



# Data Theft and PCI Compliance

Simon S. Lam

Year 2005 was conspicuously recognized as the year of “Data Theft,” exposing more than 50 million Americans to the potential of identity theft. So far, data theft in 2006 continues to run rampant, making this year possibly even worse. According to the Privacy Rights Clearinghouse, since February 2005, almost 85 million people have had their personal information potentially exposed by unauthorized access to the computer systems of companies and institutions.

Recent reports of the Veterans Affairs’ embarrassing data leak and a string of Ernst & Young stolen laptops renew serious concerns about how government and enterprises protect individual sensitive information.

According to a recent International Data Corporation (IDC) 2005 Enterprise Security Survey, 40% of respondents reported a successful attack, and 30% reported 10 or fewer successful attacks against their systems. Additionally, 50% of respondents from large companies stated that they had more than 11 successful attacks on their enterprise. The clear message from this survey is the overwhelming prevalence of at least one successful attack on the enterprise. (Diagram 1)

With the rapid advancement in technology,

data theft is the new “invisible crime” threatening every business. Enterprises are being challenged by the ever-increasing complex hacking techniques. At the same time, they have to guard against the old-fashion thieves who are making off with personal data on hundreds of thousands of people by stealing laptops and computers from cars and offices.

## Data Theft

There are two main forms of data theft: the first being stealing someone’s identity, and the second being the theft of information such as intellectual property and proprietary information like customer lists, research and development, financial data, and personal information. All these are all highly lucrative to hackers.

The most common form of data theft to obtain personal information that practically all individuals with access to the Internet are familiar with is Phishing. A typical Phishing scheme will use a seemingly legitimate E-mail to deceive the recipient into thinking it is a message from a trusted company or government agency rather than the con artist who is actually behind the communication. Their intent is simple: get the potential victim to disclose his or her account information,

credit card account numbers, Social Security number, passwords, and/or other sensitive information.

Consumers must be vigilant about Phishing and avoid exposing their sensitive information to the wrong hands. (For more information, visit the Anti-Phishing Working Group Web site: [www.antiphishing.org/consumer\\_rec.html](http://www.antiphishing.org/consumer_rec.html).) IT managers should train their users early and often about how to avoid social hacks such as Phishing.

The kinds of data theft that consumers cannot guard against are those data thefts and leaks from enterprises or institutions with whom they entrust their personal and credit card information. With the cost of the data breach during the past 15 months not yet clear, lawmakers and other parties are keeping a close eye on the impact the leaks are having on customers and on the credit card industry.

Related to any data breach, retailers have more to lose than consumers. When a fraudster makes purchases with an individual’s card, the maximum the cardholder has to pay is typically the first \$50 of unauthorized transactions or nothing at all. Retailers, however, in many cases have to cover the loss—a potentially heavy burden given the large number of potential identity thefts. Web retailers’ exposure is considerably higher because they do not see the customer’s credit card and cannot ask for a signature or an ID. As a result, Web retailers end up bearing more fraudulent transaction costs than brick-and-mortar stores.

Needless to say, businesses that are taking credit card or other electronic payments would have the best interest to protect critical databases to avoid embarrassing incidents as well as comply with the Payment Card In-

Diagram 1

How many attacks, including (but not limited to) viruses, hacks, Trojan horses, and worms, against your company’s enterprise network defenses successfully breached security in the past 12 months?

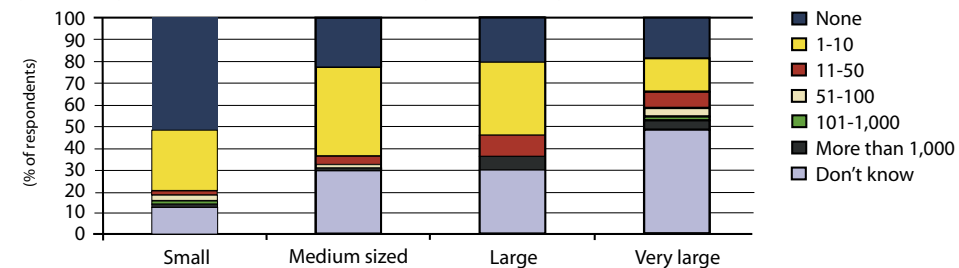


Illustration by Dave Swang for The Partner Channel.

dustry (PCI) Standard. The PCI Data Security Standard is intended to protect cardholders' credit card account and transaction information from being leaked to the general public or the wrong entities. Merchants who do not comply could face restrictions by the card brands and may be subjected to hefty fines.

