BROWN SMITH WALLACE
CONSULTING
GROUP

Brown, Smith Wallace Consulting White Paper

# Keeping Data Thieves Out:

## Best Practices in Data Security

July 2010

BROWN
SMITH LLC
WALLACE
A MEASURABLE DIFFERENCE™

BROWN SMITH WALLACE
CONSULTING
GROUP

## ABSTRACT

Now that we are living in the electronic age, it is more important than ever to keep your organization's data safe and secure. Customer data, employee data, cardholder data, and other proprietary information such as sales and marketing plans, target accounts, and product and service information all need to be kept away from people who want to steal it for their personal gain or to do your organization harm. But where do you begin? How do you put in place the necessary policies, procedures, and barriers to protect against those who want to steal your information?

Many large organizations have gotten good at this discipline commonly referred to as "cyber security." They have put the proper systems in place to protect employee and customer data, and they know what to do if a security breach occurs. They have gotten so good that small and midsized organizations have become much more attractive targets to computer hackers who can easily tap an unsecured system and steal customer and employee data, using it to create new identities, purchase products and services, or commit other crimes. If you think it can't happen to you, think again. No organization is insignificant, and no system is impenetrable when it comes to cyber security. As one information technology (IT) security expert said recently, "When it comes to business systems, the only one that is 100 percent secure is the one that is unplugged."

It is vital for organizations of all sizes to protect their data. And now that larger organizations have become vigilant about it, there is a trickle-down effect occurring, putting more pressure on smaller organizations to take the same precautions. Also, compliance laws and other regulations are affecting more and more organizations as cyber security takes on a prominent role in our society in general.

This paper will answer two important data security questions that plague many small and midsized organizations today: First, what do I need to do to protect my valuable data? And second—and perhaps more importantly—where do I begin the process? We will also examine the costs associated with a data security breach as well as the costs and benefits of investing in systems that can protect your valuable data.

## INTRODUCTION

Organizations of every kind are under daily threat of a data security breach. Quite simply, data thieves are everywhere, and they have myriad methods for obtaining information for their personal gain. You are not immune to this problem, because you have valuable information that thieves want—employee data such as social security numbers and financial information, for example, and customer data such as credit card numbers. Protecting this kind of data is no joke: A security breach at your organization means lost business, a damaged reputation, and potentially hundreds of thousands of dollars in real costs for even the smallest organization.

There are two primary threats to your data: Outsiders and insiders. Outsiders (also called "hackers") are people on the outside of your organization who try to gain access to your information through various methods—by accessing unprotected customer data through your website, for example, or by hacking into your unencrypted wireless network to access confidential human resources documents. Insiders are trusted employees who abuse their authority by stealing that confidential data they have access to day in and day out; insiders are also the rank-and-file employees who gain access to information they should not be allowed to see and then take it for their personal use. In either case, your organization is at risk of losing valuable data—and of losing your employees' and customers' trust if you are careless about keeping that data secure.

If you have an e-commerce site—a place where customers can buy products online—this is probably your biggest security risk, says IT security expert Ron Schmittling, a principal in the Risk Services practice at Brown Smith Wallace LLC, where he leads the firm's IT security and privacy practice. As a result, web application security is of the utmost importance because your online store is an easy entrance point for hackers.

But even if you don't have an e-commerce site, you are still at risk. Consider this scenario: A distributor is running wireless networking inside its building. The distributor has one or two servers that house all kinds of documents: Human resources files such as applications, resumes, benefits forms, and so on, and customer files that include the names, addresses, and credit card information for hundreds of customers.

"If I'm a hacker on the outside and I just happen to be driving by with a software program up and see the wireless access point for XYZ company with no encryption [or other security around it], I'll park in their parking lot and keep banging away at this wireless network until I get enough information to hack into that access point," Schmittling explains. "Now I have access to [the company's] internal network and I'm able to move toward where those servers are and find information relating to employees, et cetera. Now I have enough points of information to create another identity or sell the information on the black market."

Schmittling emphasizes that you would never know what this hacker was up to, because he or she would be in and out of your parking lot within minutes.

To combat these scenarios, a "layered approach" to security works best, explains Schmittling. This means implementing solutions on different facets of an organization and its network. This could range from software coding to network protocols used to operating systems in use, as well as to how applications are configured, user-activity monitoring, and the program you have in place to govern your organization's security practices. For example, running antivirus software only on workstations is not a layered approach to combating viruses. However, running antivirus software on each workstation and server, as well as applying content filtering (which screens and excludes certain content from email or websites) on a proxy server (which acts as an intermediary for requests going to your main servers), is considered a layered approach to addressing viruses.

