

How to Secure a Moving Target with Limited Resources

Effectively mitigating business risks while the evolution of threats blindfolds traditional defences

Authors: Dr. Stefan Frei, Research Analyst Director
Brian Birkvald, Technology Partner Director

Date: 29th June 2011

Table of Contents

Abstract.....	3
Evolving Threats	4
Easy Prey.....	4
Origin of Vulnerabilities.....	5
Cybercriminals Do Not Need 0-day Vulnerabilities	6
Limitations of Traditional Defences.....	6
Protecting a Moving Target.....	8
Comparing Patching Strategies	9
Patch Availability.....	12
Risk of Testing vs. Risk of Patching.....	13
Cost of a Failed Patch.....	13
Compliance, Security, and Business Risks	15
Conclusion.....	16

Abstract

Today, as security threats increase and regulatory requirements grow more complex, businesses are recognising that compliance and security are business-critical priorities. However, recent industry studies have concluded that investment in compliance does not necessarily reduce risks¹. To understand the dynamics behind this problem and how to solve it, Secunia has completed research into determining what is preventing the interrelation and harmony between IT security, risk management, and compliance.

This white paper outlines the limitations of traditional defence mechanisms; specifically how cybercriminals have refined the malware manufacturing and development process to systematically bypass them – thereby initiating an arms race with defenders. Security patches are found to be a primary and effective means to escape this arms race as they remediate the root cause of compromise. However, timely patching of the software portfolio of any organisation is like chasing a continually moving target.

Therefore, analysis within this white paper compares different patching strategies, under the assumption of limited resources, and challenges the common trade-off between the risk of patching vs. the risk of testing.

Measurements within this white paper demonstrate that an intelligent patching strategy is an effective approach for reducing vulnerability risks, as well as for maximising operational efficiency with minimal costs. Significantly, this research concludes that it is not the amount invested in IT security that is of importance for achieving optimal risk reduction with the same or less resources – rather, it is the type of technology and its capabilities that matter.

¹ HIPAA, HITECH Compliance Not Improving Health Care Data Security: Survey
<http://www.eweek.com/c/a/Security/HIPAA-HITECH-Compliance-Not-Improving-Health-Care-Data-Security-Survey-895411/>

Evolving Threats

From a Cybercriminal's Perspective

To apprehend a threat it is always a good strategy to understand it from the opponent's perspective. As a first order approximation, it could be stated that the opportunity for cybercriminals is a function of the number of hosts and the number of vulnerabilities present on these hosts:

$$\text{Opportunity} = \text{\#Hosts} \times \text{\#Vulnerabilities}$$

The number of hosts certainly correlates with the number of users with Internet access. It is estimated that around 2 billion users will have access to the Internet by the middle of 2011. This represents 28% of the Earth's population, or an increase of more than 400% in the last decade. With such a huge amount of Internet users, it becomes clear that end-points are being increasingly targeted as even the smallest rate of success of an attack translates into a considerable number of compromised systems. Furthermore, business and private end-points alike are very rewarding targets for cybercriminals as:

- ≡ **End-points are difficult to secure**
End-points are extremely dynamic environments with numerous programs and plug-ins installed. Paired with unpredictable usage patterns by users, this makes them formidable targets that are difficult to defend.
- ≡ **End-points are valuable**
End-points are where the most valuable data is found to be the least protected. By definition, end-points have access to all data needed to conduct an organisation's business.
- ≡ **Everyone is a target**
Every end-point represents a valuable target for cybercriminals, even if no sensitive data is present. The end-point's computing power and bandwidth provide valuable resources, for example as an infection point, proxy, or for distributed password cracking services.

Easy Prey

The second variable in this model is the number of vulnerabilities per host. To measure this number, data gathered from over 3 million users of the Secunia Personal Software Inspector (PSI), a free, lightweight scanner that identifies and patches insecure programs on end-points, is used. To assess the evolving risk, this white paper tracks a representative end-point consisting of the operating system (Windows XP) and a software portfolio with the Top-50 most prevalent programs found in the field. The Top-50 software portfolio is a conservative approach as 50% of users are found to have more than 66 programs installed. The Top-50 software portfolio contains software from 14 different vendors; namely 26 programs from Microsoft and 24 programs from third-parties (non-Microsoft).

