keeper + JLT

Reducing Cyber Risk in Your Organization

The First Step to Reducing Cyber Risk

Understanding Your Cyber Assets

With nearly 80,000 cyber security incidents worldwide in 2014 and more than 2,100 confirmed data breaches, all organizations in today's world face cyber threats and can be the target of hacktivists, foreign state actors, criminal networks, bad actor insiders or simply fall victim to innocent mistakes. Proactively addressing cyber concerns is essential to companies of all sizes as they seek to limit their cyber exposure and in this paper we offer some high level thoughts as to how companies should manage their data assets and transfer risk as needed.

To begin, there has been one favorable development arising out of the steady stream of costly data breach activity. As a result of media focus and enormous price tags associated with the high profile breaches, C-Suite leadership and Board members are increasingly focused on this issue and are requiring that a large variety of internal resources take steps to respond to the cyber challenges of today and tomorrow.

For example, internal technology officers are being asked to make significant investments in improved and more secure systems, internal privacy officers are tasked with better education and improved training, human resources is challenged to properly vet employees and help create a culture around protecting information assets, and internal legal teams must address the myriad of contractual issues and state, federal and international statutory and regulatory schemes. Helping to manage and coordinate all of this is risk management, who is often asked to educate and inform on cyber issues and to lead efforts to transfer cyber risk where sensible.

This is a huge job made more difficult by the ever-changing issues in the cyber world. Forward thinking companies need to inventory and catalog their information assets and determine how these assets could be impacted by a cyber event. Just as companies know what real and personal property they own or lease, who maintains its condition, its locale, etc..companies should also do so with their information assets. We think this exercise is useful not only to understand exposure but also to identify assets that are obsolete or poorly protected. Gathering this data and fully comprehending the extent of your information assets will allow you to better understand your cyber exposures and where security practices need to be improved.

This process will also prove to be a valuable asset when you enter the insurance market to consider and/or purchase cyber insurance as your ability to demonstrate cyber security best practices will favorably impact insurance pricing and terms.

Cyber Assets

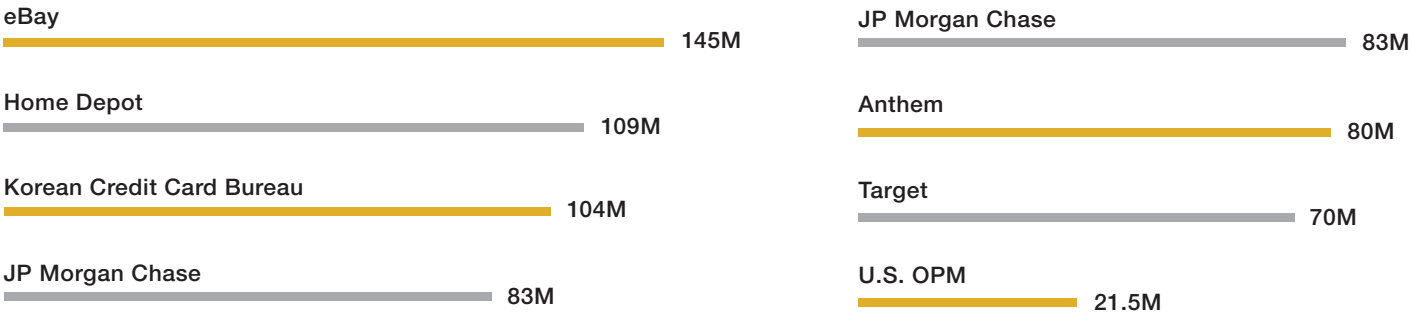
Identifying the Various Types

Personally Identifiable Information (PII) and Personal Health Information (PHI)

Every company has PII e.g. (employee data, customer data, etc.) but companies who sell directly to consumers e.g. (retailers, hospitals, banks, etc.) have large numbers of records, including credit card information, which when lost or stolen, can lead to massive costs.

Healthcare companies maintain PHI of their patients or customers, which when lost or stolen can also lead to large costs and regulatory issues. The breaches at Target, Home Depot, Anthem, the U.S. OPM (and so many others) demonstrate the massive costs for companies with large amounts of PII/PHI.

