



Patch and Vulnerability Management

The Core of a Comprehensive Security Strategy

Introduction

Organizations worldwide are increasingly taking a more formal, rigorous, and defensible approach to business management and operations. Corporate governance and risk management principles are being embraced at least in part to respond to a growing number of global regulations and standards that codify the need to diligently manage financial and operational risk.

Of course, we are also in an era where technology is critical to the business. This in turn establishes the need for IT governance and, subsequently, a comprehensive security strategy to ensure the integrity and availability of critical business systems, financial records, and other essential data. At this level organizations must tackle a wide range of challenges, including the need to prioritize their security initiatives to mitigate risk as efficiently and effectively as possible.

In this regard, this paper argues that organizations should first establish a robust patch and vulnerability management solution as the core of their information security strategy. This is because such a solution actually remediates known weaknesses, affording it a significant advantage over other countermeasures in terms of efficiency and efficacy. Nonetheless, as will be discussed, adding further layers of defense will still be appropriate to help ensure that a truly comprehensive level of protection is achieved.

The Emerging Order of Business Priorities

A growing volume of global legislation, industry regulations, and standards are causing corporate governance and risk management principles to become a top priority for business executives. Two key points pertinent to this trend are as follows.

- **It is truly a global phenomenon.** Within the US, current regulatory concerns include but are not limited to SOX, HIPAA, GLBA and the Patriot Act as well as a wide range of state regulations such as California's SB 1386. From a global perspective regulatory concerns include PIPEDA in Canada, the European Directive, Basel II Accord, and KonTraG in EMEA, and similar laws and regulations that have been established or which are being formulated in Australia, South Korea, and other Asia-Pacific countries. Clearly US businesses are not the only ones experiencing this transformation.
- **There is indeed a transformation underway.** Information security and privacy issues and the impact they have on fundamental business processes and overall fiscal responsibility are now being recognized at the executive and board level within companies of all types and sizes. The result is the treatment of these issues in a more strategic and holistic manner. Indeed, in its coverage of Top Trends for 2007 (11/17/2006), CIO Insights reports that 73 percent of surveyed organizations now have their enterprise-wide IT-security strategy being part of a larger enterprise-wide risk-management strategy that includes regulatory compliance, legal, insurance, and other risks.

Whatever the impetus, the emerging order of business priorities is to have governance and risk management be the primary focus, with compliance

achieved as a by-product of higher-level objectives. This certainly sounds like an appealing approach to take. But what does it really mean? What do corporate governance and risk management actually entail?

Understanding Corporate Governance and Risk Management

At a high level, corporate governance is concerned with the proper management of a business. The goal is to align as nearly as possible the interests of shareholders, the corporation, and society in general. In this regard, certain events of the past decade (e.g., the collapses of Enron and WorldCom), have resulted in emphasis currently being placed on ensuring the integrity of financial systems. Organizations must now be able to demonstrate that they have implemented robust, internal controls and must conduct more thorough internal and external auditing and reporting.

In addition, another inherent component of corporate governance that organizations must be able to demonstrate adherence to is the practice of risk management. This is the formal process of identifying threats to which the business is exposed and explicitly taking action either to accept, transfer, or mitigate the associated risk.

Going one level deeper, proper corporate governance, IT governance, and risk management practices must incorporate the following characteristics and capabilities.

- **Accountability** is a fundamental tenet of governance. It involves executives and board members taking responsibility for all operations critical to the organization's success, including its information security and privacy practices.
- **Maximizing the value** of (infrastructure) investments is another central theme. The protection of customer and corporate assets is important but must be balanced by responsible spending and the need to preserve/grow shareholder investments.
- **Efficiently maintaining effectiveness** depends on solutions (i.e., people, processes, and technology) being sufficiently flexible to adapt to changing conditions.
- **Measurement**, as well as internal and external reporting, facilitate continuous monitoring, improvement, transparency, and verification all of which are essential to conducting business in accordance with each of the previously listed items.

Ultimately, IT solutions must reflect these same characteristics and capabilities. However, for security and privacy, they are not the only factors that need to be addressed.

Additional Challenges Pertaining To Information Security

Additional obstacles and associated implications that are applicable when it comes to achieving comprehensive information security include the following.

