Managing Cyber Risks
Not Just for Big Retailers

Both B2C and B2B Companies Need to Focus on Risk

By ChainLink Research

Cyber attacks put customers, companies and careers at risk. It's time for companies to get serious about security. Identity and Infrastructure Security, Supply Chain Risk Management; and Customer Data Security—PCI Compliance—are some of the considerations for companies dealing with cyber challenges. Often, PCI is thought of as an issue only for retailers—but every company has customers. Our systems and processes are more vulnerable than you know!

Managing Cyber Risk

Table of Contents

Ripped from the Headlines

Trust. Secure. Standards. Compliant. These are all words our customers, our trading partners, and even our work colleagues expect to hear when interacting with our information and systems. However, the last few years have seen a significant increase in the incidence of hacking, trade secrets theft, and credit card data breaches. The problem is growing.

No one wants their CEO to have to explain to customers, employees, and *the media* that their personal information is now is the hands of *who knows who.*[1] Although big retailers make the headlines, many other sectors and midmarket companies are the easiest targets. You don't have to be a retailer, per se, to be attacked, since many B2B companies accept credit card payments from customers and have customer account data on file. Financial firms and information services firms are major targets of hackers. The technology, risk management and most industries have developed both technologies and standards to protect us from these risks, yet many companies have taken only modest or inadequate steps to counter the risk of exposing their company and customers' data.

BloombergBusinessweek
Companies & Industries

Target's chairman and chief executive officer, Gregg Steinhafel, a 35-year company veteran, is stepping down, as the massive pre-Christmas data breach suffered by the Minnesota retailer continues to roil the company. The decision is effective immediately, according to a statement posted today on the company's website. John Mulligan, Target's chief financial officer, has been appointed as interim president and CEO.

The New York Times

ASIA PACIFIC

N.S.A. Breached Chinese Servers Seen as Security Threat

By DAVID E. SANGER and NICOLE PERLROTH MARCH 22, 2014

WASHINGTON — American officials have long considered Huawei, the Chinese telecommunications giant, a security threat, blocking it from business deals in the United States for fear that the company would create "back doors" in its equipment that could allow the Chinese military or Beijing-backed hackers to steal corporate and government secrets

Many breaches are due to "inside jobs." That is, employees, suppliers, or contract workers who gain access to secure information. For example, a National Security Agency employee allowed the notorious Edward Snowden, who was a contractor, after all, to use his personal computer credentials to gain access to classified information.[2] Large hacking rings often recruit disgruntled employees to provide information. The Financial Services Industry, of course, is rife with scoundrels who provide insider information.[3] In earlier reports we talked about these supplier risks (see The Challenges of Managing Supplier Risks).

Cyber attackers are becoming more advanced and hackers can apparently easily attack governments or industry with little impunity. Arrests, court cases and punishments have been few, as many hackers operate from outside the country. With the increase in hacking and global fraud, this exposure is a ticking time bomb.

We were not pleased, therefore, when we saw that across all the business sectors in our recent Business Priorities 2014 that a *secure infrastructure* was not a top priority for companies. Yes, it was a higher concern for the B2C community, but B2B barely mentioned it. Yet don't we all have security issues? Don't we all have customer data we need to secure?

[1] And recent Target CEO appears to have lost his plumb job due the recent cyber attack

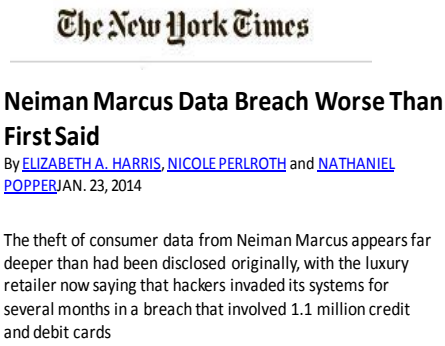
[2] And Albert Gonzales, who hacked TJX and other companies, took advantage of his position as a Secret Service informant and befriended employees inside the companies that he hacked http://www.wired.com/2010/03/tjx-sentencing/

[3] Some great cases from American Greed: http://www.cnbc.com/id/100000534

Can You Afford This?

