



WHITE PAPER

Effective Strategies for Risk Management

Business-Process Protection through Assessment, Planning, and Recovery



Where it all comes together.™



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



Introduction

Information security now demands a significant level of attention from organizations, but 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, this precaution 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 company must devise and implement a combination of interim and long-term strategies to attain and maintain an appropriate level of business protection.

VeriSign based on its experience in running intelligent Internet infrastructure services and data gathered through monitoring of intrusion-detection systems (IDS) and networks in the VeriSign® Managed Security Services (MSS) environment, as well as from the experience gained through its consulting engagements and vulnerability-assessment results, has developed a practice of business-oriented risk management for information security.

The positive results of programmatic security management, in addition to providing effective recovery when inevitable security incidents occur, present tangible benefits for VeriSign's clients in their day-to-day management.

Anatomy of a Strong Security Program

VeriSign's findings indicate that organizations with the most successful security-management programs share consistent attributes. Based on these findings, VeriSign has developed a set of criteria for measuring the effectiveness of security-management programs and, in particular, threat-management and vulnerability-management programs.

The criteria include:

- **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 (e.g., 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 on 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 nonproduction environment and cancel unsuccessful changes
- **A mechanism for regularly distributing patches with reasonable operational costs and impact**—mechanisms that cause greater downtime risk or that cannot be supported financially are not successful, and 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 time frame required to apply security patches exceeds many organizations’ tolerance for service interruption

Business Risk Management

The results obtained from VeriSign operations and practice demonstrate that successful risk management in today’s online world requires organizations to build appropriate threat-management 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 process of business risk management. A complete technology-management and risk-management program incorporates the following four principles:

- **The enterprise must understand the requirements of the business process being assessed.** These 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.
- **The enterprise must understand 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.
- **The enterprise must map failure modes to a specific response.** This procedure is critical to managing risks that require response, such as disclosure of data that may

have reporting requirements in terms of the Notice of Security Breach Act (California Civil Code 1798.82; formerly California 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.

- **The enterprise must put in place detective controls and operational monitoring** so that, when a failure mode occurs, it is detected without delay and the appropriate response is 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—failure modes in particular—begins with a clear definition of terms and an effort to ensure 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 development of language to describe business-process risk and operation of supporting programs with the right levels of operational and capital spending, resulting in successful yet cost-effective security programs.

Cost of Information Security Incidents

The cost of security incidents can have a hard-dollar financial impact in addition to regulatory fines, loss of customer confidence, and individual consumer legal action. Most Fortune 500 companies experience hundreds of incidents per year, although only a small percentage of those incidents result 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.

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 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, because it does not address how the threat horizon may or may not have an impact on 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 the actions of an internal user with authorized access to the network and its resources.

Regardless of where the threat originates, appropriate, layered security controls, in conjunction 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 and the failure modes associated with each one, and then developing and implementing

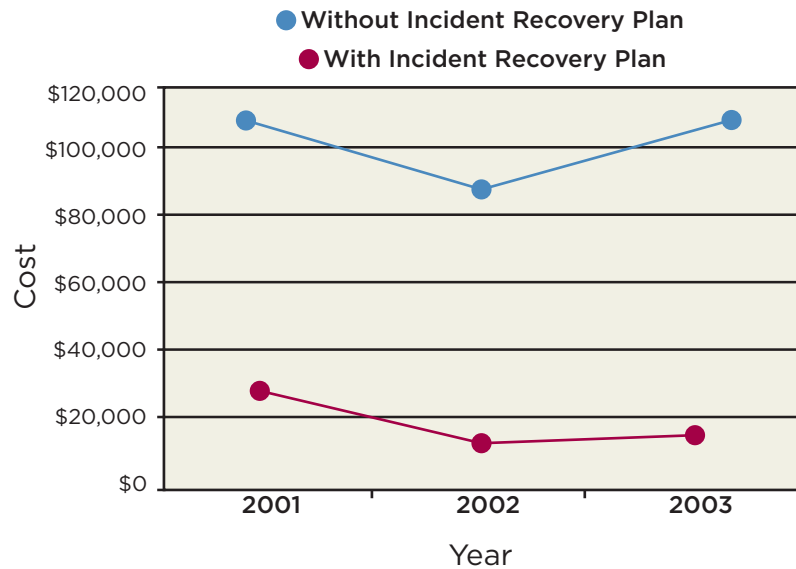
¹Other sections of the law include CA Civil Code 1798.29 and 1798.84. Act also referred to as the California Database Protection Act or the California Security Breach Information Act. For more information see http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

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 on 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 processes that represent the greatest threats, and response models that maximize risk mitigation.