To get a better understanding of how to build and maintain a secure network, IT managers should understand the tools and tricks of the hacking trade.

#### Common Vulnerabilities

There are a few common exploited vulnerabilities used by hackers to gain escalated user privilege within the IT infrastructure.

One of the most commonly exploited vulnerabilities is the buffer overflow. Buffer overflows occur when too much information can be written to a predefined memory buffer, causing a program to fail to gain escalated user privilege.

According to the SANS Institute, the leading computer security training organization, remotely exploitable buffer overflow vulnerabilities continue to be the number one issue that affects Microsoft Windows® services.

Another is a format-string vulnerability that occurs when user-supplied data is handled incorrectly and is passed by a program directly as a format string. A talented attacker can then craft a string that overwrites

memory locations with the attacker's input.

One hack that should be high on IT organizations' most-wanted list comes by way of root kits, a type of hack that is widely known in the Unix community but that now appears to be headed straight for Windows desktop and server systems.

Root kits are programs designed and written by clever hackers. These programs appear to be something you know and trust but instead hold hidden features that trick the person running them into believing the output is truthful, allowing the intruder to harvest login passwords, conceal their files, network connections, and processes. Since the files had the same timestamp as other programs in the same directory, and appeared to have the same checksums (via another Trojan horse technique), an inexperienced administrator would see nothing out of the ordinary and give up, thinking the system to be "clean." It derives its name from the Trojan horse programs that were bundled together in the form of "Root Kits" for Sun's Berkeley flavor of Unix (SunOS 4) and later for Linux.

#### Defaults, Back-doors and Mis-configuration

There is a whole class of hacking "tools" that is nothing more than expert knowledge of a particular application or operating system combined with poor security practices

by the IT implementer.

Early in the systematic stalking of an IT resource, hackers will enumerate and identify systems in a network, looking for something of interest. After identifying an interesting target, smart hackers will gently test to see if any part of a system was left in a default configuration. Such a configuration provides easy back-door entry into what might look, from the front, like an impregnable fortress.

#### Network Security Exploitation

Hackers often exploit network security weakness by scanning, sniffing, and probing network openings and weaknesses to gain access and control to your computing resources to install malicious software like spyware, adware, Trojans, or keyloggers on users' systems.

Recently, the Domain Name System (DNS) is another area of vulnerabilities being exploited. The DNS was created based on a confidence model developed in an era of mutual trust that is vastly different from today's generally hostile Internet environment. Consequently, the DNS is prone to many types of transaction attacks that take advantage of that trust, including cache poisoning, domain hijacking, and man-in-the-middle redirection. For example, DNS cache poisoning vulnerabilities were exploited to redirect users to malicious domains to install malware on users' systems. Open recursive DNS serv-

ers are frequently being used as Distributed Denial of Service (DDoS) reflectors, providing a huge amplification factor.

#### Encryption and Vulnerability Management

With so much at stake, IT Managers must be vigilant on network security and create an enforceable security policy. Today, IT managers are conversant with access controls measures for their users, using firewalls and universal threat management to secure their network perimeters. For those who are entrusted with sensitive personal information, two additional key areas they must master are encryption for all sensitive data and vulnerability management with continual security scanning for vulnerabilities and intrusion detection within the IT infrastructure.

Many ERP systems do not provide adequate encryption tools for IT managers to safeguard sensitive card data, e.g. Microsoft Dynamics™ relies on an ISV like Nodus Technologies, Inc. to provide encryption to their customers.

Automated encryption via intelligent agents should be used to apply appropriate levels of encryption to credit card holder information before storage. The key for its successful deployment is to ensure users would not need to do anything extra, that the system will handle the encryption and decryption automatically. Encryption must also be applied on individual PCs and notebooks to secure the same informa-

>> **Once Upon a Time, continued from page 21**

employees and customers to invest in your future. Stories are also a way for the owner to instill his/her passion and vision of the company throughout the fabric of the company. The Blue Moose Restaurant in East Grand Forks, Minnesota has such a strong story about customer and community that it is now one of the few \$1M restaurants in the region. They built their story on old fashion service and community. This story led them to hire the right people. These were not the most seasoned wait staff in the area. Those people often carried a price tag of traditional restaurant service. They needed a person that carried a passion for the customer. There is a difference. Isn't there a difference between the business consultants that can sell business services than the business consultant that can install software? Same story.