Let's look at the cost and impact when things go wrong.

- First, there is loss of brand value and customer loyalty. The event itself is bad enough, but subsequent revelations which are bound to unfold expose the company's internal practices—or lack thereof—and shine a light where companies don't wish to be exposed.
- Loss of shareholder value—firms lose from 2% to 8% when these breaches are announced.
- Loss of sales—wary consumers flee. And often, the company has to offer discounts and incentives to woo customers back, further reducing profits.


The New York Times

Neiman Marcus Data Breach Worse Than First Said

By ELIZABETH A. HARRIS, NICOLE PERLROTH and NATHANIEL POPPERJAN. 23, 2014

The theft of consumer data from Neiman Marcus appears far deeper than had been disclosed originally, with the luxury retailer now saying that hackers invaded its systems for several months in a breach that involved 1.1 million credit and debit cards

- Lack of business continuity—disruption of your business activities. Other work may be put on hold as employees are diverted to the diagnosis and recovery work, what to say of the effect of shutting down systems.
- Recovery costs—the forensic teams swoop in—are not a cheap affair. Firms also have to put in place reputation risk and communications teams to deal with customers, trading partners and media; and customer service staff to deal with customer issues. Firms often set up services such as credit monitoring and other services for their customers to use, so additional costs mount.
- Financial loss—many companies assume their credit card company will bear the cost of the fraudulent charges. This is a false assumption. In fact, without PCI compliance, the financial institution will often sue the merchant/enterprise for cost recovery. Consumer groups also sue firms and collect for damages and loss.
- Additional fines for non-compliance with or without a breach can occur, and run from $5,000 to $100,000 per month during the period of non-compliance. This I remind you is a B2B *and* B2C issue.
- Having your merchant status revoked—commerce can be significantly impeded by not being able to process credit cards. Imagine asking your customers to pay cash! Last year saw some major retailers asking their customers to do just that—pay with checks or cash—since they could not utilize a credit card service during their recovery. That's embarrassing and also represented a loss in revenue.
- Other recovery issues associated with the cyber attack—firms whose systems have been breached often have to scan every system, file, and *employee* (their accounts and communications); and change data centers, revise websites, change mail services and ecommerce sites. Time and costs mount up.
- Establishment of compliance processes and systems—this is not a loss, per se, but given the emotional toll companies experience, they often allocate bigger budgets than might have been planned for a reliable compliance program. This has become the norm, with companies "throwing everything at it" to ensure that a breach does not happen again.
- Criminal investigations and auditing—yes. Fraud is the dirty underside of Supply Chain, with criminal rings having access to products in the warehouses, trucks, and containers in port.
- Loss of intellectual property (IP)—rogue suppliers who copy your products, from aircraft engines to running shoes.

No one can predict these events, so if the recovery is poorly managed, it further exacerbates the loss of customer trust—and future business.

Concerns about Cloud?

Of late, companies have taken to cloud computing for everything from ERP and B2B communications to hosting their IT infrastructure. Although the driver is the benefit of lower IT operating costs, when it comes to security issues, there are still some doubts about cloud. However, the fact remains that many companies do not generally have the resources for security that a reputable cloud provider has, anyway.

Some caution is merited, though. Many companies, in the pursuit of cheap hosting, have had the ISP hacked. These cheaper hosting firms are short on staff—after all, that's how they keep their costs down. As a result, they may lack the personnel required to provide the necessary vigilance.

Using third parties to host and manage technology *does not absolve an enterprise, itself, from compliance.* The real job, then, is for the enterprise to acquire the *right oversight* and the right cloud services and technology, one that can provide all the required security—from hosting certifications[4] to PCI compliance.

IS PCI Part of the Plan?

PCI compliance[5] is not just about secure payment transactions. Customer data is present across multiple systems and is used in many enterprise applications. A lot of noise (and rightly so) is focused on the point-of-sale equipment and software (POS), but it turns out that data may also be at risk while in motion. So really, the entire process needs to be secure. And with so much cloud adoption, data will be moving more—from cloud to cloud, on premise to cloud, cloud to mobile, and so on.