Based on data compiled by the VeriSign incident response team and looking across a three-year history of engagements, a clear inverse relationship exists between up-front 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 \$90,000 to \$112,500. Conversely, the average cost for VeriSign clients with incident-response plans in place ranged from \$14,000 to \$25,000 per incident.

Cost of Security Incident



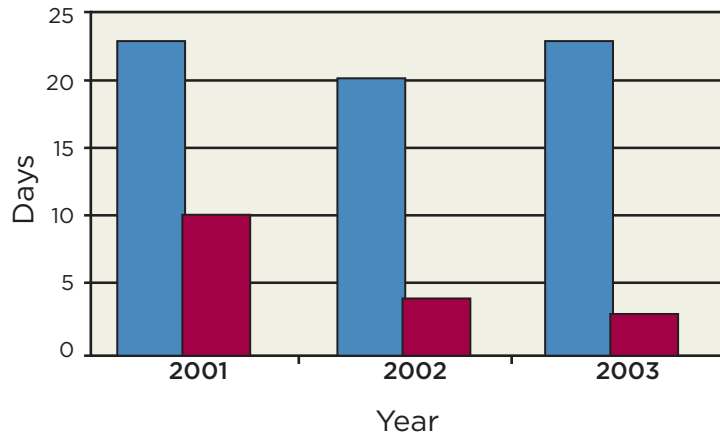
In a few notable cases, the cost could not be measured. One organization, a Visa USA merchant-services provider, lost its status with Visa due to the egregious nature of a security incident and the service provider's noncompliance with Visa USA's Cardholder Information Security Program. In another incident,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

Cost of downtime can also be measured to identify the extent of financial loss. On average, VeriSign saw a consistent range of 20 to 23 days to recovery for clients without formal incident response planning. By contrast, for organizations that had developed formal incident response plans, the average time to recovery was three to 10 days. Overall, VeriSign noted that measures of typical 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.

Mean Days to Incident Recovery (IR)

Mean Days to Incident Recovery

● Without IR Plan ● With IR 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 VeriSign® Managed Vulnerability Protection Service suite, has tracked more than a thousand distinct vulnerabilities in platforms monitored on behalf of the company’s clients.

Given that most organizations depend on a systems architecture consisting 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, applying patches, retesting for effectiveness, and managing work flow.

Most organizations treat vulnerability management as a much simpler process than it is, and do not have a plan in place for the day when they cannot effectively implement a patch yet are aware of exploits occurring against vulnerable systems. The VeriSign Alert Service provides such organizations with a much-needed advance-warning system.

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 some time before a patch is available. In these cases, the only options for risk mitigation involve compensating controls with specific ones the software provider recommends or enactment of previously prepared response plans. Adding to system-vulnerability concerns, Qualys, a company providing vulnerability-scanning services, 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 clients are most successful following the company’s recommended model of risk management. First, understand the system’s failure modes, and then prepare an appropriate vulnerability management plan that incorporates mitigation strategies such as:

- Operating System (OS) hardening
- Developing and managing standardized operating environments featuring more compact, purpose-built configuration with fewer moving parts to promote a more controlled environment with less probability of patch requirement
- Compartmentalizing the network
- Formulating contingency policies for IDS, intrusion prevention, firewalls, and routers to counter vulnerabilities that cannot be reasonably patched
- Managing patches as 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.

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



Conclusion

VeriSign encourages enterprises to take into account business risk as a guide to information security spending. Business risks such as liabilities incurred by failure to comply with government regulations and compromises of customer information that could lead to identity theft and availability failures pose a great threat to organizations. The most successful VeriSign 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 24/7 monitoring and incident response.

+ Learn More

For more information about VeriSign Managed Security Services and Global Security Consulting, please call 650-426-5310 or email enterprise_security@verisign.com.

Visit us at www.Verisign.com for more information.