Realtime publishers

The Essentials Series:
Security Information Management

The Business Case for Security Information Management

sponsored by

SecureWorks®

by Dan Sullivan

Copyright Statement

© 2008 Realtime Publishers, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers, Inc or its web site sponsors. In no event shall Realtime Publishers, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

The Business Case for Security Information Management

Executives and managers have long had constant demands for their attention, from strategic planning and operation efficiencies to financial management and human resource issues. Today, we have to add security information management (SIM) to that list. It is a mistake to assume that information security is a technical problem best left to IT professionals; it is both a technical and a business challenge that demands a broad range of expertise and business acumen to address.

Information security is fundamentally a set of business and technical practices designed to protect an organization's information assets and infrastructure. This first article in this series on SIM discusses the need for a risk management approach to information security and describes for executives and non-IT managers a framework for understanding security risks and formulating a response based on business requirements. IT professionals will find the risk management approach fits well with IT operations and management practices. The discussion of this bridge between the business and technical approaches to SIM is organized around three key topics:

- Understanding and mitigating risks
- Prioritizing resources and spending
- Realizing the benefits of SIM

SIM begins with the principle that you cannot protect assets you do not understand.

Understanding and Mitigating Risks

The practice of risk management has developed in business as a rational, methodical way to understand the extent and types of risks we face and to optimize how we allocate resources to protect assets. This leads to a two-phase approach: assess risks and implement defensive measures.

Assessing Risks

Businesses face a wide array of risks, including changing market demands, inflation, industry consolidation, and fluctuation in the labor supply, to name several. IT and information assets face other types of risks as well, including, but not limited to:

- Data loss and disclosure of private and confidential data
- Loss of system availability due to network-based attacks
- Stolen computing, storage, and network resources due to botnets and other forms of malicious software
- Degraded network and application performance because of large volumes of unauthorized traffic (that is, spam)
- Loss of data integrity due to malicious tampering with data

Cyber-threats are so pervasive that an array of government and industry regulations has been established to ensure that businesses adequately protect the confidentiality and integrity of essential data and systems. Some of the most well known include the Payment Card Industry Data Security Standard (PCI DSS) for protecting payment card data, the Gramm-Leach-Bliley Act (GLBA) security requirements for financial services, the Critical Infrastructure Protection (CIP) standards for safeguarding power-generation utilities, and the Health Insurance Portability and Accountability Act (HIPAA) for securing sensitive health information. When assessing risks, one must consider how to both protect business operations and remain in compliance.

Protecting Business Operations

To properly manage risks, we must first understand the assets in an organization and the threats to those assets. Assets include physical infrastructure, such as workstations, servers, laptops, routers, storage arrays, and other hardware components. We must also protect intangible assets such as databases, applications, and confidential information. With an inventory of all IT and data assets, we can conduct a simple exercise: imagine if that asset were compromised or no longer available; could your business still function, and if so, how?

Consider several examples:

- If a Customer Relationship Management (CRM) database were unavailable because the server were infected with malware and the entire operating system (OS) and application stack had to be reinstalled, what parts of your business would be affected?

- If an email server were unavailable because allocated storage had been consumed by inordinate amounts of spam flooding the system, what business functions would be impaired?

- If an employee launched an insider attack to steal customers' credit card information, how would you detect the theft and prevent it? If it were not prevented, how would the business protect its customers and retain their business? What legal ramifications or liability would you face?

- If a botnet had infected a sizeable percentage of the business' workstations, how much IT staff time would be required to recover, what other operations would be delayed, and what is the opportunity cost to the business of having to mitigate this threat?

In each of these cases, one could readily argue that prevention is less costly than recovery. The potential for disrupted business is not the only cost of poor risk management; there are also concerns about compliance.

Satisfying Requirements and Maintaining Compliance

Government and industry regulations often require not only security controls but also the ability to demonstrate the effectiveness of those controls. This latter requirement often involves log management in practice. For example, PCI DSS requires companies to track and monitor access to cardholder data and network resources; GLBA specifies that banks must monitor networks and hosts for policy violations, misconfigured devices, and anomalous behavior on the network; HIPAA's technical requirements dictate the need for access and audit controls on protected health information. SIM provides comprehensive log management and can readily meet compliance requirements by aggregating log data and streamlining reporting.

