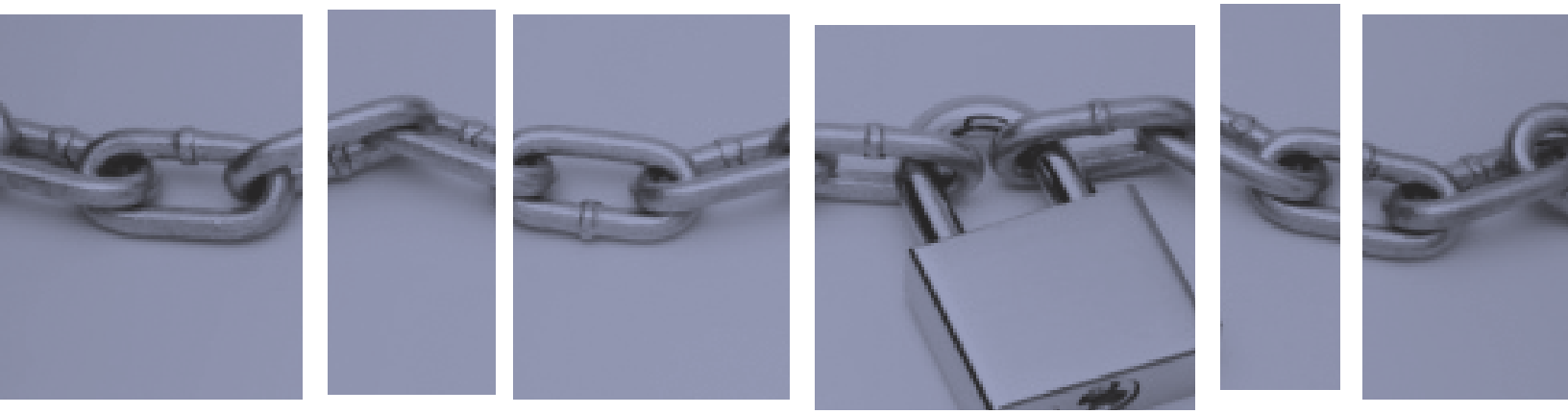
CMP
United Business Media

A CMP **WHITE PAPER**



Sound Security

Four Elements of a Successful Strategy

Brought to you by

IBM®

Sound Security:

Four Elements of a Successful Strategy

Executive Summary

Planning and executing an effective enterprise information security strategy can be a time-consuming, often-frustrating task. No single security solution exists that can address all corporate requirements, although any number of vendors are ready and willing to sell point products they promise will fill in some piece of the puzzle. But too often, just when one security solution is successfully deployed, another gap surfaces somewhere else in the infrastructure that needs to be addressed. Over time, a company is likely to wind up with a series of security tools that don't communicate to form a coordinated defense. The result is a hodgepodge of mostly disconnected products that make holistic security management difficult, if not impossible.

A confluence of factors is making the need for comprehensive information security more urgent by the day. Beyond the fact that so much precious corporate information is now online, businesses are also facing increased regulatory pressure to protect this data. Public companies must comply with strict controls mandated by the Sarbanes-Oxley Act, while any health-care concerns have to meet privacy requirements defined in the Health Insurance Portability and Accountability Act (HIPAA). Companies that process credit cards have to deal with Payment Card Industry (PCI) compliance standards to protect cardholder data. And the majority of U.S. states also now have laws dictating that companies disclose any breach of private data, such as credit card account information and Social Security numbers.

Such breaches can indeed have a devastating effect. Researchers at the Ponemon Institute put the cost of each lost customer record at $182 for detection and remediation. Forrester Research finds companies spend between $90 and $305 per compromised record. And these figures do not include the damage to a company's reputation, which can be an even higher price to pay.

