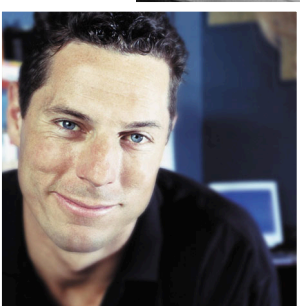


Effective Strategies for Risk Management

Business Process Protection Through Assessment, Planning, and Recovery



CONTENTS

Introduction	3
Anatomy of a Strong Security Program	3
Business Risk Management	4
Cost of Information Security Incidents	5
Patching and Vulnerability Assessment	8
Conclusion	8
About VeriSign	9

Introduction

With information security now demanding a significant level of attention from organizations, the traditional approach of identifying risk in purely technical terms has proven insufficient. Today, organizations must consider the areas that truly affect information security and integrate those findings into an overall risk management program to ensure effective and appropriate technology spending.

Perimeter security models have become a common practice for protecting critical business infrastructures and information. In particular, security controls between the Internet and an organization's internal network have become a consistent focus of technology spending. Although these organizations may have established strong perimeter security, it represents only a first line of defense. For an organization to effectively safeguard critical information, it takes more than integrating the latest security hardware and software. For critical business processes, a combination of interim and long-term strategies must be devised and implemented to attain and maintain an appropriate level of business protection.

Based on its experience in running critical Internet infrastructure services and the data gathered through the monitoring of intrusion detection systems and networks in VeriSign's Managed Security Services (MSS) environment as well as from the experience gained through its consulting engagements and vulnerability assessment results, VeriSign has developed a practice of business-oriented risk management for information security. The positive results of programmatic security management present tangible benefits for VeriSign's clients in their day-to-day management in addition to providing effective recovery when inevitable security incidents occur.

Anatomy of a Strong Security Program

VeriSign's findings indicated that organizations with the most successful security management programs shared consistent attributes. Based on these findings, VeriSign developed a set of criteria for measuring the effectiveness of security management programs, and in particular, threat and vulnerability management programs. These criteria are as follows:

- A well described inventory for critical business systems. This is a key component if threat and vulnerability management is applied to business risk management. The level of risk or threat to systems supporting a given business process is critical to the integration of business risk management and information security programs. Effective security programs target expenditures toward the most critical business risks. Unfortunately, the lack of understanding about the systems supporting a business process can lead to lengthy recovery when incident response is required.

- Diligent monitoring programs to detect attempted exploits against critical business systems and their dependencies.
- A detailed process for managing the “content” for detective systems (Intrusion Detection System (IDS) signatures, rule-sets for traffic inspection or network flows, firewall or host logging) so that the level of monitoring is well understood.
- Mechanisms in place to identify the specific vulnerabilities of systems supporting critical business processes. There are a number of mechanisms for this purpose, but they depend upon the size and complexity of the environment. Organizations can ensure that vulnerabilities are patched correctly by building standard operating environments or “gold configurations,” which are maintained and are used as the basis for developing a reference configuration to distribute, followed by the use of assessment tools or services.
- The ability to perform testing in a non-production environment and to cancel changes that are not successful.
- A mechanism for distributing patches on a regular basis with reasonable operational costs and impact. Mechanisms that cause greater downtime risk or that cannot be supported financially are not successful. A well thought-out process for testing to ensure that patches are deployed correctly is critical.
- The ability to introduce temporary countermeasures when patching cannot occur on a timely basis. A growing concern, as all evidence suggests, is that the current timeframe required to apply security patches exceeds many organizations’ tolerance for service interruption.

Business Risk Management

The results obtained from VeriSign’s operations and practice demonstrate that successful risk management in today’s online world requires organizations to build appropriate threat and vulnerability management programs to manage risks and monitor the systems deployed to support critical business processes.

VeriSign’s most successful clients incorporate technology risk into a more encompassing business risk management process. A complete technology and risk management program incorporates the following four principles:

1. An understanding of the requirements of the business process being assessed. This can include concerns over financial loss, damage to reputation, loss of intellectual property, devaluation of goods, and regulatory requirements (a critical driver), among other business specific risks.

2. An understanding of failure modes, including knowledge of how specific system compromises or failures can affect a business process and its relative risk. These risks need to be aligned with a management strategy: funding corrective measures if plausible, developing compensating controls, insuring the risk and, in most cases, developing a detection method for these failure modes.
3. Mapping of failure modes to a specific response. This is critical to managing risks that require response, such as the disclosure of data that may have reporting requirements as per Notice of Security Breach, CA Civil Code 1798.82¹ (formerly Senate Bill 1386), the failure of a system that may require administrative maintenance to return to service, or a specific failure mode that requires interruption of some activity to prevent financial loss.
4. Putting in place detective controls and operational monitoring, so that when a failure mode occurs it is detected without delay, and results in the appropriate response being enacted.

