The true cost of a data breach: Cyber security is a costly threat for organizations of all shapes and sizes

Last modified: November 5, 2012

Document version: 1.0

Although the financial cost of a cyber breach can be devastating to any organization, there are a host of other consequences that must be considered to determine the overall cost of a breach. These consequences can vary depending on what type of organization is victimized, and they can be difficult to quantify. It's much easier to calculate a hike in cyber liability insurance than the potential revenue lost due to reputation damage. By examining some case studies from various verticals and analyzing the hazards facing organizations it's possible to paint a vivid picture of how costly cyber breaches can be - and to underscore how critical it is to effectively mitigate risk.

Healthcare

One of the foundational principles of medical ethics is "First do not harm." This principle is meant as a guide for taking care of patients, but it also can pertain to taking care of patient information. Hospitals and other healthcare providers are increasingly turning to computers and other internet-enabled devices for improved record keeping efficiency. According to U.S. News and World Report[1], more than 570 million prescriptions were filed electronically in the United States in 2011. In addition, Steven Smith, chief information officer at NorthShore University Health System in Evanston, Illinois, told the news source that about 60 percent of the healthcare provider's emergency room patients have electronic records.

When it comes to personal privacy, healthcare providers store a lot of sensitive information like patient account details and billing information as well as personal medical information. In addition, larger healthcare providers like hospitals have multiple portals through which sensitive information can be stolen. Not only does this require quality anti-virus, anti-malware and other application control tactics to protect computer systems, but healthcare providers also have to ensure that data entered digitally into devices cannot be easily extracted or exported should a computer or another piece of technology be physically stolen.

Despite the high stakes when it comes to data security in the healthcare sector, a significant number of breaches continue to occur. According to Privacy Rights Clearinghouse[2], more than 23.6 million medical records have been exposed in the United States between 2005 and 2012 as a result of 769 security breaches. The attacks have been varied but their effects are typically the same - the unnecessary exposure of private medical and financial information, as well as the loss of trust in an institution.

[1] U.S. News and World Report: http://health.usnews.com/health-news/articles/2012/09/04/electronic-health-records-gaining-acceptance

[2] Privacy Right Clearinghouse: http://www.privacyrights.org/data-breach

- The names and diagnosis codes of about 20,000 patients of Stanford University Hospital[3] were found online in 2011. Those affected by the breach filed a $20 million class-action lawsuit against the hospital. Despite this high-profile data leak, the hospital again made headlines for data loss this year. A laptop stolen from the hospital in July 2012 contained information on close to 2,500 patients, including medical treatment history, birth dates and even some Social Security numbers.

Stanford University Hospital is not the only healthcare facility that has had to deal with the fallout from a data breach. Another incident, which occurred in February 2012 at Indiana University Health Goshen Hospital[4], served as a reminder that patient data is not the only sensitive information on hospital systems. As complex institutions, hospitals employ a wide range of individuals, and so hospital IT administrators must be cognizant of how to keep staff and applicant information safe.

- A computer virus stole information about more than 12,800 people from IU Health Goshen Hospital's system. The malware attack took names, addresses, Social Security numbers and medical information. The majority of those impacted - more than 12,300 people - were job applicants. The other victims - about 500 people - were primarily registered for outpatient procedures or in the maternity ward. To help those affected, the hospital offered free credit checks to allow people to see if their financial information had been compromised.

While laws do dictate certain security protocols that healthcare providers must undertake, these examples illustrate that compliance alone may not ensure the safety of medical information and preserve the trust of patients. For example, while the Health Insurance Portability and Accountability Act of 1996[5] (HIPAA) dictates that U.S. healthcare providers have industry-standard cyber security best practices in place, not all organizations have yet followed every one of the law's provisions.

In order to maintain the trust of patients, healthcare providers need to go above and beyond government protocols and create as thorough a cyber defense as possible. This can include encrypting all data, instituting application control software and requiring cyber security training for all those employed in the healthcare facility that is more thorough than what is mandated by law.