The bottom line is that you need to protect against Internet-facing and non-Internet-facing threats. If you don't, you risk losing customer and employee loyalty, damaging reputations, and facing the potential costs of failing to adhere to laws and other regulations surrounding cyber security. The remainder of this paper touches on all of these issues, keeping the focus on answering the two key questions mentioned at the outset: What do I need to do to secure my data? And where do I begin the process? Let's start by looking at a real-world example of a distributor who was a recent victim of data theft.

## WHEN YOUR ORGANIZATION IS BREACHED: A REAL-LIFE EXAMPLE

DLP Lamp Source is a small, California-based distributor of replacement parts for televisions and projectors. The distributor conducts business online through an external-facing website where customers can search for and purchase products, entering their credit card information once they have logged on with a user name and password. In July 2009, DLP reported to government authorities that the order administration portion of its e-commerce website had been compromised and that customer information was stolen. According to published reports, DLP initially contacted law enforcement agencies to investigate the incident and discovered that customer names and credit card numbers were taken from the company's system. Once the breach was confirmed and the source where the theft occurred identified, the company's website server was locked down and its data storage tables cleaned of any cardholder data.

DLP's next step was notifying its customers, which the company did in a formal letter explaining and apologizing for the incident. DLP also offered customers an online credit monitoring service for one year at DPL's expense, as required by law in many states.

Although public documents on this case do not reveal the exact cost of the incident to DLP, it is safe to say it was no small affair:

- DLP most likely hired a computer forensic professional to get to the bottom of the incident
- DLP incurred the costs associated with fixing the problem (testing the system, installing new protective hardware and software, and so on)
- DLP lost sales while its site was down (not to mention the loss of sales going forward as skeptical customers think twice about ordering from the DLP website)
- DLP incurred the cost of the credit monitoring service for customers
- And the list goes on

No organization can afford these costs. In DLP's case, the firm is a small company, with fewer than 20 employees; based on this scenario, it gets progressively worse—the larger your organization, the more you have to lose. But regardless of company size, no owner or president needs the hassle of putting out this kind of fire. According to public accounts, DLP took the right steps to address the problem; a year later, the company is still in business, its website up and running and ready for orders. But there is no doubt that DLP is more cautious about its online security systems these days. And the firm is likely to be taking precautions it never thought necessary before.

## PRECAUTIONARY STEPS

Experts agree that taking a proactive approach to IT security is the best way to stave off a security breach. That means having an IT security policy in place at your organization, developing or reinforcing that layered approach to security that Ron Schmittling advises, and testing your IT systems for "holes" on a regular basis. There is a lot at stake, so there is a lot involved—and it should all start at the top.

"A lot of people think this should start in IT, but really, data security and information security is a much larger issue," explains Schmittling. "It's really an enterprise-risk type of issue."

Schmittling advises driving security policy from the ownership or CFO level; this puts control in the hands of someone with a broad perspective on your organization and how data security affects departments, employees, suppliers, and customers. The executive in charge does not have to understand the technical details involved in securing information; he or she has to understand the wider company perspective and have the clout to get buy-in from multiple departments and personnel. Once this executive is involved, managers from operations, IT, finance, and risk management (in larger organizations) can work together to develop an IT security program.

"A critical piece is to get buy-in throughout the organization, so managers from each discipline should be involved," says Schmittling. "If things are driven from the IT side, sometimes there is a lot of resistance. But if you take the approach with [owners or CFOs] and their business unit managers, they can help drive home that message and enforce these types of policies."

Once your team is in place, the next crucial step is determining what information you need to protect and where that information is stored. You should ask yourself three key questions:

- What are we trying to protect?
- Where does the information reside?
- How do we build security around it?

For example, if you have an online store where people can purchase your products with credit cards, then cardholder data is your prime concern. First determine where that data is stored—most likely somewhere on your internal computer network where only certain employees have access to it. Your goal is to keep hackers from getting to the data, so the next step is to surround the information with layers of security: A password system shared by only key employees who need access to the information, computer virus protection, a firewall (a technological barrier designed to prevent unauthorized or unwanted communication between computer networks), a secure web server (one that supports one of the major Internet security protocols, which encrypt and decrypt messages to protect them against third-party tampering), and so on. Your IT staff can implement these technologies, often working in conjunction with a qualified software supplier or IT consulting group. Some criteria you should consider when hiring an outside firm include their experience in the field, professional certifications, and recommendations from past clients. (There are many professional certifications and designations for IT professionals.)