Even if you use third-party software, *your company is still responsible for securing and managing your customers' data throughout the whole process*.[6] As the PCI Security Standards Council says, "….PCI DSS was developed to encourage and enhance …data security *and facilitate the broad adoption of consistent data security measures,* PCI DSS, *and reporting requirements.*"

PCI compliance, then, should be thought of as the process of securing your network and application infrastructure; training your employees; and secure data management, sharing, and integration between entities. In addition, regular testing—compliance auditing—of the environment is expected. All this then needs be recorded and reported. So the *Report on Compliance* (the ROC) is a critical element of your PCI compliance program.

---

[4] Examples from tech providers can be seen right on their web pages—a good starting place is Ipswitch http://www.ipswitchft.com/; Amazon's AWS, a top hosting provider: https://aws.amazon.com/security/; or a cloud ERP player like NetSuite http://www.netsuite.com/portal/platform/infrastructure/operational-security.shtml

[5] PCI, Payment Card Industry Data Security Standard (PCI DSS) compliance, is one of those standards designed to protect customers, as well as give companies a defensible position if things go wrong. It is the "agreed-to" standard and the law of the land in certain states. In spite of that, many companies still have not implemented PCI compliance.

[6] And surely it is the responsible thing to do, in spite of any compliance or regulatory bodies.

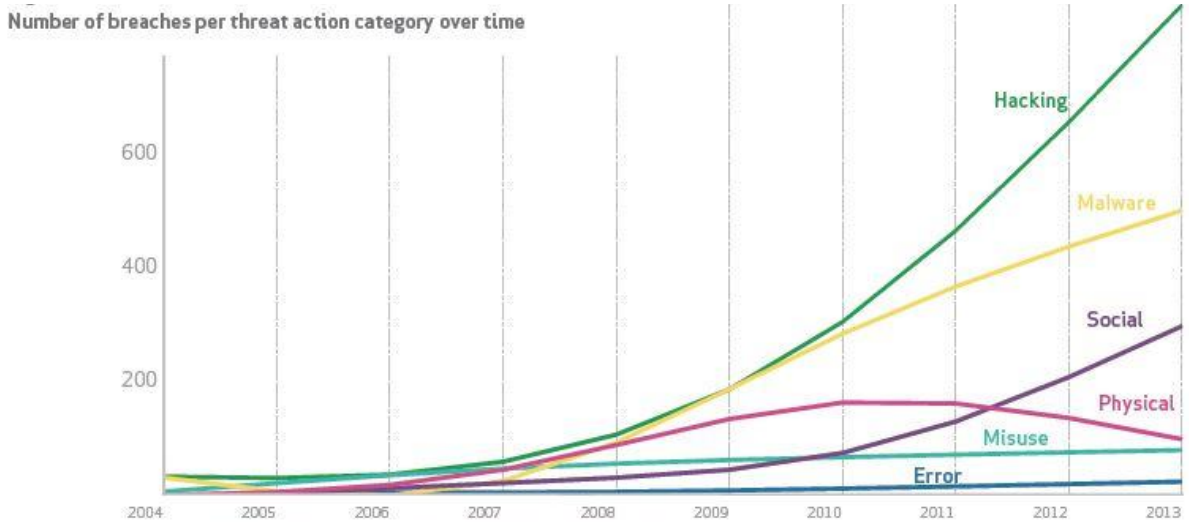
Companies are vulnerable because they often have multiple homegrown and older technologies. They also often select service providers who are “cheap,” but who may not have PCI and other security methods in place. As well, midmarket companies often lack a strong bench of compliance, security, and knowledgeable IT staff to evaluate, implement and maintain vigilant security practices. In fact most companies have no IT security. Many companies have assumed that “others" are taking care. Although the headlines are full of large companies’ breaches, *midmarket companies are the most often attacked*. So midmarket companies need to seek out service providers, not just technology, to guide the compliance process. This is especially important, as midmarket companies have been shown to be the most attractive to “hackers of opportunity.” But companies of all sizes need to take security seriously and begin to develop a roadmap for securing their most important data.