Stories are different than business visions. Stories are about customers and people, and visions are often about futuristic business directions. One of the most compelling business stories is about a small local retailer that built their business practice on finding jeans that actually fit. They built their business on the gap in jean sizes that existed in the market. Today they are one of the biggest retailers in the specialty markets--Gap, Inc. of course. Their story was about filling a customer need, and that need was finding a pair of jeans that actually fit. Now Gap jeans are outperforming the historical trend leader, Levi's, hands-down. Once again, what is your story? Is it one of finding a gap in your customer's needs?

tion. The added bonus for encryption for all credit card information on all PCs is that when they are lost or stolen, you have an added level of security that may protect the sensitive information from being dispersed to hackers.

Data theft is alarmingly easy when the IT infrastructure is left vulnerable to attack. Vulnerability management needs to be an integral task of every IT department. Subscription to automated daily vulnerability scanning tools, such as ScanAlert or an open source offering like Nessus, is a good way to reduce the burden on the stressed IT manager and to keep network devices, servers, and desktop systems in top defensive form.

PCI Standard compliance requires that any business that processes credit cards, whether it is a merchant bank, restaurant, or service provider, must be able to encrypt and properly handle credit card data. It encompasses a self-regulated security validation to an extensive third party onsite audit, depending on the amount of cards the enterprise processes. Violators may be subject to fines up to \$500,000. Based on a recent survey by Javelin Strategy and Research, the average amount per identity fault costs \$6,383 and an average 40 hours of consumer's time to resolve. Protecting individual card information is a serious business. It is not only a requirement by the Payment Card Industry, but also an obligation of every one involved in the IT industry. ❄

Building a story about your company starts with the customer. If you don't know what your story should be, interview some of your customers. Ask them what gaps they need filled. What are their biggest pain points? Ask them what they need to be successful and serve their customers in the future. Take that story back to your team, and let them create it and massage it with you. Best practices in story telling often follow a very predictable path, fraught with chaos. It starts with uncovering a future customer need. Keep the current engine running, but be on a conscientious path of transitioning in the future.

Engage in some "think tank" type activities. One group and I visited a NASCAR racing team when trying to craft a story about working as a cross functional organization. The analogies were incredibly mind provoking, and for most participants, the work was unforgettable. One group and I went sailing, since the customer need was learning to race as fast as they could against the Y2K issue.

Another way to build a story is to document the "superior" reason you are business. It really isn't just to sell software, is it? If it is, you probably have a retention problem. That's pretty boring, and most people don't wake up and say that their contribution to the world is "selling debits and credits." (Sorry to all those accountants I just offended). However, a story about software that was ultimately compelling was a story about how selling software to small businesses was actually changing the world. If you could help a small business owner be more efficient in its

payroll, he/she just might spend more time with their family. If you could help a small business owner generate reports that he/she could readily access and understand, you may be saving his/her business. If you save the small businesses across the world, you save the entrepreneurial spirit as well as the communities that are built on these businesses. Now, many of us have heard Doug Burgum tell that story. IT is compelling, isn't it? It is one that attracted some of the best industry experts and customer focused Partners and employees.

Getting to the future is going to take innovation and risk that is focused on the customer. It is more than a plan. It is even more than the best strategic plan. It is about telling your story. It is about taking the time as a CEO or business owner to create a compelling story for your customers, Partners, and employees. It's about passionately believing and telling your story every chance you get. It's about risking your reputation on a future that may be different than the present. It's about drawing your employees and customers along with you because you see something they yet don't. It is about YOUR story on GETTING TO THE FUTURE. You DO know the business and the industry better than anyone else. Do you trust yourself enough to risk it all over again? Barnes and Noble did!

For more information on building your company's story, please contact Pam McGee at pmcgee2@hotmail.com or 701-361-9270 for an initial conversation. ❄

**eTransit**  
integration with Microsoft Dynamics GP

Help your clients save time and money  
for that much needed vacation.

- Works in conjunction with eConnect
- Fast and accurate integration with Microsoft Dynamics GP, running up to 2000 transactions/minute
- Programmable automated integration
- Permits outside data sources to easily create back office documents and transactions
- Offers automated database-to-database integrations
- Supports integrations into multiple company data bases while keeping history of all integrations

*"To integrate or not to integrate was no question. We had to integrate, and when we found the cost-effective solution of eTransit for Microsoft Dynamics GP, we knew that was the way to go."*  
Mick Gunter, VP of Operations, Primo Water Corporation

Contact InterDyn - Artis for more  
information and schedule a web demo.  
888.841.0505 ext. 201 - [www.etransitintegrations.com](http://www.etransitintegrations.com)

**Microsoft**  
GOLD CERTIFIED  
Partner