When this framework is practiced, systems risk – including vulnerabilities, design flaws and/or weakness in strength of controls – can be better described. An understanding of the risk involved, in particular failure modes, begins with a clear definition of terms and ensuring that the language is well developed. As a result, when a security incident warrants an executive decision such as a “go forward” strategy, the risk management plan is already in place to mitigate the threat. This framework includes the development of the language to describe business process risk and the operation of the supporting programs with the right levels of operational and capital spending resulting in security programs that are successful while remaining cost-effective.

Cost of Information Security Incidents

The cost of security incidents can have a hard-dollar financial impact in addition to loss of customer confidence, regulatory fines and individual consumer legal action. Most Fortune 500 companies have hundreds of incidents per year, with only a small percentage of those incidents resulting in significant financial loss. However, when losses do occur, they far exceed costs associated with upfront risk assessment, ongoing risk management, and information security programs, which are focused on protecting core business processes and the underlying systems and applications that support them.

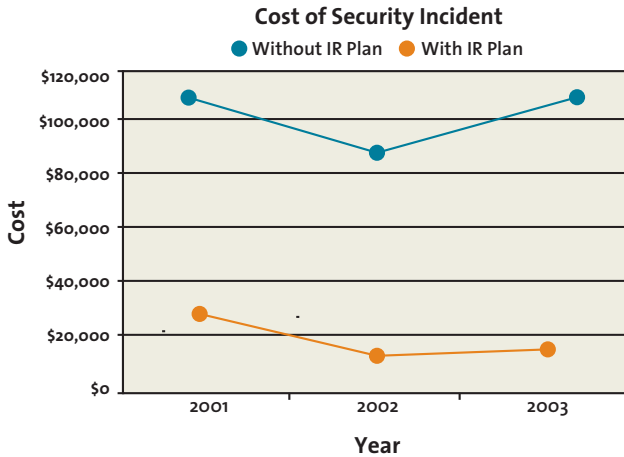
1 Other sections of the law include CA Civil Code 1798.29 and 1798.84. Act also referred to as the California Database Protection Act or the California Security Breach Information Act. For more information see http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

As organizations continue to rely on technology to Web-enable business processes, security risk increases. These risks must be identified and managed so that information security spending is closely aligned with business risk, risk management and the core business processes that are vital to an organization's ability to generate revenue or sustain operations. Spending according to generalized threats of overall Internet activity, or according to specific attack patterns, is not a comprehensive approach, since it does not address how the threat horizon may or may not impact the organization. Having a presence on the Internet makes any organization vulnerable, but in the vast majority of cases, the largest amounts of financial loss stem from an internal user, with authorized access to the network and its resources. Regardless of where the threat originates, appropriate, layered security controls, with comprehensive assessment, planning and recovery programs, are needed to address both the security threat and the growing list of regulatory requirements.

A key component of risk management is planning for the inevitable incident and ensuring that designated response plans decrease the overall impact to the organization. Incident response planning, in its most comprehensive form, is closely tied to understanding core business processes, the failure modes associated with each one, and then developing and implementing proactive, detective, preventive, and reactive countermeasures for each potential failure.

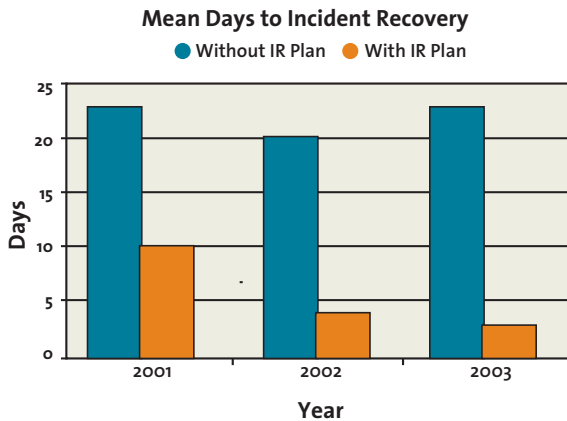
To maintain cost effectiveness and to ensure that spending on information security is not applied equally to the varying value of distributed computing assets, organizations must understand and maintain a prioritization of critical systems and applications upon which their key business functions rely. By using a business risk approach, incident response planning takes place at a more granular level that examines the most valuable information assets, failure modes for core business process that represent the greatest threats and response models that maximize risk mitigation.