But beyond merely meeting regulatory requirements or dodging disaster by reducing risk, implementing proper security measures can bring about important, positive business benefits. Companies that prevent security incidents can achieve greater system availability by avoiding downtime related to viruses, denial-of-service attacks or the cleansing that must take place after an unauthorized intrusion. This results in increased employee productivity and ensures that corporate resources are available to customers, partners and others when they need them.

Having a proper security plan in place also means that a company can bring resources online more quickly because the organization has a process in place to consistently deploy IT equipment and software with security already enabled. This means that the business can respond more efficiently to new opportunities and changing business requirements, and thus be more competitive.

Of course, to achieve these benefits, businesses need more than just a series of tools or services to provide various safeguards; they need a solid strategy for protecting corporate assets

Contents

that includes well-designed processes. To really succeed on the security front, businesses need to develop and follow a plan that continually provides four essential security functions:

- Assessing the organization's current posture to find holes and identify risks
- Defending against myriad threats, including viruses, Trojans, spyware and other forms of malware
- Securing access only to authorized resources for authorized users
- Monitoring continuously for attacks and issues of noncompliance with corporate security policies and external regulations

Each of these functions requires different tools to get the job done. While many vendors can offer some pieces of the puzzle, few can provide a comprehensive solution. IBM is able to address each of these functional areas through its extensive suite of hardware, software and services. As a result, IBM can provide enterprise customers with end-to-end security through an integrated package of tools and services. Not only does this give the business protection from internal and external threats, but this kind of solid security solution helps organizations establish a complete and accurate picture of the company's security posture at all times.

Indeed, each of the four security fundamentals outlined above not only addresses a security requirement, but carries tangible business benefits as well.

BEGIN AT THE BEGINNING

A thorough approach to enterprise security starts with a security assessment, which gives an organization the information it needs to uncover the gaps between current and desired security levels. The assessment begins with the creation of a security benchmark that catalogs all IT assets and their security posture, including software-revision level and whether each has the latest updates installed. To establish such a benchmark, a company needs to take inventory to find out exactly what equipment and software is running in the enterprise. Organizations can either opt to perform this work on their own, with the aid of specific tools, or turn to a third party to inventory their environment.

In general, the idea is to find security vulnerabilities or weaknesses in three areas:

- Data confidentiality: Blocking unauthorized access to data
- Data integrity: Ensuring that the organization can obstruct unauthorized attempts to alter data
- Data availability: Guaranteeing that data is available to authorized users who need it, when they need it

Once the organization identifies potential vulnerabilities, the next step is to conduct a risk assessment. Essentially, this involves prioritizing security risks to determine which ones represent the greatest threat to the organization's most valuable resources and services. Conducting this type of assessment typically requires input from the entire organization. This ranges from getting feedback from executive stakeholders to lower-level personnel who actually create and use data in their day-to-day jobs. The goal of a risk assessment is to gain a real-world understanding of how valuable each type of data is to the organization as a whole. Put another way: What data would cause the most damage if it were lost, corrupted or stolen? Also, compliance requirements will likely play a role in determining which vulnerabilities need to be addressed and in which order.

The assessment process is not a one-time exercise. With each change to the IT environment, a company's security posture may likewise change. As a result, businesses need to conduct periodic assessments to identify new vulnerabilities. Additionally, many organizations are required to perform assessments periodically to meet regulatory requirements. Thus, an organization needs to plan to create an assessment methodology that can be repeated time and again.

The business benefits associated with performing this type of security assessment start with acquiring better information that can help an organization manage its risks more effectively. When performed properly, a risk assessment brings structure to the question of which assets warrant the most protection from security threats. With this data in hand, the organization can be assured that it is spending its security dollars in the most cost-effective fashion by addressing the areas of greatest value first. Conversely, the risk assessment will highlight areas that don't require large security expenditures, thus saving the company from unnecessary expenses.

Equally important is the fact that by bringing vulnerabilities and risks into focus, the assessment can help ensure that organizations are proactive in addressing them. Rather than finding out about vulnerability only after suffering a costly breach of

customer data, a proper assessment can bring the vulnerability to the fore so an organization can address it before the worst happens.

