosting-security-pharmaceutical-supply-chain

Kutcher, H. (2014). Cyber attackers 'target healthcare and pharma companies'. . Retrieved from http://www.ft.com/cms/s/0/a6b09006-e5c9-11e3-aeef-00144feabdc0.html

*Mackey, T. K. and Liang, B. A. (2011), The global counterfeit drug trade: Patient safety and public health risks. *J. Pharm. Sci*., 100, 4571–4579. doi: 10.1002/jps.22679

National Research Council. (1997). *For the record: Protecting electronic health information*. Washington, DC: The National Academies Press.

*Totty, M. (2006). Technology (A special report); the dangers within: The biggest threats to information security often don't come from hackers; they come from a company's own employees; here's how you can stop them. *Wall Street Journal*, Feb 13. http://search.proquest.com.jproxy.lib.ecu.edu/docview/399005031?accountid=0639

U.S. Food and Drug Drug Administration. (2013). Supply chain security act (DSCSA): Title II of the drug quality and security act of 2013. Retrieved from http://www.fda.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct/

Vijayan, J. (2007). JPersonal data on 17,000 pfizer employees exposed; P2P aa blamed. Computerworld. Retrieved from http://www.computerworld.com/s/article/9024491/Personal_data_on_17_000_Pfizer_employees_exposed_P2P_app_blamed

World Health Organization (WHO). (2014). *What are counterfeit medicines?*. Retrieved from http://www.who.int/medicines/services/counterfeit/faqs/03/en/

*Zimmerman, Chris. (2006). Protecting the Pharmaceutical Supply Channel. *Journal of Pharmacy Practice*, 19, i4, p.236(3). Retrieved from http://jpp.sagepub.com.jproxy.lib.ecu.edu/content/19/4/196.full.pdf+html