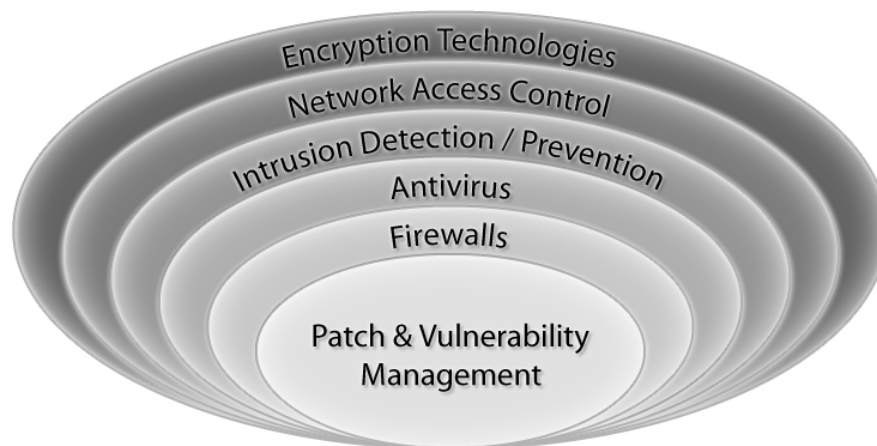
- The diversity and quantity of threats to an organization's computing systems is overwhelming. Everything from traditional and emerging malware (e.g., viruses, worms, trojans, bots, and spyware) to targeted attacks (e.g., denial of service, phishing, and general intrusions) and threats from insiders (e.g., data theft/leakage) must be addressed. This indicates the need for **countermeasures that are highly efficient** – ones that simultaneously cover multiple aspects of the threat landscape.
- Similarly, the greater elusiveness of today's threats dictates the need for **safeguards that are more effective**. This is primarily a result of attacking higher up the computing stack (e.g., at the application layer), as well as the increased modularity of threats, which enables blending and easy creation of variants.
- Quicker threat generation and faster propagation times are also problematic. No longer are infrequent or periodic scans for vulnerabilities and checks of defensive measures sufficient. Instead, both **continuous monitoring and continuous policy enforcement** are necessary.
- The number of vulnerabilities available for exploitation continues to rise as organizations continue to embrace new technologies. This conveys the need for **safeguards that are adaptable**. This way coverage can be provided without the organization having to purchase a plethora of security point products.
- Security and compliance budgets are stabilizing and, in any case, are finite. Consequently, meeting and demonstrating compliance with ever-expanding requirements means that organizations must accomplish more with less. **Extensive automation** of corresponding processes and **robust reporting** will be crucial to continued success.

One final, significant challenge for most organizations is identified by long-time security analyst Mark Bouchard of Missing Link Security Services, LLC. "With so many priorities to balance and so many best-of-breed security point products to pick from, it is not surprising that enterprises have difficulty beginning the transformation of their current security efforts into a holistic security strategy – one that is consistent with good corporate governance and the principles of risk management. Given the scope of automation, efficiency, and effectiveness that can be achieved, an appropriate place to start is with the implementation of a robust patch and vulnerability management solution."

Patch and Vulnerability Management at The Core

Having patch and vulnerability management as the core component of a comprehensive security strategy is fundamental because it provides a strong foundation as the first line of defense.

The First Line of Defense



Patch and vulnerability management makes sense as a first line of defense because it aligns well with what organizations need from a security solution in order to manage risk. Overall, it is an efficient, effective, and a highly economical countermeasure.

Efficiency is derived from the fact that patching a vulnerability stops all threats against it, both current and future, without any further effort. This is because patching actually remediates the underlying problem. In addition, in contrast to many other countermeasures, patching is definitively accurate and therefore does not generate tons of false positives for administrators to investigate. In fact, with a modicum of integration, it can even help reduce the number of false positives generated by other tools.

Effectiveness is derived primarily from the ability of patch and vulnerability management to work without having to explicitly know about a given threat. As a result, by simply correcting a known weakness, it can stop both known and unknown (i.e., zero-day) attacks. In contrast, many other tools suffer from false negatives (i.e., not stopping an actual attack) because they are dependent on the much more difficult task of predicting, identifying, and then stopping something that is unknown.

Finally, the *economy* of patch and vulnerability management is due in large part to its outstanding degree of efficiency and effectiveness. However, it also stems from its scope of coverage. Unlike many other countermeasures, patch and vulnerability management provides protection for all layers of the computing stack (e.g., network, transport, application) without having to resort to an array of supplementary, single-purpose tools.

The net result is that patching efficiently provides virtually definitive protection against all threats designed to exploit vulnerabilities in an enterprise's computing systems. Andrew Jaquith, senior analyst with Yankee Group, confirms that "Patch management is an essential part of keeping systems up-to-date, and in a known state. Identifying what systems require remediation, and determining which ones get fixed first, can be extremely costly in terms of time and soft labor dollar. The degree to which an organization keeps its infrastructure up-to-date is a strong indicator of the effectiveness of its overall security program."

PatchLink: Providing an Enhanced First Line of Defense

The foundational capabilities and benefits of patch and vulnerability management, as described in the previous section, are definitely a step in the right direction. However, the market-leading products and services available from PatchLink enable organizations to elevate their patch and vulnerability solutions to a much higher level. They do this by more fully addressing both the organization's core security needs as well as the key capabilities essential to good corporate governance and risk management.