Vulnerable?

Consider where and how vulnerability occurs. Today that is in many processes and information instances. Figure 1 shows areas where data, across all industries, can be exposed and compromised.

According to the Data Breach Investigation Report (DBIR) 2013, “Findings from the past year continue to show that target selection is based more on *opportunity* than on choice. Most victims fell prey because they were found to possess an (often easily) exploitable weakness rather than because they were pre-identified for attack.”

In Figure 1, you can see that currently, hacking is by far the top source of data breaches, with malware still a big factor. Once a lightly-secured server is breached, hackers can have their way with your data. Poorly secured FTP servers are one area of vulnerability. The other is the lack of a strong policy on password protections.



Source: 2014 DATA BREACH INVESTIGATIONS REPORT

Take note: social as an access window into the employee and enterprise is a growing risk area. With enterprise social a growing area, CIOs will have to get involved in social,[7] ad hoc MFT governance activities[8] and education in these areas.

What is most alarming about these breaches is that the victims are usually the last ones to know. Others discover the breach and then notify the company, according to the DBIR report. ChainLink's research data points to symptoms respondents told us about—such as being blacklisted or having customers detect fraud—as often being the way that an enterprise finally becomes aware of a breach. Unfortunately, that lag has usually given the hackers plenty of time to help themselves to whatever data they choose, well as financially damage your customers.

Sadly, many of the breaches are assessed to have been avoidable with more diligence.[9] ChainLink's research has indicated that recovery times for these breaches can be from 3 to 12 months and consume a significant and noticeable percentage of the operating costs[10]—particularly vexing for SMBs.

[7] We discussed social governance in Is Business Social?

[8] Read Sorry, Drop Box for a discussion on securing the gateway.

[9] The 2013 study by the Attorney General's office of California determined that most systems are not properly secured and that data in motion between systems and devices was not encrypted. *Attorney General Kamala D. Harris Releases Report on Data Breaches; 2.5 Million Californians Had Personal Information Compromised* http://oag.ca.gov/

[10] Statistics vary from $150 to $280 per data record.

The Road to a Secure Enterprise

Given the likelihood of an incident, what are the steps and considerations you should take to protect your firm and your most important customer data?

Remember there are two paths here—your internal infrastructure, policies and procedures; and *the third parties you utilize* to manage your systems and/or your data: for example, a third-party fulfillment warehouse where you share information about customers, an ecommerce site you sell your products through, or the software or hosting cloud companies that manage your applications and data.

- *Risk Assessment.* First, an objective assessment of your current state is in order. Then the planning to build in best practice policies and technologies can begin. Systems, people, and the tech world at large change so frequently that, in fact, part of PCI compliance best practices is a yearly assessment or audit. Revising your Risk/Business Continuity and/or Security Plan—whatever you may call it—each year (and of course acting on the findings) ensures that the moving target—your changing technology—is being covered and that the enterprise is maintaining vigilance. The assessment may be a baseline, but then the formal audit should become part of the corporate set of *rituals.* (We will return to the topic of the audit later.) Just as you do a quarterly or year-end closing of the books, add your Risk Assessment to the list.
- *Get Qualified Help.* Companies are not objective about their processes. Or if you are evaluating the third party, you may not have the skills, personnel, or ability to evaluate a remote location (you're in Ohio and the hosting site is in California, for example.) Since there are many nuances in any formal standard, it is often hard to understand it without some experienced interpreter. (Somehow they are never as straightforward as we would like.) So it is advisable to get some experienced assistance. For PICI, for example, retain a Qualified Security Assessor (QSA), who is certified to conduct the assessment and audits and provide advice. Outside help for Business Continuity will be more objective and won't gloss over the readiness assessment. These consultants can be advisory/project management in nature or be resident in technology firms who may also provide various technology services.
- *Cloud PCI-compliant Hosting Service and Technology* needs to secure both cloud and on-premise instances. Why is this important? Today, virtually all enterprises utilize both environments (such as accounting or planning systems on premise, and B2B integration, procurement and commerce systems in the cloud). Data is frequently moved between these environments.

