GAVIN PUBLISHERS

Journal of Pharmaceutical and Pharmacological Sciences

Jaithliya T. J Pharma Pharma Sci 02: JPPS-121.

DOI:10.29011/2574-7711.100021

Case Report

Cyber Security in Pharmacy and Pharmaceutical Companies

*Tanvay Jaithliya

Department of Pharmacy, Mewar University, Gangrar (Chittorgarh), India

*Corresponding author: Tanvay Jaithliya, Department of Pharmacy, Mewar University, Gangrar (Chittorgarh), India; Tel: Tel: +91-01471-291148; E-mail: jtanvay@gmail.com

Citation: Jaithliya T (2017) Cyber Security in Pharmacy and Pharmaceutical Companies. J Pharma Pharma Sci 02: 121. DOI: 10.29011/2574-7711.100021

Received Date: 15 March, 2017; **Accepted Date:** 19 April, 2017; **Published Date:** 27 April, 2017

Digital health is a hot topic that is booming right now in world, in this we can manage patient health very easily, accurately and combatively more effective.

Devices such as fitness trackers, heart rate monitors and insulin pumps for diabetic patients are connected to IOT (Internet of Things) to enable pharmacists and doctors to monitor and alter our activities, heart rate, blood pressure, drug concentration.

We can ask for our genome to be sequenced and pharmaceutical and health companies manage a big data about patient monitoring and alter their next drug content after analyzing this data. It helps us to find out whether the patient is getting any side effect after taking a medicine, and then they can find out the reason behind it and change the drug content to improve it. All of this data help us to maintain our personal records and we can also connect their devices to heath care professional and they can send data, alarms and notifications to the patient about his/ her current scenario.

It offers great potential for better self-care, health management and faster recovery from diseases. Within hospitals increase digitalization will decrease error rate offer faster treatment and improve skill of clinician's to co-operate across borders with sick patients. Digitization enables pharmaceutical companies to create personalized drugs based on individual genomic sequence, can also check drug uptake, plasma concentration and bioavailability and efficiently and thus increase the closer relationship between the pharmaceutical company and patient.

At the same time there is wide well known threat, cyber security breaches, into sophisticated and well balanced companies by hackers, criminals and nation states. Medical records, drug contents, intellectual property is stolen, confidential e-mails are shared publically, and medical records used to create fraud new identities. For example US retailer Target's data breach of 2014 involving a reported 70 million credit card records, JP Morgan Chase's data breach involving 76 million accounts and Anthem's loss of

personal information of its clients and employees earlier this year are some of the recent major security breaches. Over the past six months we have heard of an alarming number and sophistication of breaches into medical devices, with FDA advisories on cyber security for certain products. Examples include an infusion pump used to deliver programmed amount of fluids into a patient's body. This device could allow an unauthorized user to change the dosage delivered. We also see that medical devices can be discovered on hospital networks from internet searches which hackers may well exploit in the future. Compromised information leads to reputational damage.

So how do we understand the cyber security risks to pharmaceutical companies?

There are risks to their information and to their production systems, with both being exploited in similar ways, but the impact varies greatly. Compromising information leads to financial losses and reputational damage, but compromised production systems could have far reaching impacts including loss of life. Looking at it another way, cyber security breaches into medical devices and pharmaceutical technology impacts the confidentiality of intellectual property and personal information, but of far greater concern is integrity and availability. Scientific discovery and development is key to pharmaceutical companies.

Pharmaceutical companies must innovate and quickly turn innovations into products, possibly before potential competitors develop alternatives. However, the rush to develop could lead to other core business functions being overlooked. Insecurely protected technology increases the risk of exposing sensitive information such as intellectual property which can be exploited by competitors, hacktivists, cyber criminals or nation states for financial gain or for reputational damage. Pharmaceutical products are manufactured through a number of complex processes. There is increasing business value in connecting manufacturing systems to the company as well as the outside internet. Manufacturing systems' data can be analyzed with environmental, physical and location data to drive efficiencies and more effective production and safety processes, as well as operational cost savings. Addressing the cyber security risk. One key problem is that the use of manufacturing systems often has technology which is older than the internet itself, means that these systems are inherently insecure. They were designed as specialized and isolated systems and not built to withstand cyber security attacks. For pharmaceutical companies, any compromises to manufacturing systems can result in a loss of integrity and availability of the physical process. This can potentially lead to safety problems, breaching statute and reputational damage. The same risks apply to medical devices. Vulnerabilities in the design or implementation of a medical device such as an insulin pump or in anything interconnected to such devices could result in loss of device integrity and potential harm to patients if they are exploited in a cyber-attack. Risk is an inherent part of any business, and cyber risks are only one aspect of this. In KPMG's experience the most effective approach to addressing cyber security risk is to understand who is targeting the organization, what they want, the potential impact and the controls in place.

