WHITE PAPER • OCTOBER 2014

Protecting Customer Data – and Your Reputation – Against Technology-Related Security Breaches

BY SAL DIFRANCO, GLOBAL LEADER, ADVANCED TECHNOLOGY PRACTICE GROUP

DIANE COLETTI, EXECUTIVE VICE PRESIDENT

Executive Summary

With volumes of information being exchanged across all industries, data is an increasingly core component to most businesses—and, as a result, securing that data has become a crucial precaution.

Due to the threat of costly data security breaches that can potentially cause permanent harm to a company's reputation, the nature of corporate security needs, and internal security officer roles, have changed in recent years.

Historically, the security officer role primarily centered on technology and engineering requirements. However, data security concerns have caused many organizations' high-level information security roles, notably the Chief Security Information Officer (CISO), also sometimes referred to as the Chief Security Officer (CSO) position, to become more focused on risk management.

This white paper will outline the factors that have prompted the rising emphasis on data security; how security management roles within organizations have transformed to meet those needs; common traits chief security officers possess, regardless of company size, scope or structure; how companies are defining C-level security roles and how the position is evolving to meet current and future security needs.

The Dawn of Data Security Concerns

Fueled in part by e-commerce, businesses now submit, transmit and store personal data, such as credit card information, at a growing rate.

For decades, e-commerce has served as an increasingly popular sales option. E-commerce made its U.K. debut in spring 1984, when 72-year-old Jane Snowball ordered margarine, cornflakes and eggs from her local supermarket, according to BBC News, using brand new TV-based technology as part of a community council initiative to help elderly residents with mobility issues.

E-commerce premiered in the U.S. around 1994, according to CNet; the first item bought using commercially available data encryption technology, a Sting CD, was sold the same year. The method has gained popularity since.

Ecommerce is now the fabric of consumerism and business. In the first quarter of 2014, U.S. retail e-commerce sales were estimated to be $71.2 billion, according to Census Bureau data—a 15 percent increase from the first quarter of 2013.

Companies also now receive and store an increased amount of data due to the rise in customer-based business intelligence. Information can range from shopper preferences to personal health care records, which have risen in popularity due to initiatives such as the 2009 Health Information Technology for Economic and Clinical Health Act, which Forbes noted included $27 billion in health care provider incentives to spur digital record use.

Customer purchasing habits have proved particularly useful for marketing purposes. Big data—items such as customer social media interactions and product transactions—let businesses more effectively measure how outreach efforts are working and adjust future plans, according to the Harvard Business Review. Organizations that gain insight from big data typically improve their marketing ROI by 15 to 20 percent, according to an analysis by global management consultant McKinsey & Company.

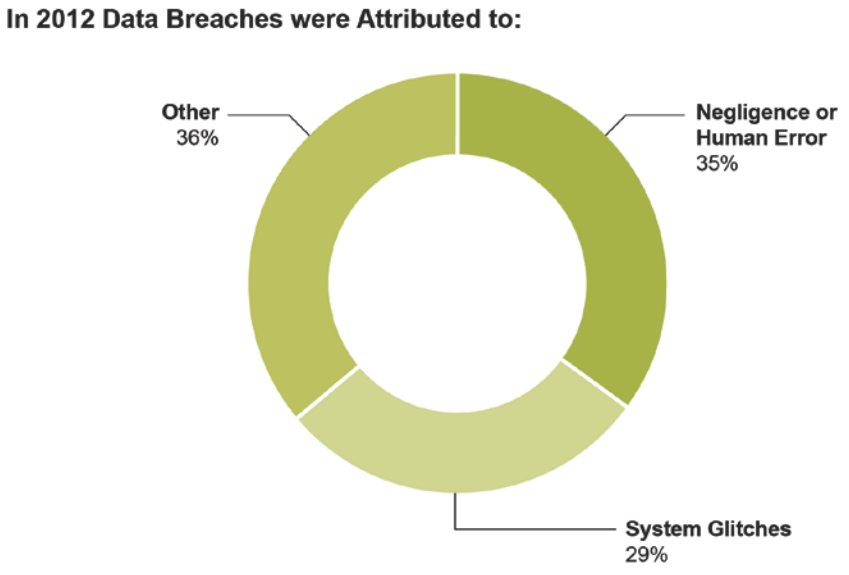
As a result, it has become increasingly acceptable to gather consumer-related information. Many companies, according to the FTC, collect personal information from customers, including names, phone numbers, addresses, credit card numbers, income information, credit histories and Social Security numbers.

