SUNGARD

FIVE BLIND SPOTS

Executive Brief Series

Avoiding Common Exposures in Your Information Security Program

OVERVIEW

Information security is a critical concern for all technology-dependent enterprises. Nevertheless, many organizations are still struggling to successfully implement and maintain an effective program. Even those firms that believe they have a firm handle on security often overlook critical weaknesses and vulnerabilities. In fact, the SunGard Availability Services team of information security consultants has found that organizations' self-assessments are off by as much as 30 to 50 percent when compared to a comprehensive, third-party evaluation.

At SunGard, we recommend and use a comprehensive, standards-based approach. Known as the SunGard Information Security Performance Model, our approach incorporates:

- Policy, Procedures and Regulatory Compliance
- Access Control and Organizational Skills
- Exposure Analysis and Reporting Metrics
- Architecture and Project Management
- Awareness, Education and Training

These five areas are absolutely critical to any organization's information security. And yet, almost every firm has weaknesses in one or more of those categories. SunGard's consultants encounter those weaknesses every day—as they work alongside clients to improve their information security programs. In this executive brief, we summarize the five "blind spots" that could prove costly for your organization. More important, we provide suggestions for addressing these vulnerabilities.

BLIND SPOT #1: LACK OF POLICIES

Policy, Procedures and Regulatory Compliance

The most common blind spot is lack of a security framework—and the most common cause is the way security is organized within an enterprise. If security is treated only as an information technology function, we typically find a heavy focus on tools. While tools are important, they are not a replacement for a pragmatic, policy-based approach.

At SunGard, we recommend that enterprises build a solid security framework comprised of clear policies that are applied throughout the organization. To that end, they should be approved by executive management and communicated throughout the ranks.

Without that kind of standardization, organizations are likely to use ad hoc business and technology practices. For instance, virtually all IT operations employees have their own preferred methods for maintaining individual servers. To optimize security, there should be a single set of standard policies and practices—and everyone should adhere to them. After all, consistency is one of the most important requirements for security. And, one of the best ways to improve consistency is through a policy-based framework.

To eliminate this blind spot, take a hard look at the way you've structured your organization's security function. Remember, security is a strategic requirement and a strategic function that involves more than just IT. For maximum effectiveness, your security function should be managed centrally by an executive—ideally the chief security officer (CSO) or chief information officer (CIO).

BLIND SPOT #2: PASSWORD MISMANAGEMENT

Access Control and Organizational Skills

American humorist Josh Billing has said, "It is the little bits of things that fret and worry us. We can dodge an elephant, but we can't a fly." When it comes to access control and organizational skills, passwords are the troublesome "fly." SunGard's consultants have identified three key issues around password management:

- Generic and default passwords. There's no excuse for not changing the default passwords from hardware and software manufacturers. After all, maintaining the default creates an easy point of entry for hackers—especially since these industry-standard defaults often safeguard critical system access.
- End-user passwords. End users that rely on obvious passwords create a major vulnerability for your organization. It's critical that you educate users about the importance of selecting unique passwords—and changing them regularly.
- Employee status changes. When employees move among departments, you need to ensure that their access levels change accordingly. Make certain that employees can log in to only those systems relevant to their current position. This is especially important for contract and temporary employees. When their positions change or are terminated, be sure to close off all system access, as well.

To eliminate this blind spot, use strong, two-factor authentication incorporating passwords plus smart cards, biometrics or other forms of authentication. Apply that two-factor authentication consistently throughout your enterprise—from system accounts to individual end-user accounts, including those belonging to temporary employees.

BLIND SPOT #3: EXECUTIVE-LEVEL REPORTING

Exposure Analysis and Reporting Metrics

To be sure, IT-oriented reports are important; you need detailed log reviews to monitor and analyze attempted intrusions. But those kind of "nitty gritty" reports are not meaningful to CFOs, CEOs or board members. Consequently, those reports probably won't help advance the business case to increase security resources, whether human or budgetary.

To communicate effectively—and achieve your desired results—you need to create and maintain executive-level reports. Of course, your CIO will likely still want in-depth technical reports. But, distill that technical data into business information for other C-suite executives on a monthly or quarterly basis and for your Board of Directors on an annual basis. Those audiences don't need to know the particulars of any log review; they want assurance that your security program is protecting the enterprise and addressing compliance with applicable regulations.

To eliminate this blind spot, consider implementing an executive dashboard system. That way, you can deliver the level of detail most appropriate for the audience. If a project of that scope isn't feasible, consider enlisting the help of a third party, such as SunGard. Our team of consultants can provide an objective review of your current approach and then help you establish a workable standard report that meets a wide range of needs.