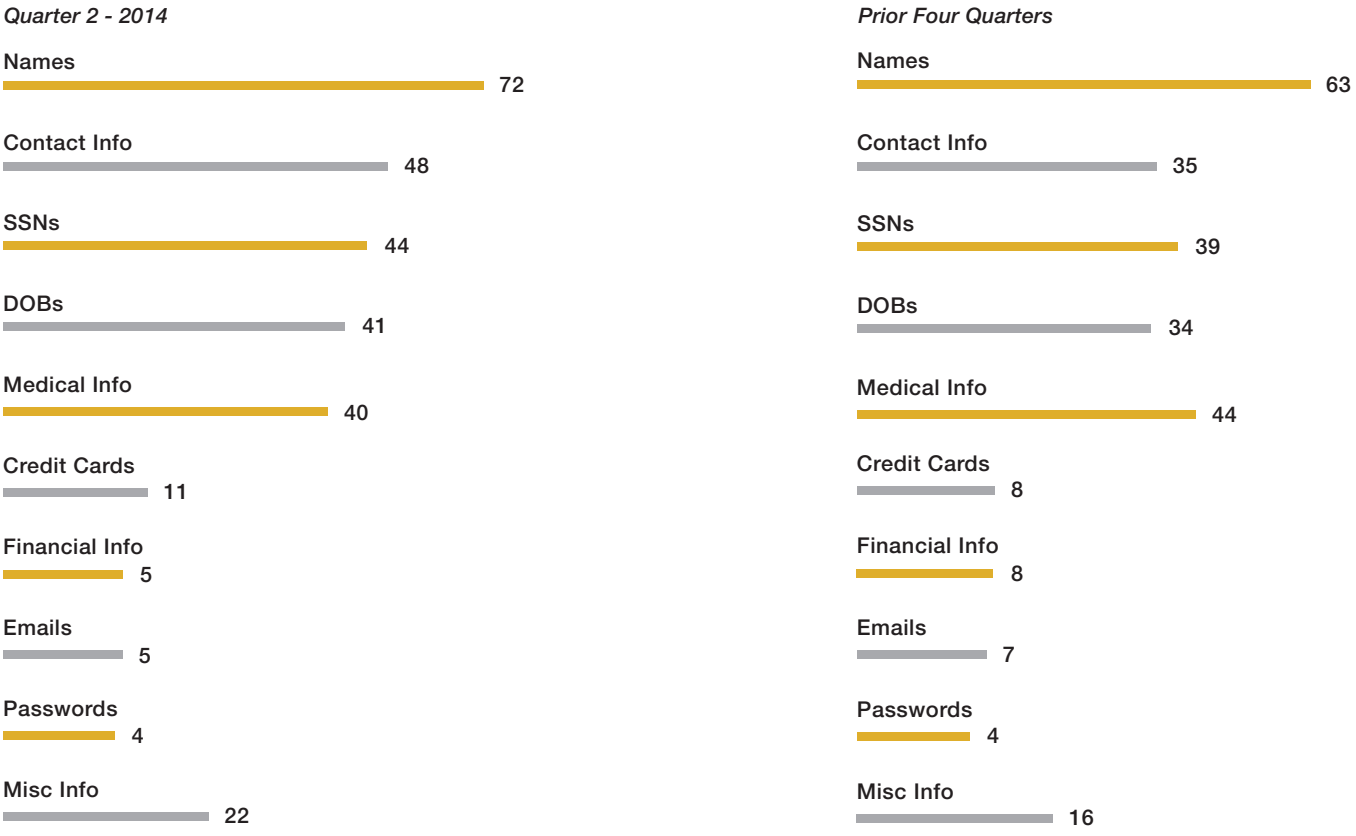
Number of Records Compromised in Major Data Breaches



Personally Identifiable Information (PII) and Personal Health Information (PHI)

This includes items of tangible value (formulas, research, corporate strategies, intellectual property, etc.) and information of seemingly little value, like email correspondence, text messages, social media posts, draft and final memos on internal matters, etc. In addition, these data assets include both your own information and that of others. Losses here, regardless of whose confidential information or its inherent value, can cause great harm – though there are significant challenges in valuing the damage. The Sony breach is an example of a cyber incident in which very little PII was accessed, but all sorts of corporate confidential information was stolen. The harm to Sony was mostly reputational as corporate leaders and others were embarrassed by leaked emails and memos. A more damaging scenario would be cyber espionage, where the theft by a foreign state actor or a competitor of intellectual property leads to a copycat product down the road and the loss of significant revenue.

Breaches by Types of Information



Software and Systems

In today's world much of the value for many companies is derived from their intellectual property, including proprietary software and systems. In addition, leased or purchased software from others and leased services from third party vendors, including cloud providers, represent huge investments and assets. Cyber-attacks on these systems could lead to degradation of network services and/or the inability to operate systems resulting in increased costs and lost revenue. Companies must understand where these systems are located, who is operating and protecting them, what data is located on them, by whom it can be accessed, etc.

Hardware

Although also included in an inventory of property, computer hardware is a cyber asset that must be inventoried and considered. Where are servers located, who is managing them, how are they physically protected, and what data sits on them? Similarly, which employees have laptops and other mobile devices? Are they owned by the company or the employee? What kind of data is on them and are they encrypted? Having a complete understanding of these questions is a key cyber risk management best practice.

Company Websites and Social Media

160,000 Facebook accounts [7] are compromised per day and that number is much larger when you include other social media sites such as Twitter and LinkedIn. In today's linked and social world, all companies need to understand what sites and tools they use, who manages the content published on these platforms, if clearance procedures are in place, and how site registration is maintained. Passwords across all corporate sites and social media accounts should be unique, complex, and lengthy and two-factor authentication should be enabled on all sites and services that allow it. These two practices will greatly reduce the chances of a hacker gaining unauthorized access via stolen login credentials.