The key is to place appropriate focus on both the strategic and the tactical elements. The tactical elements are important to deliver cost saving and quick value-add, but the strategic elements are usually even more important to ensure sustainable investment. The increasing digitization of the enterprise and production systems together with improved data analytics capabilities opens up numerous opportunities for pharmaceutical organizations to improve efficiency, enhance productivity and achieve substantial revenue generation and cost savings. In addition, medical devices, the IoT's, improved data collection and analysis technology have a great potential to improve health care. Cyber risks resulting from interconnectivity to the internet and enterprise systems must be taken into account as we increasingly interconnect devices.

We suggest that pharmaceutical organizations should analyze and understand the risks of increasing connectivity together with understanding how they can protect their key assets. It is crucial that security must be included during the design process and as an inherent part of any system. As with every year, there was no shortage of big healthcare stories in 2014. Several publications made good lists (here and there) and not surprisingly-Ebola appeared at or near the top of many.

I do think Ebola qualifies as The Top Global Healthcare Story for 2014, but I also think there's room for a U.S. specific version as well. As healthcare becomes increasingly digitized (and more devices become network attached, attachable or aware), cyber security captured as the top U.S. healthcare story for 2014. Here are the 5 compelling reasons why:

1. The SANS Institute Report (February).
2. The FBI Private Industry Notification (PIN) to the health care industry (April).
3. The "hacktivism" cyber-attack on Boston Children's Hospital (April).

4. The breach of 4.5 million health records at Community Health Systems-the second largest hospital chain in the country (August) Recommended by Forbes.
5. The Sony Pictures Entertainment breach-which included detailed employee, spouse and dependent medical information (December).

The SANS Institute Report was specifically targeted at the healthcare sector-and I added detailed coverage to the report in February with this headline. New cyber threat report by SANS Institute Delivers Chilling Warning to Healthcare Industry. A key quote from the report was this one by lead analyst and author Barbara Filkins: This level of compromise and control could easily lead to a wide range of criminal activities that are currently not being detected. For example, hackers can engage in widespread theft of patient information that includes everything from medical conditions to social security numbers to home addresses, and they can even manipulate medical devices used to administer critical care.

Barbara Filkins-Senior SANS Analyst and Healthcare Specialist

It's an important assessment that expands on the findings of the Ponemon Institute report in 2013. In that report, the Ponemon Institute calculated the cost of Medical Identity Theft at $12 billion annually. That's just the financial calculation. The clinical calculation included these additional risks as reported by actual victims of Medical Identity Theft, 15% of respondents experienced a misdiagnosis, 13% of respondents experienced a mistreatment, 14% of respondents experienced a delay in treatment, 11% of respondents were prescribed the wrong pharmaceutical, 50% of respondents have done nothing to resolve the incident in April.

"Boston Children's Hospital was attacked by a hacker collective known as Anonymous. While the attack was classified as hacktivism, the group issued direct threats prior to launching a sizable Distributed Denial-of-Service (DDoS) attack on the hospital. The attack was short lived about a week, but escalated quickly and did have an impact on critical communications-including email services for the entire hospital. The attack also included the release of personal information on both the Judge and the doctor presiding over the pediatric case in question. The cyber-attack against BCH earlier this year did take us by surprise and we reacted quickly in ways that did control the threat, but that also required a disruption in normal IT services like email. If there is any real message here you can't schedule these kinds of attacks so it's critical to have cyber threats as a key part of IT budget and planning. In our case, we don't think the motivation was financial, but the attack was sophisticated."