[3] Stanford University Hospital's data breach: http://threatpost.com/en_us/blogs/stanford-hospital-suffers-second-data-breach-year-080812

[4] Indiana University hospital data breach: http://www.scmagazine.com/indiana-university-hospital-hacked-to-steal-data/article/225887/

[5] HIPAA: http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2001.html

First Responders

Like healthcare providers, police officers and first responders need to ensure the proper safety protocols are in place not just to protect their own data, but to also ensure that they can effectively safeguard the population. Police officers, firefighters, EMTs and other first responders increasingly rely on technology for communicating during a crisis situation, electronic record keeping, and having proper cyber security protocols in place, which keeps operations running smoothly.

Two incidents that occurred earlier this year in Chicago underscored the importance of quality cyber security for police forces and other first responders.

- In May 2012, hacktivists - a name for politically-minded hackers - used a denial-of-service attack to take down the website of the Chicago Police Department (CPD). The attack shut down the CPD website at a critical moment, when a NATO summit had brought international dignitaries and a large number of protesters to the Windy City. ABC News[6] reported that the attack "temporarily crippled" the CPD website at a time when "chaos" was occurring in the city - chaos that included the arrest of three men on attempted terrorism charges.

- In the Chicago suburb of Lemont, hackers turned on all of the town's tornado sirens for 30 minutes in July 2012. As a result, the local police department was "flooded" with calls from confused and concerned residents, the Chicago Tribune[7] reported. The sirens had been legitimately activated two nights before this incident, during a storm that brought winds in excess of 60 miles per hour, but the weather was clear when the hack occurred. The hackers caused the sirens to alternate between severe weather and military attack warnings.

While each incident caused little damage from a monetary standpoint, the two events suggest what might happen in a worst case scenario. In the case of the Chicago Police Department, hackers could have used a well-timed denial-of-service attack or malware to shut down critical police computer infrastructure, not just the website. This would prevent data theft of information like arrest records or personnel information, compounding urban disorder like the NATO protests to the point at which people would be endangered. With the incident in Lemont, the results could have been much more dire if hackers had prevented the alarms from going off when they should have been warning area residents to seek safety. In that instance, a crucial piece of equipment used by first responders to protect people was shown to be faulty due to a lack of preventative layered security.

[6] ABC News: http://news.yahoo.com/nato-summit-hackers-target-police-city-chicago-websites-172246691--abc-news-topstories.html

[7] Chicago Tribune: http://articles.chicagotribune.com/2012-07-03/news/chi-police-hacker-lemont-tornado-siren-20120703_1_tornado-sirens-sound-warning-lemont-police

In order to prevent these dire consequences, local agencies need to team up with private enterprise to make sure that first responders are provided with the technology, skills and training needed to ensure networks will remain operational during a catastrophe. While police forces are trained in how to deal with situations from burglary to automobile accidents, often they are ill- equipped to understand all the issues that relate to cyber security. Because of this, private sector cyber security experts can enhance the offerings of police forces, fire departments and other first responders, lending their expertise both in the implementation of computer security software but also with training first responders on the safe use of technology.

An emerging issue relating to how the police and other first responders deal with cyber security relates to use of the cloud. More than many organizations, police forces see tremendous benefits from the ability to easily share information and store data from any location. For example, cloud computing can enable an officer in the field to access information about a stolen vehicle or a suspect. However, the cloud-based solutions of police forces must meet dual requirements.[8]

On one hand, the nature of police work requires data to be inaccessible except to approved parties. However, as public entities, police departments need to be overseen and audited. Ideal cloud-based solutions need to be private and secure, containing only encrypted information. Yet, some of that information often needs to be accessible on some level to the public. In addition, mission critical information needs to be constant available 24/7 regardless of which officer is in which police car.

Police departments and other first responders have begun to understand the necessity of having quality cyber security measures in place, and are taking the proactive steps needed to hackers and cyber criminals before they strike.

- The Los Angeles Police Department[9] (LAPD) had Faronics reboot-to-restore solution and application control solution installed on laptop computers used in about 1,600 patrol cars. The mobile laptops are used in tasks such as call dispatch and data queries, and contain sensitive information. The cyber security measures used by the LAPD ensure that no third-party software can be installed on the computers. In addition, should anything happen to the computers, a simple restart will restore the machines to working condition without worrying that sensitive data might have been lost in the process. When it comes to technology, the main concerns for First Responders are 24/7 availability, reliability, and reducing IT workload and related costs. These solutions fit the bill on three fronts.