But it's not enough simply to take these steps. Schmittling emphasizes the importance of documenting what you have done and the reasons behind it in a formal IT security policy that spells out how your organization addresses the issue. The policy explains the specific data you aim to protect, how you will protect it, and the steps you will take to handle a security breach should it occur. What's more, all of your employees should understand the policy because, at the end of the day, IT security potentially affects everyone in your organization. For example, if cardholder data is stolen, your finance department will have to deal with the aftermath of erroneous charges and other accounting-related issues, sales and customer service reps will be on the front lines dealing with angry customers, IT will be in the trenches fixing the problem, top managers will be responsible for overseeing the resolution to the problem and communicating a message to customers, and so on. In a nutshell, if your organization is breached, it's going to be an enterprise issue, not an issue confined to one department.

A note on cardholder data: Whenever possible, do not store this information on your company network. Protecting this data is crucial, as evidenced by the industry security standard known as PCI-DSS (Payment Card Industry Data Security Standard). This set of standards aims to help organizations that process credit card payments prevent fraud through increased controls around cardholder data and its exposure to compromise. PCI-DSS addresses security surrounding companies' management, policies, procedures, network architecture, software design, and other measures created to protect customer account data. The standards were developed by the PCI Security Standards Council, which is made up of American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.

PCI-DSS has been in place for about five years, and it applies to all organizations that hold, process, or exchange cardholder information from any of those card brands. A related standard is PA-DSS (Payment Application Data Security Standard), which governs software companies that develop payment applications. All software companies that develop or provide payment application software must adhere to PA-DSS. If you process customer payments with credit cards, you must be familiar with both of these standards.

The PCI-DSS standard includes 12 requirements in six categories. They are as follows, taken directly from the PCI Security Standard Council's website (www.pcisecuritystandards.org):

### Build and Maintain a Secure Network

*Requirement 1:* Install and maintain a firewall configuration to protect cardholder data.

*Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters.

### Protect Cardholder Data

*Requirement 3:* Protect stored cardholder data.

*Requirement 4:* Encrypt transmission of cardholder data across open, public networks.

### Maintain a Vulnerability Management Program

*Requirement 5:* Use and regularly update antivirus software.

*Requirement 6:* Develop and maintain secure systems and applications.

### Implement Strong Access Control Measures

*Requirement 7:* Restrict access to cardholder data by business need-to-know.

*Requirement 8:* Assign a unique ID to each person with computer access.

*Requirement 9:* Restrict physical access to cardholder data.

### Regularly Monitor and Test Networks

*Requirement 10:* Track and monitor all access to network resources and cardholder data.

*Requirement 11:* Regularly test security systems and processes.

### Maintain an Information Security Policy

*Requirement 12:* Maintain a policy that addresses information security.

Using PA-DSS-compliant software can help ensure that your organization complies with the PCI-DSS standard. Working in conjunction with your software vendor or IT consultant, your IT department can ensure that you are meeting all of these requirements.

Interestingly, these payment application security standards mirror the general IT security protocols Schmittling recommends; this underscores the importance of taking a top-down, proactive approach to security across the board. And it brings up one last key point: The importance of testing your systems regularly for vulnerabilities that may expose your information to compromise. This is especially important on the Internet-facing side of your organization.

"New holes and vulnerabilities open up constantly," Schmittling explains. "By leaving those holes out there for a period of time, hackers and other people trying to do some sort of harm are going to dive into the easiest holes."

## THE IMPORTANCE OF TESTING

Schmittling says both internally developed and third-party application software should be tested regularly to find security flaws.

"Testing should be performed to assess vulnerabilities in the areas of input validation, user interfaces, information disclosure, session management, password parameters, application-based firewalls, et cetera, just to name a few," he says. "The development process for coding and implementing web applications should also be reviewed to determine that security is included at certain checkpoints. For third-party application software, organizations should verify that vendors have conducted detailed security testing of their products. For in-house developed applications, organizations must conduct such testing themselves, or engage an outside firm to conduct such testing."

Schmittling likens the testing process to a financial audit: Just as an organization independently verifies its financial statements every year, so should it seek verification of its data security programs.

"Testing security in an organization is really no different," he says. "On a quarterly or annual basis, [you] should look to an external provider that specializes in this to do a review or audit of your system configuration."