THE BEST DEFENSE

With a clear notion of where an organization's vulnerabilities are, a company can set about defending itself against the threats that capitalize on these vulnerabilities. These threats are many, but generally speaking, an organization must provide for:

- **Network security: Protect against threats at the network perimeter from across the Internet**
- **End-point security: Safeguard servers and client machines from Internet and internal threats**
- **Mail security: Defend the messaging infrastructure**

Implementing these kinds of defenses requires a layered approach, one that recognizes no single security measure is 100 percent effective all of the time. The theory behind a layered approach is that if a threat succeeds in getting past one security measure, there is another line of defense to block an attack. So, for a threat to succeed in infiltrating the enterprise, it would have to thwart multiple defensive measures.

Providing perimeter security requires a mix of technologies to defend against such threats as viruses, worms, unauthorized intruders, spam and nefarious Web content. These technologies include intrusion prevention and detection systems, antivirus tools, firewalls, Web filters and antispam tools.

Even within these categories, multiple technologies may be required. In terms of antivirus, for example, organizations will need systems that rely both on signatures for known viruses and behavioral techniques to identify abnormal patterns that signify a virus. The latter defends against new viruses for which signatures have not yet been released, including "zero-day" viruses.

While perimeter safeguards protect network entry points, end-point security measures protect individual servers, and desktop and laptop machines. Also known as host protection, these systems protect individual systems against attacks that take advantage of vulnerabilities specific to those machines, such as flaws in the operating system or the Web browser.

For servers, host-based measures include the intrinsic integrity features of the platform itself, data encryption and vulnerability-based intrusion prevention systems (IPS), to protect against previously unknown forms of attacks. Web application protection helps prevent applications from performing unintended functions, while buffer-overflow prevention tools protect against exploits that enable hackers to take over a machine. Client machines will need many of the same defenses, including IPS, antivirus, antispyware, buffer-overflow protection and encryption.

Given how integral e-mail has become to most organizations, and the fact that many types of threats travel via e-mail, the messaging infrastructure warrants special protection. Specific defenses include spam analysis and control, content filtering, IPS, behavioral virus prevention and, perhaps, signature-based virus prevention.

With the mix of technologies involved, threat defense is an area where an integrated product set can be especially beneficial. Many organizations opt to have a third party assist in the selection and installation of security products. Some also turn to an outside expert to provide security defenses on an ongoing basis. This is an especially attractive option for organizations without significant security expertise in-house or for those that simply wish to have their IT staffs focused on other tasks more closely aligned to their core business goals.

The business benefits of proper, multilayered security defenses are undeniable, in that this protection allows an organization to keep ahead of threats, even the zero-day form that hits without warning. This in turn can translate to increased system availability and uptime for internal employees, external customers and business partners. Proper defenses reduce risk of costly incidents, such as from the loss of intellectual property. Similarly, good defenses can limit exposure to legal liabilities, including those related to breaches that result in the theft of customer data, as well as fines and other costs associated with regulatory noncompliance.

A DELICATE BALANCE

Secure access to information requires a delicate balance. On the one hand, corporate information does a business no good if those who need it cannot easily access and use it. On the other hand, the consequences of data falling into the wrong hands can be devastating.

Unauthorized access to information assets is a growing threat to organizations, and one that comes from both inside and outside corporate walls. With this in mind, businesses need a way to centrally manage user identities and authorizations while consistently enforcing access policies across the enterprise. The goal is to provide easy access to information for those who are authorized to see it, while preventing access from users without the right to use the data, including employees.

In organizations of almost any size, keeping track of what data each user is and is not authorized to use or see quickly becomes an unwieldy task. What is required is a centralized, policy-based access control system that allows an administrator to quickly provision access rights to a user based on that person's role in the organization. For example, all marketing department employees would be granted access to marketing-related sources, but not human resource systems. The system should also have an automated approval engine that can delegate approval authority to appropriate managers throughout the organization, making it possible for them to provide more granular access rights as necessary.