Data from this analysis reveals an alarming trend: the number of vulnerabilities affecting this typical end-point increased from 225 in 2007 to 729 in 2010, or by 71% in the last year, as illustrated in Figure 1.

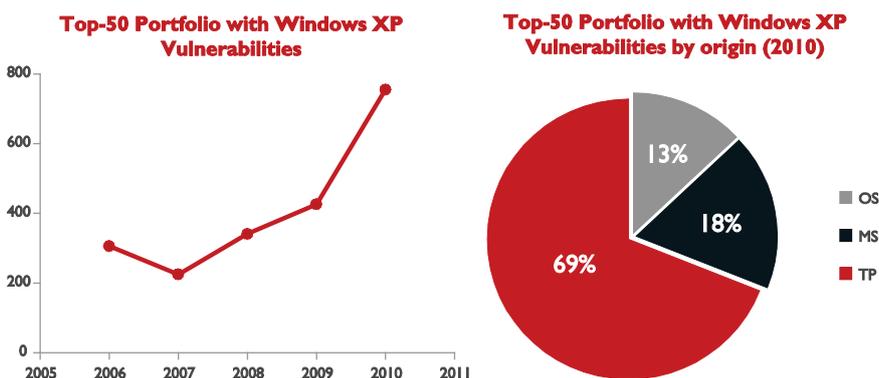


Figure 1 – History of the number of vulnerabilities affecting a typical end-point with Windows XP (left), distribution of the origin of vulnerabilities in 2010: OS operating system, MS Microsoft programs, TP Third-party programs (right)

This alarming trend supports the notion that end-point security is increasingly targeted. Furthermore, it is a relevant trend as most of these vulnerabilities are exploitable from remote and provide system access to the attacker.

Origin of Vulnerabilities

A breakdown of these vulnerabilities by origin reveals the driver behind this trend. The right panel of Figure 1 shows that vulnerabilities in third-party programs (TP) by far outnumber vulnerabilities in the operating system (OS) or vulnerabilities in the Microsoft programs (MS).

The share of vulnerabilities found in the operating system and the Microsoft programs versus all vulnerabilities found on the end-point, almost halved from 55% in 2006 to 31% in 2010. Thus, while patching the operating system and all

Microsoft products on a typical end-point remediated 55% of the vulnerabilities in 2006, the same patching strategy remediated only 31% of the vulnerabilities in 2010.

To fully patch a typical end-point, the user (or administrator of the system) has to master at least 14 different update mechanisms, as the Top-50 software portfolio comprises programs from 14 different vendors. With one update mechanism, namely “Microsoft Update”, the operating system and the 26 Microsoft programs can be patched to remediate 31% of the vulnerabilities. In addition to this, another 13 update mechanisms are needed to patch the remaining 24 third-party programs to remediate 69% of the vulnerabilities. This complexity to stay secure will undoubtedly leave a large number of systems incompletely patched – and thus vulnerable. Measurements support this belief. For example, research for Q4 2010 shows that, typically, 2% of the Microsoft programs are found to be insecure, while 6-12% of the third-party programs are insecure.

Cybercriminals Do Not Need 0-day Vulnerabilities

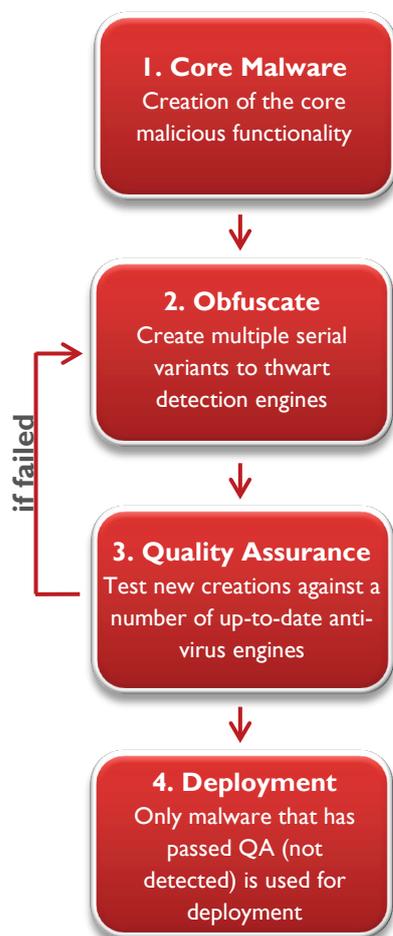
Figure 1 also reveals that timely patching of all Microsoft programs and the operating system does not disrupt cybercriminals’ opportunities at all. There remain plenty of opportunities for system compromise in the 69% of the third-party program vulnerabilities. Furthermore, it becomes clear that cybercriminals do not need precious 0-day exploits at all – at any given time there will always be a large number of systems present with numerous unpatched programs.