Dr. Daniel Nigrin-CIO Boston Children's Hospital

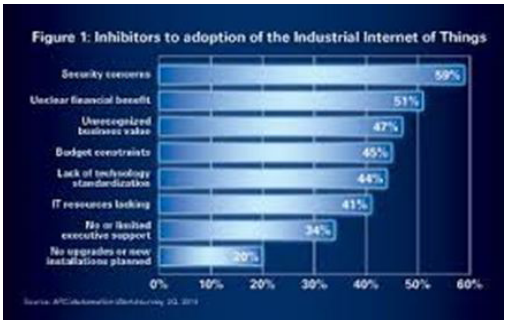
"In August, Community Health Systems (the nation's 2nd largest hospital system with 206 hospitals in 29 states covered) announced a breach of 4.5 million patient records. Included in coverage of that story (Cyber Attack Nets 4.5 million records from Large Hospital System) were references to other notable cybersecurity threats this year. We see about a million hits a day from China alone trying to break into our network''.

Bert Reese- CIO of Sentara (Top Healthcare CISO's Hard to Come by-May, 2014)

The medical device makers were not aware of the cyber breach until federal authorities contacted them, and they have formed task forces to investigate the breach, [an inside source said].

Hackers break into networks of 3 big medical device makers-SF Gate (February, 2014) which brings us to the latest noteworthy healthcare breach announced just this month-Sony Pictures Entertainment (SPE). While the global interest and attention was mostly centered on the release of the film the Interview-and secondarily whether North Korea was to blame-this was a large healthcare breach that included deeply personal health information on employees and their family members. As a result, it will absolutely be subject to the rules and penalties of HIPAA violations. One memo by a human resources executive, addressed to the company's benefits committee, disclosed details on an employee's child with special needs, including the diagnosis and the type of treatment the child was receiving. The memo discussed the employee's appeal of thousands of dollars in medical claims denied by the insurance company. Another document leaked in the hack is a spreadsheet from a human resources folder on Sony's servers that includes the birth dates, gender, health condition and medical costs for 34 Sony employees, their spouses and children who had very high medical bills. The conditions listed include premature births, cancer, kidney failure and alcoholic liver cirrhosis. The document doesn't include employees' names. Sony's Hacking Nightmare Gets Worse: Employees Medical Records Revealed-Bloomberg, December 12 Sony acknowledged this outright in their notification to employees earlier this month. In addition, unauthorized individuals may have obtained HIPAA protected health information, such as name, social security number, claims appeals information you submitted to SPE including diagnosis and disability code, date of birth, home address, and member ID number to the extent that you and/or your dependents participated in SPE health plans, and health/medical information that you provided to us outside of SPE health plans.

SPE Notice to Employees on December 8.While many were quick to simply lump this into the traditional category of data breach-like Forbes, Target TGT +1.42%, Staples SPLS +2.34%andHome Depot HD +0.59%-it was vastly different.



This was a massive enterprise data breach that has healthcare repercussions well beyond just the data that was stolen. Self-insured employers often share detailed employee and dependent health information with companies they contract with for benefit management and claims processing. Whether a company is self-insured or not is irrelevant. Managing and maintaining PHI greatly expands their responsibility and liability for security compliance, audit and data breach under HIPAA. Credit cards have a relatively short usable life after theft and a typically small personal liability-often only $50 to the consumer. This is also why the courts often frown on consumer lawsuits for financial identity theft. Medical identity theft, however, is vastly different and the courts will review these class-action employee/employer cases very differently. Full legal liability for PHI under HIPAA is not something that many employers are familiar or prepared to deal with. The plaintiffs are suing Sony on grounds of negligence, invasion of privacy, bailment and violations of multiple California laws that require a corporation to protect the private medical information of its employees and notify them of data breaches in a timely fashion. They're seeking "an award of appropriate relief, including actual damages, restitution, disgorgement, and statutory damages." Sony Hit with Fourth Class Action Law Suit Beyond the legal liability is the larger issue for all of cyber security-trust. Earlier this year the French telecom conglomerate did a study that produced these results. 1.78% of consumer's states that it is hard to trust companies when it comes to the way they use consumer personal data, 2.70% agree that there are few or no trusted way to find out about personal data management and protection online. 3.78% feel that service providers hold too much information about consumer behavior and preferences. In this new age of hacktivism, massive health data breaches and global cyber threats, privacy may well be dead, but trust most certainly isn't. As we study in these memos for more than 25 years, we can afford to lose money-even a lot of money. But we can't afford to lose reputation- even a thread of reputation.

References

1. http://www.europeanpharmaceuticalreview.com/35994/news/blog/cyber-security-in-pharmaceuticals/
2. https://www.forbes.com/sites/danmunro/2014/12/21/the-top-u-s-healthcare-story-for-2014-cybersecurity/#6dc8a91a50e1