A good identity management system should offer reporting mechanisms that make it easy to see the life cycle of each user's identity, extending from the point in time it was first created; from when the user was given access to various resources; who authorized all account privileges; any account changes and so on. Other helpful functions include self-service mechanisms that let users change their own passwords as necessary, thus saving valuable help desk time. Single sign-on (SSO) capabilities can also help improve security, especially when used with strong authentication systems that require two forms of identification, such as a smart card or hardware token and a password. And federated identity services make it possible for an organization to extend its existing identity infrastructure to trusted business partners, customers and suppliers, or even to provide easy access to resources across the internal organization.

A centralized identity management system also makes it easier to consistently enforce corporate access policies. Such policies are defined centrally and include built-in audit controls, along with an automated approval process. This helps ensure that these access policies are consistently enforced across the organization.

Centralized identity management yields business benefits that start with the protection of information assets from unauthorized access, whether that attempt comes from outside intruders or corporate insiders. Automated provisioning saves time and money, while improving security by ensuring that access privileges change along with a user's role. This is most notable when a user leaves the organization, in which case all access rights can be easily revoked with one simple change.

Features such as self-help and SSO also carry monetary benefits. These tools can help reduce IT costs and improve user productivity by minimizing the downtime that employees would experience while waiting for password resets and by saving valuable time users would spend logging into multiple applications each day.

The reporting functions that come along with a good identity management infrastructure also make it easy to provide accurate information for audits, an important consideration in the compliance arena. And the ability to offer federated identity management can greatly ease the process of granting access to data to trusted partners and customers, potentially resulting in new or improved business opportunities.

ON THE RIGHT TRACK

The final discipline required to properly secure an enterprise infrastructure is an effective monitoring and reporting capability, one that can help identify and correlate security events while enforcing policy across the organization.

This capability, often referred to as security information and event management (SIEM), identifies threats to the organization no matter where or when they occur. This means the system must be able to collect raw data from across the infrastructure, including gathering incident and other information from security tools as well as other components, storing data in a centralized database and then translating this data into meaningful information.

Ideally, a centralized monitoring tool will correlate alerts coming from the myriad of systems and devices on the network and then alert IT administrators to the threats that need to be acted on immediately. This centralized monitoring tool should also provide a consolidated view into the

security posture of the entire organization, saving IT administrators the trouble of having to track each tool individually. However, a good SIEM tool will also provide the capability to drill down and investigate any given alert.

By looking through log files, a centralized monitoring tool can also help identify user behavior that violates company security policy, in order to expedite corrective actions.

This type of centralized monitoring and reporting can bring important business benefits, such as automated threat response, which supplies immediate corrective action to block security breaches. Additionally, the ability to provide visibility into security operations across the enterprise saves an IT administrator valuable time, while helping the IT manager be more effective in keeping track of security across the business.

The auditing and reporting capabilities of a good centralized management tool can help businesses comply with established security best practices. This is an important consideration in proving to auditors that an organization is in compliance with regulations. The ability to translate log data into plain-English reports helps executives stay on top of their most pressing security concerns and prove to auditors that the company is in compliance with relevant rules and regulations. Such reports also help executives maintain the right balance between good security controls and effective business operation, ensuring that the business is well protected but not overburdened by security measures.

COVERING ALL THE BASES

With its mix of security hardware and software, professional services and managed services, IBM can address all the functional requirements required for end-to-end information security. No matter whether the organization has the in-house resources and expertise to operate its own security infrastructure or whether it is in the business's best interest to outsource some or all functions, IBM has a solution that can be tailored to a company's specific needs.

IBM has products and services that specifically address one of the four core security functions — assess, defend, access and monitor — as well as products and suites that address multiple functions. For example, IBM Tivoli Compliance Insight Manager and IBM Tivoli zSecure Suite both address functions that fall into the assess, access and monitor categories.