Traditionally, organisations perceive the operating system and Microsoft products to be the primary attack vector, thereby largely ignoring third-party programs in their risk matrixes. Thus, the prioritisation of patching most Microsoft products and perhaps a few third-party products is often found to be an established strategy. This strategy may have proved effective in the past to achieve the desired level of risk. However, data shows that the dynamics of the threat environment over the last five years results in an increasing gap of unmitigated risk if the patching strategy remains unchanged.

Limitations of Traditional Defences

To further understand today’s threat landscape traditional defences must also be reviewed. Since the mass adoption of firewalls, organisations’ main defence against cyber-threats relies mostly on technologies such as anti-virus and intrusion detection/prevention systems. However, creators of malicious software and botnet agents have developed and used a broad spectrum of tools and techniques to create “one of a kind” packages that can easily bypass traditional anti-virus technologies. Knowledge of the *malware development process*² helps to better understand the limitations of current defence technologies. The key process is the automated generation of new, obfuscated variants of malware on a massive scale followed by quality assurance, to ensure that only malware that is not detected is deployed. Today’s malware is typically developed using the following four step process:

² Serial Variant Evasion Techniques, Damballa
http://www.damballa.com/downloads/r_pubs/WP_SerialVariantEvasionTactics.pdf



1. Creation of the core malicious functionality

The core functionality of malware is created based on source code – either a compiled version, or a “commercially” available do-it-yourself malware creation kit.

2. Obfuscate malware

In order to render defence technologies, especially signature-based technologies, ineffective; a large number of serial variants/permutations of the core malware are created. While functionally identical, each permutation is a unique sample of malware which renders detection mechanisms ineffective.

3. Quality assurance

All samples created in step two go through a quality assurance process, which means that they are tested against all major, up-to-date anti-virus engines. Only samples that successfully pass this test (i.e. are not detected) are then used for deployment. Thus, at the time of attack, malware is known to be undetectable by anti-virus.

4. Controlled deployment in campaigns

Cybercriminals release a first batch of their malware and then monitor the detection rate in the field. By measuring the time to detection, they can then release subsequent batches in shorter intervals.

The result is a stealthy threat that evades signature-based detection systems, static analysis tools, behavioural monitoring environments, and sandbox technologies. Recent research and independent testing repeatedly confirms the scale of new virus variants and the limitations of anti-virus and malware detection technologies.

Results from NSS Labs, an independent research firm that tested 123 publicly known exploits against the corporate versions of the top 10 anti-virus software products, confirm the effectiveness of malware obfuscation techniques³. On average, exploit prevention software missed about a quarter of all known vulnerabilities. Furthermore, when these exploits are tweaked slightly in order to be less easily recognised, more than 40% get through. In 2008 Secunia tested 12 up-to-date security suites against 144 malicious files and 156 malicious web pages triggering vulnerabilities and found the best performing product to stop only 21% of the attacks⁴.

³ Study Shows Programs Designed To Catch Hackers’ Exploits Miss Nearly Half, Forbes <http://blogs.forbes.com/andygreenberg/2010/08/17/study-shows-programs-designed-to-catch-hackers-exploits-miss-nearly-half/>

⁴ Symantec beats the competition <http://secunia.com/blog/29/>

Symantec reported 286 million unique malware samples for 2010⁵. This helps explain why up to 9% of end-points in large enterprises were found to be bot infected, despite the implementation of best-of-breed security policies and perimeter protection⁶.

These numbers clearly demonstrate the ongoing arms race between cybercriminals and defence technologies trying to keep up.

Protecting a Moving Target

With 286 million malware samples counted in 2010, it becomes clear that patching vulnerabilities in software is a very effective security measure. A patch remediates the root cause of compromise and thereby neutralises a large number of attack vectors.