[8] Council on Foreign Relations: http://www.cfr.org/cybersecurity/police-data-cloud/p26657

[9] LAPD: http://www.faronics.com/press-releases/article/lapd-deploys-faronics-software-with-technology-upgrade/

Municipal Governments

The cyber security concerns of local governments are as varied as their responsibilities and they must use limited resources to make sure that all systems within an area are protected. These systems can affect everything from the deployment of snowplows and city worker paychecks to the collection of taxes and the maintenance of utilities. Any systems breach can have devastating consequences on a town, and in some cases can even mean that an elected official loses his or her job.

While cyber attacks on federal government entities like the U.S. Federal Bureau of Investigation make splashy headlines, attacks on local level agencies can have devastating impacts that often go unnoticed. According to the National Security Cyberspace Institute[10], local government agencies are responsible for handling more private citizen information than many might expect, including data related to national government safety net programs. Considering the breadth of information that local, provincial and state governments collect and store, protective measures are of paramount importance. Otherwise, a municipal government may experience an incident like the two below.

- In 2010, hackers believed to be based in Moscow were able to steal about $200,000 in tax payments intended for recipients in Gregg County, Texas. The money was being moved via automated clearinghouse transfers from the tax assessor/collector's office to a bank when it was redirected through a Trojan, according to the local newspaper the News-Journal[11]. The theft cost the city of Kilgore more than $17,000 in property tax payments, and it was unclear whether the municipality was insured against the loss.

- Two USB thumb drives containing the personal information of almost 2.6 million people were stolen from the provincial office of Ontario's elections board. Despite a policy that the information on the sticks needed to be encrypted, it was not. A provincial official quoted by IDG News Service[12] said that workers thought encryption was the same as compressing files. IDG quoted the official as saying, "A policy is not enough sitting on some shelf, not understood." The loss of the sticks led to the dismissal of two workers and a criminal investigation.

Like police forces and other public agencies, local governments need to balance the public's need to have information freely available with the need to encrypt and protect hundreds of thousands of pieces of information. An ideal cyber security solution for municipalities would be one that allows for multiple highly secure access points, allowing authorized parties to freely access data while also keeping out any malware or other cyber threats.

[10] National Security Cyberspace Institute: http://www.nsci-va.org/WhitePapers/2011-02-25-State-Municipality%20Cybersecurity-NSCI-Crouch-McKee.pdf

[11] News-Journal: http://www.news-journal.com/news/local/article_435ad702-0626-595b-990e-1ba232f50bca.html

[12] IDG: http://www.csoonline.com/article/712678/missing-canadian-personal-data-could-hit-4-million

Prisons

Prisons and jails have to do more than keep inmates behind bars. They have to keep information insulated as well. Prisons are run with the assistance of complex computer systems. Should these systems ever be taken down by hackers or malware, it could mean the unauthorized release of information on prisoners or guards, or even a breakdown of the physical security apparatus of the jail itself. After all, many electric fences and cells are powered and monitored by computer systems.

Such a doomsday scenario has not only been envisioned, but demonstrated.

- John Strauchs[13], an ex-operations officer for the U.S. Central Intelligence Agency, presented his work in 2011. He showed that it was not only possible but relatively simple to override the industrial control systems used to keep prisons running smoothly. His program was able to remotely open all cells in a facility while making it appear to prison authorities that all of the cells were closed and secure. The prison-override program cost Strauchs only $2,500 and could be set off remotely.

Strauchs showed how important it is for jails to have security systems in place to repel exploits from outside attackers. However, another threat that prisons have to deal with comes from within. Just as with most other organizations, internal diligence is important. Cyber criminals are known to spread viruses and other types of malware through email, and should a guard open up the wrong attachment at work the consequences could be dire. Inmates who are incarcerated for computer-related crimes pose a serious internal risk. As well many jails have learning centers for the criminals, who if clever enough or if they know the right people, could introduce dangerous security threats to the prison machines.