IBM Tivoli Compliance InSight Manager (TCIM) is an enterprisewide solution that provides for centralized event and alert management of information coming from numerous security devices and platforms, including the mainframe. The solution translates security log data into easily understood language. TCIM includes a compliance management component that provides regulation-specific compliance templates and targeted reports, as well as a dashboard geared specifically toward compliance activities related to SOX, HIPAA, the Gramm-Leach-Bliley Act and others. The system also screens data to ensure that systems and users, including trusted insiders, comply with corporate security policies.

The zSecure Suite consists of products intended to address security requirements for IBM eServer zSeries servers and products. Separate modular components include:

- **IBM Tivoli zSecure Audit**, an event and status-auditing solution for the mainframe. Tivoli zSecure Audit performs security analysis, event reporting and system-integrity analysis for mainframe sites that run z/OS and RACF or ACF2.
- **IBM Tivoli zSecure Alert** monitors the mainframe for intruders and configuration errors. It goes beyond the capabilities of conventional intrusion detection solutions to take on intrusion prevention as well. Tivoli zSecure Alert takes action to stop an attack, thereby addressing both the defend and monitoring functions.
- **IBM Tivoli zSecure Command Verifier** monitors for policy enforcement, helping facilitate mainframe compliance to policy and regulatory requirements by preventing erroneous commands. This helps organizations increase control over their environments while decreasing the potential for security risks and cleanup costs.

While the Tivoli Compliance Insight Manager and Tivoli zSecure suites address multiple security requirements, numerous other IBM offerings target specific functions.

Assess Solutions

IBM provides numerous services that address different aspects of the assess function, including:

- **IBM Vulnerability Management Service:** Combines a managed scanning service from IBM Global Services with expert workflow and case management to protect the network

infrastructure from intrusions that could potentially damage your business.

- **IBM Information Security Assessment:** This solution, in which IBM Internet Security Systems (ISS) security experts provide a thorough analysis of an organization's current security state, is based on the globally recognized ISO 17799 standard and industry best practices. The service is intended to uncover vulnerabilities and provide a specific, actionable plan to improve overall security posture based on business needs.
- **IBM Penetration Testing:** IBM Internet Security Solution Professional Security Services experts actively probe the network seeking security holes that a hacker could potentially exploit. Deliverables include a complete list of the problems discovered; steps detailing how the tester was able to exploit any discovered vulnerabilities, and a complete remediation guide to shore up weak defenses.
- **IBM X-Force® Threat Analysis Service (XFTAS):** This service combines high-quality, real-time threat information from the Internet Security Systems (ISS) international network of security operations centers with security intelligence from the ISS X-Force research and development team. The X-Force team acts as the foundation of the IBM ISS preemptive approach to security, and its research intelligence is built into every product and service IBM ISS offers. With this offering, XFTAS security experts develop comprehensive evaluations and recommendations suited to the business.
- **IBM Proventia® Network Enterprise Scanner:** This solution helps ensure the availability of revenue-producing services and protects corporate data by identifying where risks exist, prioritizing and assigning protection activities, and providing a complete analysis report on the results, along with remediation guidance.

Defend Options

IBM Internet Security Systems (ISS) offers preemptive protection that is tightly integrated with existing IT business processes to help fortify the entire infrastructure — from the gateway to the core, and out to the most remote endpoints. The foundation of this protection is the IBM Proventia® product family, which comprises the following technologies:

- Traditional antivirus and next-generation behavioral virus prevention system (VPS)
- Managed and monitored firewall services
- VPN
- Intrusion detection and prevention
- Antispam
- Content filtering

IBM server platforms provide secure hubs for enterprise data with technologies that provide data and application integrity, encryption solutions to protect sensitive data, and solutions to help protect access from the network. IBM offers a variety of forms of data encryption to help protect sensitive data as it crosses the Internet or while it resides in a file, database or tape cartridge.