In light of limited security resources, it is imperative to utilise them optimally in order to achieve the desired level of risk compliance. The numerous vulnerabilities constantly found in the diverse software portfolio of any organisation represent the main security threat. In light of the limitations of anti-virus and other defence technologies, and the effectiveness of patches to remediate the root cause of compromise, controlled and timely patching of the infrastructure in order to minimise the business risk should be considered as a primary security measure. For typical organisations patching all programs is operationally and economically prohibitive. Furthermore, identifying and patching the right programs to achieve the largest reduction in risk is a significant challenge. From a security perspective, it is a bad investment to only deploy a patch for a program with vulnerabilities that are “Not critical” or “Less critical” while programs with “Highly critical” vulnerabilities remain unpatched.

Figure 2 illustrates the programs with critical vulnerabilities out of the 50 most prevalent programs for the period of 2006-2011. The 50 programs are listed vertically, with the most prevalent program at position 1 and the least prevalent program at position 50. Programs in which “Highly critical” and “Extremely critical” vulnerabilities are found in a given year are marked in red. Figure 2 illustrates that identifying the critical programs worth patching is similar to chasing a moving target. While some programs are vulnerable in several consecutive years, many programs are only vulnerable in some years while not in others. Programs with low prevalence are also frequently found to be considered critical in some years.

Today’s attacks typically use a large number of different exploits to open up attacks against a wide range of vulnerable programs. Different exploits are tried in sequence until one succeeds to compromise a vulnerable program; a process which is fully automated. New exploits are simply loaded as plug-ins, thereby ensuring that attackers can quickly and easily adapt to diverse target

⁵ Internet Security threat Report, Volume 16
<http://www.symantec.com/business/threatreport/index.jsp>

⁶ Damballa on Darkreading
<http://bit.ly/EntBot>

environments. Thus, less prevalent programs can also lead to compromise as these are not ruled out by cybercriminals.

Programs with highly/extremely critical vulnerabilities



Figure 2 – Visualisation of the programs with critical vulnerabilities in any given year from 2005 to 2011. The top 50 most prevalent programs are listed vertically, with the most prevalent at the bottom. Programs in which “Highly” and “Extremely critical” vulnerabilities are found in a given year are marked in red

Comparing Patching Strategies

What is the optimal strategy to achieve the largest reduction in risk for a given investment of security resources? Let us assume that an organisation with 200 programs in its infrastructure already patches the operating system, which is reasonable with the availability of “Microsoft Update”, and has the resources to additionally patch 10 different programs. The challenge is to identify and patch the “right” 10 programs out of the 200 – it is this approach that results in the largest reduction in risk.

To analyse the effectiveness of different patching approaches, two strategies of selecting 10 out of 200 programs to be patched every year over a five year period, are compared.

Strategy	Criteria
Top-10 by share	Every year patch the Top-10 programs with the largest market share found on end-points.
Top-10 by risk	Every year patch the Top-10 most critical programs based on the criticality of vulnerabilities.

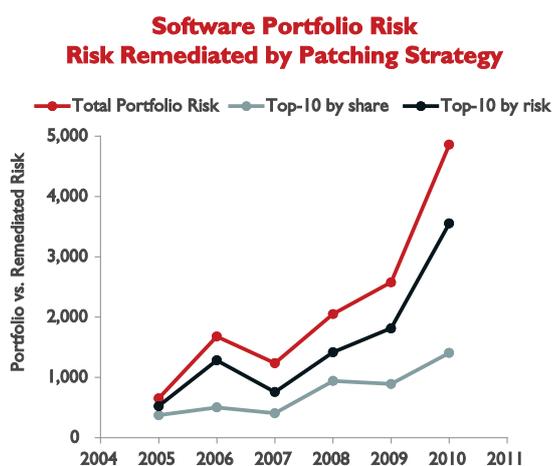


Figure 3 – Comparison of the resulting risk remediation over six years by A) patching the Top-10 most prevalent programs, or B) by patching the Top-10 most critical programs every year

Figure 3 above shows the risk remediated by the two patching strategies, compared to the total risk of all vulnerabilities in the 200 programs of the portfolio. The risk is calculated as the weighted sum of the vulnerabilities found in the programs:

$$\text{Risk} = 4 \times \# \{ \text{Extremely + Highly critical vulnerabilities} \} + 2 \times \# \{ \text{Moderately critical vulnerabilities} \} + 1 \times \# \{ \text{Not critical vulnerabilities} \}$$

Vulnerability data and criticality ratings are taken from Secunia’s vulnerability database⁷. The results are rather insensitive to the weight factors as long as higher criticalities are attributed increasing weights.