More and more of these companies spring up every day. Often, they are small "boutique" firms that specialize in security, but your software or hardware vendor may also offer such a service. In either case, Schmittling recommends going through a vendor selection process to make sure you are getting the right company to address your needs. As noted earlier, you are looking for a company or individual with experience in the field, relevant industry certifications, and recommendations from past clients.

## HOW TO HANDLE A SECURITY BREACH

When it comes to protecting your organization's data, everything boils down to the specific information you are trying to protect and where it resides. Once you understand that at a detailed level, Schmittling explains, you can architect what your layered approach to security should look like and how you should continually monitor it.

But despite your best efforts, there is always the possibility of a security breach—similar to what we saw in the DLP example earlier. With some skill and determination, a good hacker or untrustworthy insider may gain access to your information. As a result, you need to know how to handle a security breach—and you need to make that process part of your IT security policy.

"You need to have an incident procedure in place," advises Schmittling. "In most situations, organizations have not done that, and they end up scrambling to get people involved and [rectify the situation]."

If your organization is breached, Schmittling recommends the following "triage" steps:

1. Hire a computer forensic specialist to determine whether or not a breach actually occurred.
2. If a breach has occurred, your IT personnel should begin "locking down" parts of your system. Depending on the type of breach, this could mean taking your website offline for a short time while data tables area cleaned of any customer data (as we saw in the DLP example).
3. If cardholder data was stolen, get your bank involved to determine the steps you need to take to protect that information and guard against any fraudulent charges.
4. No matter what kind of data has been stolen, contact your attorney to find out what legal requirements you must meet and develop a plan to address them.
5. Contact those people affected by the breach—customers, employees, suppliers—to let them know that the breach occurred and that you are working to resolve the issue.

Schmittling emphasizes the importance of getting your attorney involved in the process because the laws surrounding cyber security vary from state to state and are evolving. Disclosure laws in most states require organizations to notify affected parties about an IT security breach within certain timeframes, for example. Some states also require organizations to provide credit monitoring services to those affected by the breach. There are also issues surrounding human resources data, especially employee health-related information. The Health Insurance Privacy and Portability Act of 1996 (HIPAA), for instance, requires that (among other things) employee health information be kept confidential. You could be held liable if such information is stolen or otherwise compromised as a result of a security breach at your organization. This opens your organization to fines, potential lawsuits, and other headaches you and your human resources department could do without—not to mention the damage to your employees.

Thus the importance of a well-thought-out, well communicated incident procedure. Knowing ahead of time how you will handle a security breach can keep you from scrambling to figure things out when the time comes. This makes a real difference in how those employees, customers, and suppliers affected by the breach will react to the situation. Knowing that your organization has everything under control and is taking the proper steps to protect their privacy will go a long way.

Think of it this way: Would your employees, customers, or vendors feel comfortable working with you if you were breached?

“If you can understand the size and scope of the problem, you can better monitor it,” adds Schmittling. “So these [triage] steps need to be in place. And that takes us back to where we started—if you’ve gone through a risk assessment or similar process, this [requirement] would have been identified up front.”

## THE COST OF A CYBER BREACH

We have already identified some of the most important losses you will suffer if your data is stolen and you have done little or nothing to protect it: First and foremost is the loss of your reputation and an erosion of trust among your employees and business partners. The cost of these losses is incalculable. But there are other costs, as well: Fees for hiring forensic specialists, attorneys’ fees, and data breach notification fees, to name a few. And if your customer data is stolen, it will cost you roughly $204 per compromised record, Schmittling says. A “record” is a single credit card number and customer name. To put this in perspective, Schmittling says cyber security liability for a small restaurant (one that does about $500,000 in business per year) is around $100,000. Of course, you must add to all of this any fines associated with a PCI-DSS or HIPAA breach. The credit card companies and others can impose fines for such violations, depending on your level of negligence.

Needless to say, it is worthwhile to take the steps outlined in this paper to avoid such consequences. But, admittedly, taking precautionary steps will cost you time and money as well. Experts like Schmittling say the cost pales in comparison to the cost of a security breach, however. The best place to start is with a risk assessment, and depending on the size of your organization, that will cost anywhere from $5,000 to $20,000.

“The larger and more complex the organization, the higher the cost,” says Schmittling. “Most organizations don’t want to pay for something like this, but when you consider the protection, it’s a small drop in the bucket compared to what you would have to pay [if your data is stolen].