- The industry's first drive-based tape encryption solution – the IBM System Storage™ TS1120 Tape Drive
- IBM Servers with options for encryption acceleration and tape encryption key management
- System z servers with CryptoExpress2 for tamper-resistant key processing
- IBM Encryption Facility for z/OS® servers for file encryption
- IBM Data Encryption for IMS™ and DB2® Databases
- IBM DB2 v9 encryption enhancements

Access Management Tools

For managing user identities and authorizations, in addition to the Consul zSecure suite of mainframe tools, IBM also provides numerous IBM Tivoli security solutions.

IBM Tivoli security management solutions help business quickly realize ROI by bringing users, systems and applications online fast, while effectively managing employees, access rights and privacy preferences throughout the identity life cycle. The Tivoli portfolio of security management solutions includes:

- **The Tivoli Identity Manager family:** These products provide a secure, automated and policy-based user management solution to effectively manage user identities throughout their life cycles across both legacy and e-business environments.
- **The Tivoli Access Manager family:** An end-to-end, policy-based access control security solution for operating systems, e-business and enterprise applications, featuring Web-based SSO and distributed Web-based administration.
- **Tivoli Federated Identity Manager:** This solution helps companies share rather than duplicate identity data. The Tivoli Federated Identity Manager handles all the configuration information for a federation, including the

partner relationships, identity mapping and identity token management.

- **IBM® Tivoli® Access Manager for Enterprise Single Sign-On:** Provides simple authentication capability across applications. It helps automate single sign-on, enhances security with automatic password management, and extends audit and reporting capabilities in a quick, simple-to-deploy solution.
- **Tivoli Directory Server and Tivoli Directory Integrator:** These solutions offer an identity data foundation for rapid development and deployment of Web applications, security and identity management and real-time synchronization between identity data sources, enabling enterprises to establish an authoritative, up-to-date identity data infrastructure.

Monitoring Solutions

IBM Tivoli compliance, security information and event management solutions help companies actively monitor, correlate and quickly respond to IT security incidents across an e-business. In addition to the IBM Tivoli Compliance Insight Manager and the Tivoli zSecure suites referenced above, IBM solutions include:

- **IBM ISS Proventia SiteProtector™:** Supplies centralized visibility and management to the entire IBM ISS protection platform, as well as third-party security solutions.
- **IBM Tivoli Security Operations Manager:** Offers real-time security threat management with event correlation and incident management capabilities.
- **IBM Health Checker for z/OS:** Provides a foundation to help simplify and automate the identification of potential configuration problems before they affect system availability.
- **IBM Tivoli Security Compliance Manager:** Helps organizations quickly identify whether operating systems are in compliance with security policies, as well as establish security policies to help businesses comply with corporate and industry standards. The solution provides policies that can be customized to address specific corporate needs.

Conclusion

In the current regulatory climate, and with a seemingly never-ending variety of threats to combat, no organization can be complacent when it comes to security. Similarly, no organization can depend on a single security tool or service to provide complete, end-to-end information security. Instead, a business has to count on numerous security tools and services working in concert to get the job done.

No company understands this better than IBM. IBM has developed and assembled an array of security products and services that can address security requirements, no matter whether the organization is a small business that's just trying to mount a sensible defense or a sprawling global business facing regulatory compliance requirements and a burning desire not to become the next big security breach headline.

Whether you opt for a proven product, professional services to help you get your efforts off to a good start, or managed services that will handle your security needs day-to-day, you can be assured that your choice is backed by IBM and its more than 40 years of leadership in the IT security field.

For more information on IBM security products and services, go to: http://www.ibm.com/itsolutions/security.

ABOUT IBM

IBM is the world's largest information technology company, with 80 years of leadership in helping clients innovate. Drawing on a breadth of capabilities and best practices from across IBM and our extensive partner ecosystem, we offer clients within every industry a wide range of services, solutions and technologies that can help them improve productivity, respond rapidly to the needs of their business and reduce development and operations costs.