BLIND SPOT #4: CHANGE MANAGEMENT PROCESSES

Architecture and Project Management

Security programs—and the supporting policies—are living "creatures." They must evolve and adapt to continuous change within any enterprise. But what we sometimes encounter are sound policies that have not been appropriately applied as new business and/or technology changes emerge.

Your security function should be informed and involved any time business processes and/or IT systems are being introduced or modified. Whether it's a new human resources application, an accounting system or a marketing database, data is being used, stored and transmitted. And that means your information security folks should evaluate your needs to safeguard your data.

That's especially true if a third-party partner or vendor is involved. Indeed, if your organization is like most, you're becoming increasingly strict when evaluating and selecting your vendors. The Gramm-Leach-Bliley Act is just one example of a regulation that holds organizations accountable for the security and continuity practices of their business partners. You simply must ensure that business processes and supporting technologies—both within your walls and throughout your value chain—are secure.

To eliminate this blind spot, implement a formal policy requiring that your information security function be included in all organizational changes. What we often find is that functional departments make decisions without consulting IT. And, even when IT is involved, they sometimes execute the wishes of the human resources, accounting, marketing or other departments—without considering impact to security. Only with your information security team's input can you proactively and properly address security risks.

BLIND SPOT #5: SOCIAL ENGINEERING

Awareness, Education and Training

Even a world-class security program—complete with optimal policies, procedures and tools—is virtually worthless if employees are not aware and informed. Despite that, SunGard consistently finds that the Awareness, Education and Training component of the Information Security Performance Model is the most neglected.

Our information security consultants continually see examples where sound practices are being adopted and implemented—but not communicated. To truly safeguard your enterprise, everyone—including your front-desk receptionist, IT and other support personnel, as well as customer-facing employees—must be up-to-speed on some key security concepts and precautions.

When they aren't, it creates a huge vulnerability in the area of social engineering. Quite simply, it's human nature to want to help other people. However, when it comes to your company's information security, the actions of well-meaning employees can lead to major problems. Just one example: a hacker could call an employee at his or her desk, pose as a member of your organization's help desk, and request that your employee provide a critical password. To be "nice," the employee may willingly reveal that sensitive information.

To eliminate this blind spot, conduct ongoing employee training. Make sure everyone—including all new hires—understands that security threats don't always take the form of a nameless, faceless hacker. Breaches can also occur through seemingly harmless human interactions on the phone, via e-mail and even in person. Without the right level of awareness, it's virtually impossible to stop those types of attacks.

CONCLUSION

We can't emphasize enough: information security isn't just about IT. To be effective, you need more than firewalls, anti-virus software and other technical tools. You need more than log reports that detail attempted intrusions and other suspicious activity. And you need more than well-trained IT employees. While all of those components are important, they are only pieces of a much larger whole.

Take a step back and assess your current approach to information security. What are your capabilities in each of the five areas of our Information Security Performance Model? Is your approach truly comprehensive? And, more to the point, where does your organization stand with the common blind spots we've discussed—policies, passwords, reporting, change management and social engineering?

To eliminate these blind spots, your organization must adopt, execute and continuously maintain a comprehensive approach to information security. You can go it alone—or with assistance from an expert third party, such as SunGard. Either way, this type of approach is the only way to truly protect your organization.

SUNGARD SERVICES

SunGard Availability Services is dedicated to helping organizations measure, implement, manage and maintain information security and protection programs. Through our Information Security practice, we deliver a complete array of physical and IT security evaluation and planning services ranging from enterprise threat and vulnerability assessments to comprehensive security program development all based on the ISO 17799 Code of Practice for Information Security Management.

We built our security philosophy upon fundamental information security management goals. The goals, as outlined in our Information Security Performance Model, are:

- Policy, Procedures and Regulatory Compliance
- Access Control and Organizational Skills
- Exposure Analysis and Reporting Metrics
- Architecture and Project Management
- Awareness, Education and Training

Our specific security solutions span the service areas and reflect our proven, comprehensive expertise in addressing organizational confidentiality, integrity, and availability (CIA) concerns. Delivered using SunGard's Enterprise Availability Methodology, practice solutions include:

- Enterprise Risk Assessments
- Technical Security Assessments
- Regulatory Compliance and Business Associate Reviews
- Managed Security Services

SunGard Availability Services | 680 East Swedesford Road | Wayne, PA 19087 | 800-468-7483 | www.sungardas.com

www.sungardas.com

SunGard Availability Services
680 East Swedesford Road
Wayne, PA 19087
Tel: 800-468-7483