Small- and Medium-Sized Businesses

Many SMBs are run on a tight budget that limits the amount of time and money that can be spent on cyber security initiatives, unlike big businesses that potentially have a lot more to spend on IT infrastructure.

Previously, people believed that hackers and cyber thieves were only looking to score big paydays and thus were disproportionately targeting big businesses. However, thousands of SMBs fall prey to malware every year, and some studies show that SMBs may be even more vulnerable as hackers expect to encounter a less robust security system. A report from Verizon Communications found that 72 percent of the 855 data breaches that occurred in 2011 targeted companies that had 100 employees or less.[14]

[13] Washington Times: http://www.washingtontimes.com/news/2011/nov/6/prisons-bureau-alerted-to-hacking-into-lockups/?page=all#pagebreak

[14] The Wall Street Journal: http://online.wsj.com/article/SB10001424052702303933404577504790964060610.html

An SMB that does not take a strong enough approach toward cyber security will end up regretting it both in terms of its bottom line and its future reputation with customers. Take the example of Lifestyle Forms & Displays Inc.

- In May 2012, mannequin manufacturer and retailer Lifestyle had $1.2 million stolen from its bank accounts after cyber thieves were able to take account login information from the company's computer systems. While the company was able to recoup some of its losses, it was never able to get back $160,000 of the stolen funds. For future protection the company took out a $1 million insurance policy that now costs Lifestyle Forms & Displays $13,000 a year.[15]

What can SMBs do to mitigate threats? It's key to ensure proper training and to implement strong network protection solutions. One of the best ways smaller firms can protect themselves is to train employees about smart internet strategies so as not to accidentally expose a company to risk.

Smaller companies with limited resources frequently rely on third-party software for protection. However, turning exclusively to a firewall and anti-virus software may unintentionally expose a smaller enterprise to harm. In particular, anti-virus software is designed specifically to stop known threats. Considering the increasing proliferation of new and previously unknown malware, this methodology leaves businesses vulnerable.

A more robust security approach will include application control, which can protect against zero-day threats and mutating malware. Instead of keeping a database of known threats, application control works by maintaining a list of approved programs. Any program that is not trusted and listed as approved is blocked. Using a default deny approach, even a brand new virus will be automatically blocked from executing on the computer.

Conclusion: Key Takeaways

For every cyber breach experienced, an organization needs to deal with a loss of assets and reputation. According to a Ponemon Institute study[16], the average data breach cost U.S. companies about $194 per compromised record in 2011, with total per-incident costs totaling $5.5 million for an organization. Yet, from every incident comes a lesson that can apply to the cyber security infrastructure of organizations from police forces and prisons to hospitals and small businesses.

[15] The Wall Street Journal: http://online.wsj.com/article/SB10001424052702303962304577509210831518418.html

[16] Ponemon Institute: http://www.ponemon.org/news-2/23

Here is a summary of the ways in which organizations of any size or industry can effectively protect themselves:

- **Data encryption**: For organizations dealing with sensitive personal data, encryption is key to ensuring the information cannot be read should it fall into the wrong hands. This is an especially useful tactic for fields in which data is spread out across a number of devices, where the theft or loss of even one piece of technology could be ruinous for hundreds or thousands of people.

- **Application control**: This works to protect a network via an inside-out model. Using a default deny approach, application control allows approved programs to run and rejects any new programs that are not approved, whether malicious, untrusted or unknown. This approach is the most effective defense against modern advanced threats.

- **System reboot-to-restore**: For organizations that require 100 percent availability and reliability, full restoration software is key. Now when a computer goes haywire, the machine can be restored to its desired settings by restarting the machine, ensuring that mission critical systems are up and running at all times.

- **End-user training**: At many organizations, the end-user is the gatekeeper protecting a system from harm. The wrong email opened or the wrong click can spell disaster. Regardless of the size of an organization, it is imperative that all employees within it receive adequate training on safe internet practices.

Pairing knowledge with quality software solutions helps organizations achieve better peace of mind and create a more robust security system that will keep them safe from sophisticated cyber threats. The cost of implementing a well-rounded safety net may seem considerable, but the costs of a breach make the initial efforts worthwhile for any organization.