Defending the Network

Defending a network is a multi-faceted operation. A defense-in-depth strategy, which incorporates multiple, varied security measures in a layered approach, is often used in network defenses. There are many forms of attacks, and the most sophisticated malware and directed attacks exploit multiple vulnerabilities. Analogously, network managers and systems administrators can use a SIM approach to coordinate multiple countermeasures to protect a business' information assets, ensure compliance with relevant regulations, and enable defense-in-depth measures.

A coordinated approach to collecting and analyzing security information provides several advantages over more isolated management approaches. Those advantages include the ability to detect targeted attacks, respond more quickly to attacks, and improve other technical controls.

Ability to Detect Targeted Attacks

Businesses can be the victim of targeted attacks—not just indiscriminate malware attacks—against their particular systems. These attacks take advantage of specific vulnerabilities in a network and its applications. For example, an attack may exploit a SQL injection vulnerability in a Web application, cause a buffer overflow on a network service running on an improperly configured server, or use a simple dictionary attack to discover administrator passwords on key servers. With a consolidated reporting system, information on the state of servers, firewalls, Intrusion Prevention Systems (IPSs), and applications can provide a comprehensive picture of your overall security posture. The ability to detect targeted attacks and other anomalous behavior is required by regulations such as GLBA and HIPAA.

Respond Faster to Attacks

Manually reviewing log files and alerts from different data sources takes time. Automatically collecting and correlating that data can help to significantly reduce the time to detect and diagnose an attack. This in turn reduces the time to mitigate the threat, minimizing the window attackers have to steal data or compromise systems.

Improve Other Controls

The information provided by a SIM system is a valuable resource for understanding the effectiveness of other security controls. For example, weaknesses in authentication systems may become apparent from log data indicating administrator activities on the financial system outside of normal business hours. This information in turn can motivate changes to server deployment and patch management processes. SIM information could also help identify firewall rules that can be tightened or IPS policies the need refining.

These advantages of SIM aid the needs of both the business and the technical managers.

Tools to Prioritize Resources and Spending

SIM systems can help business planning by providing tools and information to help assess the risk to assets. SIM applications can provide real-time risk management data, especially with regard to the level of activity for specific threats. For example, if the SIM system indicates a particular group of servers most subject to attack. These servers could then become top priority for patching because they are the most likely to be attacked. SIM systems are also useful for day-to-day management operations as well as long-term strategic planning. Operational metrics, such as the number of malware infections or the number of login failures, are useful for spotting events outside of normal, baseline ranges.

Long-Term Benefits of SIM

SIM practices may appear primarily defensive in nature, but they also enable more reliable business operations. When line managers and executives are confident their operation procedures can and will function under a range of circumstances, these processes will be more adaptive to the changing demands of the market:

- Would an executive be willing to sign off on a new project to launch a Web-based customer service portal if she was not sure the customer database was secure?
- Would a CIO allow employees to use their personal mobile devices to access corporate email and databases if those devices were not properly secured?
- Could an IT administrator support remote networks without proper monitoring and management tools?

SIMs and other security measures reduce the likelihood that concerns about security will curtail innovation.

As the demands for compliance grow, businesses need tools to monitor and respond to security incidents and to document and report on their ability to respond. SIMs can help reduce the time and staff resources required to meet immediate compliance requirements as well as facilitate compliance over the long term.

Perhaps the most significant cost justification for a SIM investment is saving the cost of a single data loss incident:

- A 2007 study by the Ponemon Institute in the United States found, on average, companies lost $197 per lost record, up from $182 per record lost in 2006.
- A 2007 Gartner study found the cost of complying with PCI was about $16 per account.

In short, the cost of compliance can range roughly from as little as one-twentieth to one-fifth the cost of non-compliance.

Average costs per record can sometimes hide the magnitude of breaches. For example, a breach of customer data at TJX stores appears to have cost the retailer more than $250 million. A breach at Fidelity National Information Services, Inc. in 2007 may have exposed 2.3 million bank and credit card records, and another at Hannaford Bros. Co from late 2007 to early 2008 may have exposed 4.2 million credit card numbers and related data. Given the cost per record and the number of records lost in some data breaches, the ROI on SIM can be substantial.

Summary

SIM is a business enabler. A secure information infrastructure is required to function in today's business world, but it must be maintained in a timely and cost-effective manner. This in turn requires the sound security strategy and cost-effective monitoring and data analysis that is enabled by SIM systems. CIOs, CSOs, and other IT professionals formulate security strategies by understanding and mitigating risks and prioritizing resources. SIM technologies are a key enabler for such strategic planning, they provide immediate benefits to day-to-day operations, and they can help avoid costly security incidents.