  Ironically, one of the largest industry organizations to record hacking incidents is Information Management, equal in number of incidents to Financial Services and more than Retail. Since so many companies have installed much of their ecommerce or other database software on hosting ISPs (who are often unaware of the day-to-day activities of their customers), these environments become easy targets. ISPs/hosts and enterprises should work together to procure a cloud-based PCI compliance technology and the necessary services to ensure that the policies are implemented and *maintained*.[11]

[11] We recommend this since, in general, ISP lack the expertise to ensure PCI. Working with the enterprise to maintain PCI compliance can provide an additional benefit for the ISP who can then market that they can support additional customers.

Here we also recommend that the assessments, auditing, and installation of such technology, as well as a review of governance used by the hosting companies be included in the contract for service with your ISP. Then institutionalize/ritualize the audit, review, and assessments, which include not only your processes, but your ISP's.

- *Ensure the software and services you procure are Secure and PCI-compliant Technologies.*[12] This covers several areas since, as noted above, there are many points of vulnerability—not just POS. For example, EDI transactions that have electronic payment data is an area often not even discussed. Then there are also documents such as credit applications, 401K or other investment documentation, customer warranty information, Product Design specs, on and on. Note, again, that some of these transactions are B2B—not just B2C. Often the documents and data associated with these transactions are passed from system to system to process data, run reports, backup, store and share data.

  Technology areas to consider are:

  - If you have POS the software should be PA-DSS certified[13]
  - A secure Managed File Transfer (MFT) system to protect data movement is a key element. Data movement is not just system-to-system transfer, but also includes downloads. Outmoded, unsecured FTP servers are easy targets, as are old and often-missed scripts written for integration or data transformation one-offs. Companies of all sizes have these types of exposures. With the increasing need to communicate between trading partners and customers, and with other services, the movement of unsecured data between entities and systems poses a huge risk.[14]
  - Purchase professional grade secure and compliant ad hoc file sharing software. Employees, in pursuit of expediency (or through a moment of carelessness), send sensitive data files through email or through web-based, so-called file-sync-and-share that circumvent corporate gateways. CIO's should face up to this need to ensure that confidential data movement is monitored so that there is an auditable trail showing by whom and to where data was sent.[15]

---

[12] Along with a *Report on Compliance (ROC)*, part of PCI compliance is the yearly audit, as mentioned above. It is expected that firms will be audited and the QSA will fill out the ROC. There are various compliance reporting criteria based on the type of organization you are and the kind of commerce model you have. The ROC submitted to the bank may actually have narrower and more specific requirements than the enterprise's overall security protection policies and efforts. Doing this exercise, though, demonstrates discipline and preparedness. Later if a breach occurs, the enterprise is in a much better position to recover and avoid fines that may occur.

[13] PCI (PA-DSS) is for software providers who sell commercial applications for accepting and processing payment cards. But as mentioned, the point of sale is not the only point of vulnerability.

[14] Some interesting breach case studies can be read about at The Privacy Rights Clearing House: http://www.privacyrights.org/data-breach/new

[15] Other weak points are due to employees using mail or the internet for file and media downloads, as well as desktop reporting and analyses that are downloaded into spreadsheets and systems and onto employees' laptops. Several major exposures exploiting this weakness have been reported by financial institutions. Outbound data monitoring and loss prevention methods and technology need to be effective. CIOs need to provide a secure gateway for all messaging, integration, and data movement.