Gathering and storing large amounts of consumer sales information, however, comes with a significant responsibility.

The chance that personal information may be compromised has risen as the volume of e-commerce and marketing data being exchanged has increased; and systems, unfortunately, may not always be as secure as consumers think.

Fifty-nine percent of respondents in the 2013 “Trends in Cloud Encryption” study from tech security service provider Thales and the Ponemom Institute said sensitive or confidential data that was at rest in an infrastructure (Iaas) and platform (PaaS) as a service environment was readable, or not protected by encryption. Nearly half of the companies using software as a service (SaaS) environment didn't know what measures their cloud provider was taking to protect their confidential data.

With unprotected systems in place, opportunities for errors—including accidental ones—abound. Almost two-thirds of the data breaches in 2012 could be attributed to negligence or human error (35%) and system glitches (29%), according to the Ponemon Global Cost of a Data Breach study.



Security Issues and Market Perception

In 2013, several high-profile data security breaches received major media coverage, prompting both consumers and companies to pay renewed attention to data protection:

- In February 2013, luxury department store Neiman Marcus said that 350,000 credit cards may have been compromised, due to covertly installed software, from mid-July to late October, according to Bloomberg.
- Arts and craft supply retailer Michaels' systems and customer credit and debit card numbers and expiration dates were exposed at various U.S. locations from May 8, 2013 to Jan. 27, 2014. The New York Times reported in April 2014 that the retail chain's security breach, which affected 3 million customers, involved a point-of-sale system failure. Michaels estimated that hackers may have accessed information from 2.6 million cards, roughly 7 percent of the cards used in U.S. Michaels stores during that period, according to the New York Times.
- In discount retailer Target's 2013 security breach—which Businessweek referred to as the biggest retail hack in U.S. history—Target says approximately 40 million credit and debit card accounts and up to 70 million individuals may have been affected. The retail chain discovered in mid-December 2013 that criminals had accessed customer credit and debit card information in its system dating back to late November 2013; a subsequent investigation found other information, including e-mail addresses, phone numbers, names and mailing addresses, had also been taken.

Data security breaches can have a lasting negative financial, branding and consumer opinion impact. At least one lawsuit has been filed in connection with the Neiman Marcus security breach, according to Bloomberg. After Target's November-December 2013 issue, sales declined 40 percent in the fourth quarter, according to the New York Times.

During the holiday shopping period, Target's number of transactions showed the biggest decline since Target had started publicly reporting that information in 2008, according to Businessweek. Customers and banks, Bloomberg Businessweek said, have filed more than 90 lawsuits for negligence and compensatory damages; the retailer also spent a $17 million net expense responding to the breach, according to its fourth-quarter report to investors.

Security breaches are something companies aren't aware of; generally, they know they face data security risks, and most, if not all, have stringent security methods in place to protect consumers.

However, hackers are skilled, inventive criminals—and they sometimes successfully break into seemingly secure systems. Online crime has become so widespread that it currently comprises 0.8 percent of the worldwide GDP, according to U.S. News & World Report.

The way modern hackers operate makes anticipating and handling threats difficult. Many attacks originate from foreign countries and can be hard to trace, due to techniques hackers have developed in the past decade—such as Tor anonymizer web connections, which encrypt and send data to various locations to throw investigators off their trail, according to The Economist.

Despite persistent cyberattack threats, companies sometimes underestimate security risks and implement less-than-ideal systems that provide only minimal protection.

“Some companies will add a checkbox to say, ‘Am I compliant?’” says Julian Waits, president and CEO for cyberthreat solutions provider ThreatTrack Security. “The problem is, compliance, most often, doesn't equal security.”

Hackers cost companies and consumers between $375 and $575 billion a year, according to study from the Center for Strategic and International Studies—a number that U.S. News & World Report says only stands to increase as Internet use continues to grow.

Ironically, publicity surrounding the recent increase in security breaches may have actually helped prevention efforts.

According to the Financial Times, the post-breach resignation of Target’s chief information officer helped highlight the growing focus on senior executives’ data security-related responsibilities.

The potential impact a high-profile security breach can have on both overall business and a CEO’s position has prompted both board members and chief executive officers to pay more attention to how data and risk security are being handled.

High-ranking corporate officials no longer automatically just trust that things have been adequately taken care of, according to Paul Crosthwaite, vice president and chief information security officer, governance and application support at fixed annuity market leader Athene USA.

“There is an increased level of interest and awareness at an executive/board level,” Crosthwaite says. “Security breaches, cyber security and reputation risk are topics the modern CEO needs to understand.”