“These things can be done pretty inexpensively, as long as you get the right provider in there who is going to add value.”

A risk assessment should include testing and evaluation of all your systems as well as a thorough look at your internal processes and procedures—specifically, what kind of access your people have to privileged information and whether or not they really need it to do their jobs. The assessment should also include recommendations for changing, updating, or enhancing your security measures. From there, the cost to implement security solutions—which can include computer hardware as well as various software programs (such as antivirus and secure credit card payment systems, to name just two)—will vary according to the solution and the size of your organization. It's a long list, to be sure, and Schmittling points to the human part of the equation as the most vulnerable point—one that organizations often don't consider when evaluating their IT security.

"It's kind of funny, over the last few years, the thing everyone wants is a penetration study, where they hire someone to hack into their network," he says. "But the weakest link is always the human element. It's less of an issue in smaller organizations, but it's where you get down to who has access to certain information and making sure that information is locked down only to the people who need it."

Another important note: Securing your valuable information is important in and of itself, but you can also use it to your advantage. For instance, when you become PCI compliant (meaning that you meet all the requirements of the PCI-DSS standard and have been found to be in compliance by an independent reviewer) you should market this advantage to your customers—to give them peace of mind that they are doing business with an organization that values their information and is taking measures to keep it safe.

"Also, there are organizations that do things above and beyond what they have to do because they want to provide that extra degree of insurance—and they communicate that to customers because that's what they see as adding value for their customer base," Schmittling adds.

## CONCLUSION

Securing valuable information has never been more important than it is today. Threats lurk around every corner, both inside and outside your organization walls. And in this Internet age, where online purchasing is prevalent, those threats multiply regularly. But you can take steps to keep your valuable data as safe and secure as possible—and to prepare yourself to handle a security breach should one, unfortunately, befall your organization.

As we have established, the first step is to actually take a step back and examine your organization from an IT security perspective. With the help of IT professionals, evaluate your systems, perform a risk assessment, implement a layered approach to security, create an incident procedure, and perhaps most importantly, wrap all of these into an IT security policy that governs your thoughts and actions about protecting employee, customer, supplier, and other key data. Such a proactive approach will go a long way toward not only protecting your valuable information, but also putting your employees and trading partners at ease when it comes to cyber security.

Some key points to remember (in no certain order) are:

- Have an annual security risk assessment performed to identify business, technology, and operational risks that affect your organization
- Review the development and implementation process for your key websites or systems, especially for those housing private information (credit card numbers and the like)
- Regularly scan your website for vulnerabilities and take corrective action immediately
- Have a network and website penetration test performed annually
- Become compliant with security regulations that affect your business, such as PCI and HIPAA
- And always take a proactive approach to security

BROWN SMITH WALLACE
CONSULTING
GROUP

## ABOUT THE EXPERT

Ron Schmittling, CPA/CITP, QSA, CISA, CIA, is the leader for Brown Smith Wallace's Security & Privacy practice. Ron's 18+ years of experience include more than five years in senior-level technical leadership roles at a major financial services firm, as well as positions in information security and technology consulting for several international organizations. Ron is a thought leader, frequent speaker, and author on topics in the information security and PCI compliance arena. Ron is a member of the American Institute of Certified Public Accountants (AICPA), the Illinois CPA Society (ICPAS), the Missouri Society of CPAs (MSCPA), ISACA, Institute of Internal Auditors (IIA), Infragard, International High Technology Crime Investigation Association (HTCIA), Information Systems Security Association (ISSA), and the Institute of Computer Forensic Professionals (ICFP).

## ABOUT THE AUTHOR

Victoria Fraza Kickham is a freelance journalist who covers the distribution industry. She has 17 years' experience in journalism, serving as a general assignment reporter for several Boston-area newspapers before joining Industrial Distribution magazine, where she held a variety of roles and served as managing editor for 10 years.

Victoria holds a bachelor's degree in English from the University of New Hampshire and a master's degree in English from Northeastern University.

## ABOUT BROWN SMITH WALLACE CONSULTING

The Brown Smith Wallace Consulting Group has been serving the distribution community for more than 20 years through the publication of various Software Guides, an online evaluation center and resource center at www.software4distributors.com and assisting companies who need help selecting the best software packages for their business and maximizing the benefits from their investment.

**BSW Consulting**
10151 Corporate Square Drive
Suite 100
St. Louis, MO 63132

314-983-1200
www.bswllc.com
www.software4distributor.com