White Paper: **Managed Security**

Managed Security for a Not-So-Secure World

CIOs need a strategy for a secure enterprise in today's insecure world.

Qwest BUSINESS

NETWORKWORLD® Custom Solutions Group

It turns out that the infamous TJX Companies breach in January 2007 was only the tip of the iceberg: there has been an explosion of data security incidents in the past few years. In 2008, the Identity Theft Resource Center (ITRC) reported 656 breaches, a 47 percent increase over 2007. And there have been 213 data breaches in the first five months of this year alone.

This risky data environment is colliding with an IT landscape of shrinking resources. An April 2009 Lieberman Software survey of IT professionals discovered that 60 percent of respondents work at organizations that have cut their IT budgets, and 40 percent of organizations have reduced their IT teams. Such cuts leave fewer resources available to handle the ongoing need for compliance with a bevy of regulations—from the Sarbanes-Oxley Act (SOX) to the Health Insurance Portability and Accountability Act (HIPAA) to the Payment Card

Industry Data Security Standard (PCI DSS)—to whatever new transparency requirements will arise from the banking crisis.

But business must go on. CIOs must manage security risks while addressing business needs and focusing on revenue-generating activities. This paper offers a strategy for providing data security and protection that addresses the rising data threat landscape, the need for compliance, and today's lean IT staffs.

For more information about Qwest's managed security services, visit us at **www.qwest.com/business**

Good Enough Isn't Always Enough

Unlike conventional projects with a beginning, middle and an end, IT security is never finished. The security program implemented yesterday may not be adequate tomorrow because new threats arise every day.

Opportunistic predators, for example, exist both inside and outside the organization. Organized crime is a major concern from a financial perspective because their motivation is typically financial gain, which causes them to continually seek out potential network infrastructure vulnerabilities, and create new viruses and worms. This has significantly raised the quality of threats that companies must defend themselves against.

Though most IT managers are vigilant and diligent in using the tools they have to protect corporate data, there are often blind spots that these predators will find and exploit. Ensuring corporate data is safe takes considerable proactive, continual monitoring—or outside help.

"Keeping up with the high traffic in vulnerability disclosures is a perennial challenge and an important part of our program since we focus on proactively identifying and remediating risks," says Michael Glenn, director of information security and chief information security official (CISO) at Qwest Communications International Inc., a managed security provider. "We have to balance our resources between our proactive, innovative programs and our reactive obligations, including a growing list of compliance auditing, certification and reporting activities."

Those compliance issues can be burdensome. Mandated compliance with a wide and growing variety of state, federal and industry regulations places an increasing strain on IT staff.

Being Compliant

Some of these regulations, or parts of them, promote data protection within particular industries. For example, the Gramm-Leach-Bliley Act (GLBA) has privacy stipulations to protect information in the financial services industry, including companies providing financial products and services to consumers. For example, the GLBA's Financial Privacy Rule requires financial institutions to give their customers privacy notices that explain the institution's information collection and sharing practices. In addition, customers have the right to limit the sharing of their information.

Failure to comply with these regulations can lead to stiff penalties—HIPAA fines, for example, can be as high as $50,000 *per violation.* And the American Recovery and Reinvestment Act of 2009 will further tighten HIPAA's privacy and security rules for data breach notification, enforcement, audit trails and encryption. Then there's the PCI DSS, which governs payment card transactions. Here again, noncompliance can be expensive: for example, Visa could fine transaction processors between $5,000 and $25,000 a month if the merchants or retailers they represent are not PCI compliant.

What's troublesome is that companies often think they're in compliance but end up finding out the hard way that they're not. Take the examples of RBS WorldPay and Heartland Payment Systems, which process credit card payments. Before the end of 2008, they were believed to be PCI compliant. However, hackers tapped into their data, including cardholders' private information. The point is that just checking a checkbox for compliance may not protect your organization's data; you must have solid security practices in place to first protect data, and then meet compliance obligations.

WP090991 8/09

There are intangible costs as well. A breach in security of this magnitude causes a lack of confidence among current and prospective customers. CIOs and IT managers recognize this threat. In a recent survey conducted by IDG Research Services on behalf of Fiberlink Communications, 81 percent of respondents said that damage to their company's reputation from a data breach was their greatest concern, followed by legal consequences and costs (79 percent) and loss of critical data (74 percent).

Things like proactive network monitoring, testing and tracking, complex firewall configuration, a comprehensive vulnerability management program, centralized logging and auditing, an access control program, and sound, comprehensive security policies are necessary for a good security program and to meet compliance obligations. Considerable staff and resources are also required.

So, how does the CIO face these challenges?