With a heightened focus on security risks, CEOs want a solid candidate on board who they can trust to handle their company’s comprehensive data protection needs.

As a result, the CISO role, once a relatively insignificant IT department member, has become a bigger player in the overall strategic operations at many organizations.

C-level Security Officer Roles’ Evolution

The CISO role isn’t a brand new position. In its previous incarnations, the title may have differed—a CISO may have been referred to as the vice president of security or IT in the early 1990s; in the past, the role also frequently involved more targeted technology-related duties.

However, as technology became increasingly essential to running a business—and certain elements, like cloud-based computing, introduced new security concerns—the CISO role began to involve tasks like running all hardware and software systems.

"The cloud has presented new opportunities, but also new challenges,” Crosthwaite says. “The point of entry and threat vectors are more varied than they used to be."

Over time, as technology-related security risks that were poised to affect multiple operational areas expanded, CISOs had to understand the organization's technology needs and determine more proactive, strategic ways to integrate business operations with IT strategy.

"In the past, you had a chief risk officer who was more worried about operational risk and compliance, and a CISO/CSO who was more concerned with technological risk and compliance," Waits says.

Today, more companies are combining aspects of those roles. "If you have risk people working with a tech person who understands the nature of the business and risk to the business, things will be tied together [better] if they're managing things as one consistent loop, and not disjointed functions," Waits says.

"The role has changed fundamentally," says Phil Gardner, founder and CEO of IANS, a Boston-based information security decision support company. "It's a far more expansive, tougher position. The CISO officer has moved from a technologist to being a business risk executive."

The CISO role—referred to as a CSO at some organizations—is now a staple on many management teams. In North America, 65 percent of organizations employ a dedicated CISO, according to the 2014 PwC Global State of Information Security Survey.

As information management professionals' responsibilities have increased, their reporting structure has followed suit. CISOs have been called more often in recent years to sit at the executive table. "Chief security officers traditionally reported to the CIO; they're now reporting to CEOs," Waits says.

The move can indicate that the CISO position isn't specifically limited to IT duties. As cyberthreats increase, and the business world continues to collect, use and share more information electronically, the chief information security officer role is likely to become even more important—and require an individual with the skill set to consistently protect both physical and cyber-centric data.

"Organizations are asking for CISOs to really spread their wings and not just think about the technology they can employ, but to really understand what the business risks are and what the business is trying to do—how it will grow and win in the marketplace, what the associated risks are and how you can mitigate them," Gardner says.

The result: a more well-rounded, big-picture take on company security needs, financial targets and other goals.

"Ultimately, once the dust settles, you're going to find a maturing CISO who thinks much more like a businessperson," Gardner says.

Crucial Chief Information Security Officer Skills

CISOs' backgrounds may differ. They don't all necessarily possess masters and doctorates in information security; however, as Richard Starnes, president of the Information Systems Security Association UK, told Computer Weekly, educational experience in fields such as business, hard sciences and law enforcement can be beneficial.

The classic school of thought involves a candidate who is well-versed in technology security standards and practices; but that's not the only indicator of CISO success, according to Crosthwaite.

"While understanding technology is important, being a technician isn't," he says. "[The CISO] needs to understand the business: defining value, aligning a program with business needs, developing appropriate performance standards and evaluations—someone with a good sense of balancing risk and reward."

Generally, CISO roles often share some major responsibilities and traits, even across organizations of varying sizes, including:

- **Strong management skills.** C-level security officers' central job involves controlling enterprise-wide risk to the company's infrastructure, internally and externally. Management skills are key, as the work can involve overseeing a network of security directors and vendors who safeguard the company's assets, intellectual property and computer systems.
- **The ability to handle regulation and compliance initiatives.** Monitoring incident response planning efforts is often an important duty; C-level security officers also need to be able to manage global security policy, standard, guideline and procedure development and implementation to ensure ongoing security maintenance.
- **Flexibility.** As hackers become more security system-savvy, business grows and online transactions and information exchanges increase, a company's security needs will transform. CISOs need to be able to address current and changing needs. "The CISO job is one of constant negotiations," Crosthwaite says. "You work in imperfect conditions, but you have to be able to deliver value and protect the business, despite those conditions."
- **Presentation skills.** In addition to possessing comprehensive knowledge about data systems and threats, C-level security professionals must be able to break down complex principles and situations into digestible, easy-to-understand information. "You need a good ability to translate," Crosthwaite says. "Most of what we do is intensely technical, and most of your audience is often not so technical."
- Strategic thinking skills. Strong CISOs are, Gardner says, all very qualified technologists who can think strategically. Even if they aren't up-to-date on the very latest vendor offering, they understand major important concepts.