Based on data compiled by VeriSign's incident response team and looking across a three-year history of engagements, there is a clear inverse relationship between upfront incident response planning and the total cost associated with incidents. From 2001 to 2003, VeriSign saw a fairly consistent average cost for security incidents for organizations with no prior incident response plan, ranging from a cost of \$112,500 to \$90,000. Conversely, the average for VeriSign clients with incident response plans in place ranged from a cost of \$25,000 to \$14,000 per incident.



In a few notable cases, the cost could not be measured. One organization, a VISA USA merchant services provider, lost their status with VISA due to the egregious nature of a security incident and the service provider’s non-compliance with VISA USA’s Cardholder Information Security Program. In another incident, intellectual property was stolen from a global financial services organization. They were not able to quantify the loss to the organization.

Cost of downtime can also be measured to identify the extent of financial loss. On average, VeriSign saw a consistent range of between 20- and 23- days to recovery for clients without formal incident response planning. For organizations with formal incident response plans, the average time to recovery was between three- and 10-days. Overall, VeriSign noted that recovery time over three years remained virtually the same for organizations without incident response plans, but recovery time improved over that same duration for organizations with an incident response plan.



Effective Patching

“Basketball is like war in that offensive weapons are developed first, and it always takes a while for the defense to catch up.”

- Red Auerbach

The VeriSign Alert Service, a component of the Managed Vulnerability Protection Service suite, has tracked over 1000 distinct vulnerabilities in the platforms that are monitored on behalf of the company’s clients.

Given that most organizations depend on a systems architecture comprised of technologies from a bevy of vendors, the number of vulnerabilities and subsequent patches clearly present a daunting problem in change management.

Each vulnerability in a production system represents a need for testing, patch application, re-testing for effectiveness and managing all of the workflow involved.

Unfortunately, most organizations treat vulnerability management as a much simpler process than it is, and do not have a plan in place for the day that they cannot effectively implement a patch, yet are aware of exploits occurring against vulnerable systems.

Patching and Vulnerability Assessment

Timing or reducing the window of opportunity once a vulnerability has been discovered is a critical parameter in mitigating risk. Unfortunately, an exploit is sometimes available for a period of time before a patch is available. In these cases, the only options for risk mitigation involve compensating controls with specific ones recommended by the software provider, or the enactment of response plans previously prepared. Adding to system vulnerability concerns, Qualys, a vulnerability assessment services company, recently published research showing that 80 percent of vulnerability exploits are available within 60-days after their release.²

The sheer magnitude of the problem and the risk it presents if not dealt with expeditiously, cause organizations to make difficult decisions: which patches are appropriate, when are they appropriate, and to what systems should they be applied? VeriSign's clients are most successful following its recommended model of risk management. First, understand the systems failure modes and then prepare an appropriate vulnerability management plan that incorporates mitigation strategies such as:

- OS hardening
- Development and management of standardized operating environments to promote a more controlled environment with less probability of patch requirement by nature of being a more compact "purpose-built" configuration with fewer moving parts
- Network compartmentalization
- Contingency policies for intrusion detection systems, firewalls, and routers to counter vulnerabilities which cannot be reasonably patched
- Patch management as a part of an overall configuration management program

Each of these strategies is supported by a set of technologies that ensures a best practice approach to this area.

Conclusion

VeriSign encourages corporations to take into account "business risk" as a guide to information security spending. Business risks such as liabilities incurred by not complying with government regulations, compromises of customer information that could lead to identity theft and availability failures, pose a great threat to organizations. VeriSign's most successful clients use a business protection strategy to identify critical systems, determine their failure conditions, and build mitigating controls that can detect or eliminate these failures and then support these controls with operating budgets that enable 24x7 monitoring and incident response.

² Source: Qualys, *Laws of Vulnerabilities*, 30 July 2003.

About VeriSign

VeriSign Inc. (NASDAQ:VRSN) delivers critical infrastructure services that make the Internet and telecommunications networks more intelligent, reliable and secure. Every day VeriSign helps thousands of businesses and millions of consumers connect, communicate, and transact with confidence. For more information on VeriSign's full line of security services, visit: **www.verisign.com**.

Note: In February 2004, VeriSign acquired Guardent, a recognized leader³ in Managed Security Services. Guardent's security consulting and managed services are integrated into VeriSign's solution portfolio.

³ See <http://www.gartner.com/reprints/guardent/118599.html> for more information.

© 2004 VeriSign, Inc. All rights reserved.

VeriSign and the VeriSign logo are trademarks and service marks or registered trademarks and service marks of VeriSign, Inc. All other trademarks are the properties of their respective owners. WP 050 0104