Benefits of an Outsourcing Partner

- ☑ **STAFF:** Professionally trained talent to manage and implement security programs and plans
- ☑ **SOLUTIONS:** Carefully researched and selected security technologies
- ☑ **COST:** Lower total cost of ownership for labor and technology through scaling, configuration, maintenance of technology solutions, training personnel, and researching processes and products
- ☑ **KNOWLEDGE:** Experience and knowledge base to discover vulnerabilities, face new security threats and solve complex security problems

Outsourcing Managed Security

Given the security risk climate and the reduction in IT staffs, working with an IT and security service provider is more practical. With the appropriate foundation of outsourced services, security becomes manageable and reliable.

Of course, cost is a consideration. You should conduct a thorough analysis of the time and expenses involved in using internal resources and then weigh it against an outsourcing provider's cost model. For example, the cost of managing and configuring technology is a key component of the total cost of a security program. And you have to consider whether your in-house expertise is up to the task.

"Inevitably, difficult economic times can cause otherwise good people to make poor decisions," says Glenn. "I expect to see a continued need for vigilance against malicious software and attacks like spear phishing that are rooted in fraud, along with the ever-present insider threat. In a downturned economy, you do not want to be significantly cutting your information security program."

To stay abreast of vulnerabilities and threats, IT personnel must continually expand their knowledge and expertise, which can be challenging if budgets do not allow for a fully dedicated security staff or ongoing training. In addition, expert security professionals, especially those with credentials from professional associations, are in high demand, so retaining them can be difficult.

On the flipside, a well-recognized, comprehensive security service provider has already gone through the rigors of recruiting and training quality security personnel. In addition, these teams have been exposed to a variety of enterprise security challenges from a diverse clientele. Tapping into this expertise offers not only a skilled security strategy, but also a fresh look at how to address risks.

Another consideration is that IT and business processes are often in flux, due to changing market conditions and business demands. Managing them requires both time and broad experience; organizations with tight IT budgets can suffer process management constraints. An outsourcing partner can add value by bringing a wide range of expertise and the ability to look at the entire scope of a company's processes to identify potential obstacles or problem areas.

Employing the best people and processes are only parts of the equation. You also need the right tech-

WP090991 8/09

nology. Because new security tools and solutions are introduced every day, evaluating, purchasing and maintaining them requires time and an understanding of how they will best fit the organization. A feasible alternative is to lean on a managed security provider that has experience with a wide variety of solutions, and that can provide a thorough analysis of which tools are most appropriate.

Conclusion

In the IT landscape, vulnerabilities and threats arise constantly while new and shifting compliance regulations place increased pressure on data protection. And CIOs must face these issues with reduced staff and contracted budgets.

A solid relationship with a managed service provider can be of great help, freeing CIOs to focus on core business operations, build better relationships with stakeholders and ultimately achieve short and long-term business goals. Using managed services to address security risks is a best practice to reduce costs, ensure compliance and allow IT staff to focus on critical business operations.

Glenn offers this closing advice: "Spend just as much, and preferably more of your energy on building relationships with key stakeholders across your enterprise than you spend learning the bits and bytes of the latest technical toy. If you have the right relationships with your business, you can always find a means to accomplish your objectives by making your business successful through good security practices and risk management. Learning those technical means together gives you more credibility."

Take an honest look at your internal capabilities, and compare them to what a managed security services provider can offer, including economies of scale. It's likely that a security strategy that includes outsourcing in its mix will be a cost-effective, practical and winning solution.

Failing to Comply

Data breaches have resulted in disciplinary actions and fines by the Federal Trade Commission (FTC) in numerous cases. Here are a few examples:

- ☑ The FTC disciplined a Texas-based mortgage company after it failed to provide reasonable security to protect sensitive customer data. Third-party home sellers were able to access private data without security measures in place. A hacker compromised the data by breaking into a home seller's computer, obtaining the lender's credentials and using them to access hundreds of consumer reports. Because this mortgage company had inadequate data protection, they were liable for the security breach.
- ☑ When hackers stole the personal data of some 46 million customers of retail conglomerate TJX Companies, the FTC attributed the breach to a failure by TJX to use reasonable and appropriate security measures on its networks. As a result, a third party must audit the company every other year for 20 years and TJX must show improvement in its network security, service provider selection and how it handles consumer information. The retailer also negotiated a settlement reported at more than $40 million with Visa International.
- ☑ After it was discovered that hackers had accessed the sensitive information of hundreds of consumers, an online seller of computer supplies was admonished by the FTC. The company failed to provide reasonable security to protect sensitive customer data such as personal information and credit card numbers. The vendor suffered bad publicity and diminished overall customer confidence.

SOURCE: www.ftc.gov

WP090991 8/09