PatchLink Update is the heart of the market's #1 selling patch and vulnerability management solution. It features the world's largest repository of platform and application patches, an agent-based architecture, PatchLink Pre-Testing and patented Digital Fingerprint Technology. PatchLink Pre-Testing saves customers considerable time by providing complete packages for patch implementation (e.g., scripts, applicability information) and hundreds of hours of quality assurance checks to ensure the suitability of patch packages in all necessary environments. Patching accuracy is subsequently assured by using Patch Fingerprints, or unique profiles for each machine, to continually monitor that applicable patches remain properly installed.

Overall these capabilities enable PatchLink Update to automate a best-practices, lifecycle-based approach that consists of:

- Thorough assessment, to compile an ongoing inventory of all endpoint resources (e.g., software, services, and hardware) that are susceptible to vulnerabilities;
- Intelligent remediation, to accommodate policy-based deployment of patches, software, and even data;
- Continuous validation, to ensure patches remain properly installed over time; and
- Comprehensive audit reporting, in the form of standard, real-time reports that document changes, patch process status, and policy compliance.

PatchLink Developers Kit extends the power and capability of PatchLink Update, enabling organizations to (a) deploy and patch custom applications, which are then automatically included in detection, verification, audit, and reporting processes, and (b) develop, test, deploy, and continuously monitor and enforce custom configuration policies.

PatchLink Enterprise Reporting, integrated with PatchLink Update, is a fully customizable, centralized reporting solution that enables organizations to (a) measure and manage all aspects of the patch and vulnerability management process, and (b) accurately and efficiently demonstrate the real-time status of security and regulatory compliance.

According to Mike Wittig, President and CTO of PatchLink Corporation and Certified Information Systems Security Professional (CISSP), "The high degrees of automation, accuracy, and extensive scope of coverage provided by these three products are what set our solution apart from the rest of the market. Moreover, the core capabilities they provide can be enhanced and extended even further by taking advantage of additional elements of the PatchLink portfolio, including PatchLink Scanner Integration, PatchLink Quarantine, and a full range of professional and educational services."

Of course, it is important to recognize that when it comes to information security, there are no silver bullets – no one solution acting alone can provide all of the protection an organization needs.

The Need for Additional Lines of Defense

Despite the significant advantages that a robust patch and vulnerability management can bring to the table, additional measures are still needed to help secure an organization's computing resources. This is due primarily to the fact that there are numerous types of threats and attacks that operate without needing to exploit code-related vulnerabilities. Denial-of-service attacks and spam are based largely on taking advantage of normal operating conditions, phishing is based primarily on social engineering techniques, and many targeted intrusions simply take advantage of configuration errors. Furthermore, there are also scenarios where patching is simply not an option. Patching certain medical systems, other than during an annual maintenance window, may void certifications associated with their safe and legal operation.

For all of these reasons, it is important for organizations to employ additional layers of defense including firewalls, antivirus, intrusion detection/prevention, network access control, encryption technologies, and so forth.

Indeed, PatchLink customer Building Material Holding Corporation (BMHC), a Fortune 1000 company, is testament to the success of taking a multi-layer approach. BMHC relies on PatchLink Update and the PatchLink Developers Kit as the foundation of their security strategy, using them to help ensure their computing endpoints are resistant to attack. By complementing these PatchLink products with a range of other tools, including firewalls, antivirus, URL filtering, and intrusion prevention/detection systems, BMHC has been able to completely avoid service outages due to malware related attacks.

Conclusion

Corporate governance, risk management, and compliance initiatives dictate one set of requirements for IT solutions. A dynamic threat and vulnerability landscape dictates yet another. Taken in combination, these requirements point to the need for organizations to architect and implement a comprehensive information security strategy. This begins with establishing a robust patch and vulnerability solution as the core of such a solution – a role which PatchLink Update and the rest of the PatchLink solutions portfolio are well-suited to fulfill.

ABOUT THE AUTHOR

Mike Wittig, CISSP, has served in executive positions for several industry leading network security providers developing innovative technologies, and corporate and acquisition strategies. Currently, Wittig is President and Chief Technology Officer of PatchLink Corporation, and previously served as President and Chief Technology Officer of CyberGuard (NASDAQ: CGFW).

Wittig has garnered more than 15 "best of breed" technology awards by leading organizations and trade press, and are considered to be among the industry's best security solutions. Under his leadership, CyberGuard products achieved the most stringent industry certifications and became one of the most credentialed product lines in the industry. These credentials include ITSEC E-3 level security for the United Kingdom and Australian governments, FIPS-140-2, and Common Criteria EAL4+ evaluation, which is recognized by more than 18 countries.

Wittig holds a BS degree from the University of Florida's College of Engineering.



PatchLink Corporation
Scottsdale, AZ 85255
480.970.1025

www.patchlink.com