Brand Reputation

According to a 2014 Experian study, data breaches are one of the top three occurrences that have the largest impact on brand reputation [8]. Historically, a company's reputation has not been considered a cyber asset, but in today's world the thinking has changed. This is easy to inventory, harder to maintain, and very difficult to rehabilitate once a cyber-event has happened. Ultimately, this may be the most valuable asset that many companies have. The link between revenue and reputation is strong; Deloitte's 2014 Global Survey on Reputation Risk found that reputation problems have the largest impact on revenue and brand value [9].

Your Data Held Elsewhere

Finally, just as you hold corporate confidential information of others, your corporate confidential information is held by others. What partners, vendors and government agencies hold your information? How are they protecting it and what contractual remedies do you have should something go wrong?

As you inventory these assets it is important to understand where the asset is, who can access it, who helps manage or store it and what contractual rights or responsibilities you have with counterparties in the custody chain.

Then it is crucial that companies understand how the asset is protected. Let's look at two key vulnerabilities – common vulnerabilities and exposures ("CVE") and weak passwords – to demonstrate the importance of implementing the proper tools to protect your systems. We know that many breaches occur due to exploitation of CVE but the troubling fact, according to the Verizon 2015 Data Breach Investigations Report, is that 99.9% of the exploited CVEs were compromised more than a year after the CVE was published [10]. Companies can significantly lower their cyber exposure just by maintaining an active and disciplined patch process.

Studies have also shown that two out of three breaches involved attackers using stolen or misused credentials; therefore it is critical to protect data and systems by securing and simplifying password management, including the use of encryption to protect passwords and digital file storage. Enterprise password management software is built to protect businesses of all sizes from hackers gaining entry via hacked login credentials. Administrators can reduce cyber risk by enforcing and utilizing security policies and controls such as two-factor authentication, password strength auditing, role-based access and large-scale provisioning - all within a centralized console.

Following this sort of process will help companies understand the extent to which they rely on networks and utilize data. Most companies will realize just how big an exposure they have and will understand that no matter what they do from a security and education perspective, they will still face loss scenarios of significant magnitude. Cyber insurance can solve many of these issues and forward-thinking companies are utilizing these policies as part of a holistic and proactive cyber risk management plan.

About Us

JLT Specialty USA

Jardine Lloyd Thompson (JLT) is the world's leading specialty focused provider of insurance, reinsurance and employee benefits related advice, brokerage and associated services. We provide our clients with deep specialist knowledge, advocacy, tailored advice and service excellence. Our 10,600 experts worldwide are focused on our client industries and are supported by the second largest international placement network with unparalleled capabilities and resources in 135 countries.

JLT Specialty Insurance Services (JLT Specialty USA) is the U.S. platform of the leading specialty business advisory firm, Jardine Lloyd Thompson Group. Our experts have deep industry and product experience serving leading US and global firms. Our key to client success is our freedom to be creative, collaborative and analytical while challenging conventions, redefining problems, creating new analytical insights and exploring new boundaries to deliver solutions for each client's unique business and risks.

Contact

- jlt.com
- 312.235.8223
- Steve.Bridges@jltus.com

Keeper Security

Keeper Security is transforming the way businesses and individuals protect their passwords and sensitive digital assets to significantly reduce cyber theft. As the leading password manager and digital vault, Keeper helps millions of people and thousands of businesses substantially mitigate the risk of a data breach. Keeper is SOC 2 Certified and utilizes best-in-class encryption to safeguard its customers. Keeper protects industry-leading companies including Sony, Chipotle, and The University of Alabama at Birmingham. Keeper partners with global OEMs and mobile operators to preload Keeper on smartphones and tablets.

Contact

- keepersecurity.com
- 312.829.2680
- sales@keepersecurity.com

Resources Cited

[1] http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

[2] http://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282

[3] http://thenextweb.com/insider/2015/02/05/us-medical-insurer-anthem-hacked-80-million-records-stolen/

[4] http://www.npr.org/sections/thetwo-way/2015/07/09/421502905/opm-21-5-million-social-security-numbers-stolen-from-government-computers

[5] http://www.cnbc.com/2015/02/12/year-of-the-hack-a-billion-records-compromised-in-2014.html

[6] http://www.navigant.com/~/media/WWW/Site/Insights/Disputes%20Investigations/Data%20Breach%20Q2%202014_Oct%20FINAL.ashx

[7] http://nypost.com/2015/03/01/big-brother-2-0-160000-facebook-pages-are-hacked-a-day/

[8] http://www.experian.com/data-breach/2014-aftermath-study-consumer-sentiment.html

[9] http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report_FINAL.pdf

[10] http://www.verizonenterprise.com/DBIR/2015/