According to Gardner, CISOs also need to have strong budgeting and management skills—and are ready and willing to be involved in operational decisions made by the board or other company ruling body.

“CISOs need to have a seat at that table,” he says. “If they come in and don't understand [how the company works], they won’t get very far.”

Building internal excitement about data protection can be challenging when, as Crosthwaite puts it, employees “assume you’re a police officer and your job is to punish people;” but providing a way for the CISO to contribute direct, influential input for a company’s future course is a necessary component for a risk management program’s overall success.

“Managing information security is not just about preventing harm for the business, [which] is a negative description,” Crosthwaite says. “It is also about providing the business with comfort and assurance of the confidentiality, integrity and availability of its information.”

The Future of the Chief Information Security Officer Role

As the person responsible for your company’s data collection, use and storage, your CISO should be determining where your organization might be exposed to risk on an ongoing basis.

Information security officers can improve their business acumen through executive education programs, online coursework and other similar resources. Potential areas of focus could include management skills, marketing, finance and project management, Gardner says.

Waits suggests becoming active in communities like the Information Systems Security Association (ISAA), that involve like-minded peers sharing information at meetings and conferences.

If your company is involved with e-commerce/e-procurement or electronic health records, your CISO needs to be investigating your biggest internal network security risks, or ones an external provider might pose, to ensure your system is safeguarded. CISOs need to determine if the way customers, suppliers or other associates submit data to the organization through mobile devices is secure—and consistently be aware that security threats are constantly evolving.

Hackers’ tactics are evolving to attack the weakest points in any industry—through user passwords, API or even weakly protected printing information, according to information security industry publication SC magazine; CISOs need to be prepared to make frequent system reviews and updates as needed to prevent ongoing threats.

In some cases, widespread institutional changes may be necessary to ensure protection. Employees who work from home—and other employees who connect wirelessly—may need to be treated as remote workers who need top-shelf laptop protection.

Companies may also find they benefit from additional training on security breach warning signs. “Even though spear fishing attacks are becoming more and more sophisticated, there are things you can recognize—such as, if you hover over this link and the actual address it resolves to very different than the link listed, you shouldn't click on this button to share information,” Waits says. “Technology may not catch that—but a person will.”

With the proper mix of technology competence, business practices and measurement capabilities, CISOs are becoming truly resourceful, adaptable security leaders, according to IBM’s Center for Applied Insights. Some industry players, such as Brown University’s CISO, David Sherry, expect the information security leadership role to fully transition to risk and governance work in the next few years.

Regardless of the amount of risk control your chief information security officer currently handles—or what protection methods your organization ultimately utilizes—support for your security program needs to come from the top down.

“The biggest issue is that other C-level executives don’t always see the security team as business enablers,” Waits says. “They see them as people who add more complexity and put things on mobile devices that slow executives down when they’re in an airport checking e-mail, instead of understanding some of those technologies are necessary to protect assets.”

Conclusion

Companies’ increased cyberdata usage and exchange has presented a number of new, constantly evolving information security concerns. Data security breaches can be costly—and have a major negative impact on a company’s business.

Most companies are aware data-related security threats exist; however, if they haven’t experienced any issues, they may not be fully prioritizing data protection. Qualified, experienced C-level information security officers can help companies prevent potential security breaches by addressing any current—and future—system weaknesses. As technology use has increased in recent years, the CISO role has evolved to include a growing focus on anticipating upcoming threats and assuming a truly strategic role within the organization.

Unfortunately, security threats are constantly surfacing; and, as a result, your suppliers, potential clients and current customer base will continue to ask what precautions you’re taking, and expect you to have infallible systems in place.

Being proactive—and prepared—by employing a thoroughly ingrained, qualified CISO and having cyberdata security safeguards in place can help your organization prevent a security breach-related issue—and successfully avoid potentially negative PR, a devastating customer loss, and vastly diminished revenue.

Established in 1989, DHR International is one of the largest retained executive search firms in the world, with more than 50 offices around the globe. We conduct search assignments at the board of director, C-level and functional vice president levels. DHR's renowned consultants specialize in all industries and functions in order to provide unparalleled senior-level executive search, management assessment and succession planning services tailored to the unique qualities and specifications of our select client base.

DHR International
Worldwide Headquarters
71 South Wacker Drive • Suite 2700
Chicago, IL 60606
P 312.782.1581 • F 312.888.9346
www.dhrinternational.com