- *Testing*. Create the preparedness plan and test it! It is not merely a best practice to plan ahead—preparation and routine testing of the response plan are essential. In general, business continuity programs often fail due to lack of testing. PCI compliance, for example, *requires* testing to be reported as part of the process (in the ROC). In fact, failure to test can result in fines or the revocation of the ability to process credit cards. Without practicing the plan, you just don't know if it will be effective. Practice exposes any plan weaknesses.
- *Data Custodian/Cloud Management Capabilities*. Rather than have your IT department install various technologies and attempt to monitor and control many applications and the network, it might be desirable to use a managed service to monitor your environment. This would be over and above your ISP[16] security efforts or any manual efforts you may employ. Most desirable would be active software and services that monitor and prevent intrusion as well as provide ongoing upgrades, employee education, etc.
- *Monitoring*. Our research at ChainLink has shown that companies can be unaware for a very long time that they have been beached, allowing hackers full access to data and systems while they innocently continue to process more data, increasing the damage to their customers and their firm. In short, a notification should occur as soon as possible. You alerting your trading partners vs. the other way around shows you are responsible and in control. In another study by InfoWorld, their research showed that only 16% of companies[17] detected their own breaches. Beyond the ongoing risk this exhibits, discovery by your credit card company generally means they will demand a forensic investigation, costing tens or hundreds of thousands of dollars. Seek technology and/or service providers who will monitor and alert your firm about issues to avoid breaches or at least to demonstrate that *you* are in control and in charge of the recovery.
- *Implementation of Security Methods and Controls*. These are both technology and process initiatives. Again start with the assessment which should reveal vulnerability for cyber, compliance and business process that can help provide insights to what investments and changes need to be made.

[16] ISPs have not always been shown to be that helpful (unless they, themselves, have gone through PCI compliance and maintain and update as standards evolve).
[17] *Data Loss Prevention Deep Dive*, InfoWorld February 7th 2012. This study also discovered that "…analysis found that attackers had an average of 173.5 days within the victim's environment before detection occurred"!

Conclusion—Creating a Risk-Aware and Secure Enterprise

Whether you are using an outside resource or going it alone, assessing your situation is critical. Then you have to put in place the recommendations that are called for by that assessment. It is not a once and done. Rather, it should be part of the ongoing business operations.

Not everything can be implemented. So the assessment and recommendations should be based on their value to the business—including your customers and reputation.[18] For PCI, specifically, you need to demonstrate compliance by undergoing the annual audit and filling out and submitting the ROC. An affirmative audit means you have taken important steps to being in control. Most PCI articles and documents dwell on obtuse compliance terminology with a specific focus on PCI. But PCI is part of a much larger issue—security, or Business Continuity Planning or overall Enterprise Risk Planning.[19] Ultimately the assessment and planning engage many functions in the company. And in executing, everybody is engaged. That is, create the methods, processes, make the investments now.

Awareness can start the process. Communicating with employees about the importance of security goes a long way. That communication should provide guidance on behavior and what to do when they see things that don't jive.

The bottom line is the impact of cyber attacks is truly devastating and the financial cost is enormous. And the risk is growing. Globally, hackers are becoming increasingly organized and many companies make themselves unwitting targets of opportunity. You don't want to be one of those opportunities!

[18] We provide some guidance here in 12 Attributes of Successful Business Continuity.

[19] In this report, we have endeavored to maintain the spirit of PCI and also provide the broader context which the enterprise should consider.

References and Further Reading

ChainLink Research: http://www.chainlinkresearch.com/risk/index.cfm

Verizon's
http://www.verizonenterprise.com/DBIR/2014/?gclid=CIa_0Lzgmb4CFbIDOgodz1sAQA

And Verizon's 2013 report: http://www.verizonenterprise.com/DBIR/2013/. These reports are different, and therefore, we recommend reading both.

The PCI Security Standards Council home page: https://www.pcisecuritystandards.org/

PCI DSS Guidance for Outsourcers:
https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf

The Open Web Application Security Project—Top Ten Vulnerabilities:
https://www.owasp.org/index.php/Top_10_2013-Top_10

Payment Card Industry Data Security Standard (PCI DSS) on Wikipedia:
http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

Several many states have specific laws about reporting breaches that impact customer data. Here you can see Massachusetts requirements:
https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h/Section1

719 Washington St., Suite 144

Newton, MA 02458

617-762-4040

Email: info@CLResearch.com

Web: www.ChainLinkResearch.com