⁷ Secunia Advisories Terminology
<http://secunia.com/advisories/terminology/>

Results show that the total risk of the 200 programs in the software portfolio increased manifold since 2005 as expected. These results are also compatible with the findings reported in Figure 1. Surprisingly, the choice of patching strategy has a considerable effect on how much risk can be remediated by patching 10 programs every year. Averaged over the last six years, patching the Top-10 most critical programs remediates 71% of the total risk while patching the Top10 most prevalent programs remediates 31% of the risk, or 2.3 times less. Over the last six years, the strategy of patching the Top10 most critical programs every year covered 18 different programs in total. This further supports the notion of the moving target.

Metric	Patching Strategy	
	Top-10 by share	Top-10 by risk
Average percentage of risk remediated over the last six years	31%	71%
Total number of different programs patched over the last six years	18	10
Total number of “Highly” & “Extremely critical” vulnerabilities patched over the last six years	1,077	2,249

Thus, knowing what to patch is crucial in light of limited security resources. While patching the same number of programs per year at roughly the same expense, the optimal strategy results in 2.3 more risk remediated.

A considerable increase of security with limited resources is entirely possible, but requires the identification of the most critical programs. Prioritisation or knowing what to do pays off considerably. This is further highlighted by Figure 4 which plots the percentage of risk remediated by the two strategies when patching N out of the 200 programs.

Percentage of risk remediated Patching N programs by strategy

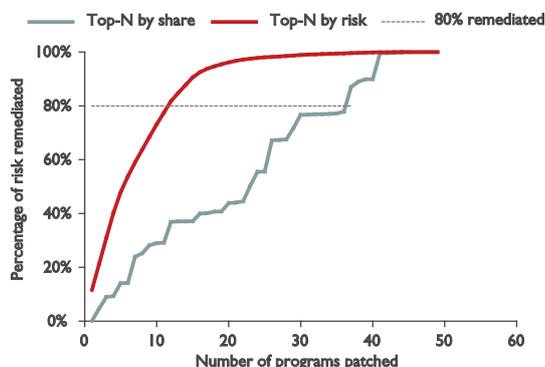


Figure 4 – Risk remediated by A) patching the Top-N most prevalent programs or B) by patching the Top-N most critical programs in 2010

In 2010, about 50 of the 200 programs had vulnerabilities. The challenge therefore remains in identifying the critical programs out of the 200, which implies constant monitoring of all 200 programs for security vulnerabilities. Figure 4 clearly demonstrates that the strategy of selecting the N programs to be patched has a considerable effect on the risk that can be remediated. If risk requirements demand that at least 80% of the risk has to be remediated, this can be achieved by either patching the Top-12 most critical programs or by patching the Top-37 most prevalent programs, as seen in Figure 4.

The dynamics of a software portfolio, paired with the rapid changes in the threat environment, imply a dynamic approach to ensure that organisations patch what is most critical from the risk compliance perspective.

The continued manual tracking of the criticality of vulnerabilities affecting all programs used in an organisation is cost prohibitive. However, solutions exist to automate this task and the cost of such solutions has to be weighed against the increase in security that can be achieved with less resources.

Patch Availability

The limited feasible protection against 0-day exploits⁸, paired with extensive media coverage, often leads to an overreaction of this threat. However, research indicates that for all vulnerabilities affecting a typical end-point in 2010, 65% had a patch available on the day of the disclosure of the vulnerability, and 75% of the vulnerabilities had a patch available within 10 days of disclosure. The mere possibility of 0-day exploits, a force majeure, does not justify ignoring 65% of the cases where effective remediation is possible and at users' fingertips.

⁸ Exploits taking advantage of a vulnerability before information of the vulnerability is publicly disclosed and a patch is available are commonly referred to as 0-day exploits

Thus, organisations can hardly hide behind the threat of 0-days when a solution is available for 65% of vulnerabilities.

Risk of Testing vs. Risk of Patching

Testing security patches before deployment is a crucial step to identify and prevent potential issues or incompatibilities introduced by the patch. However, extensive testing that considerably delays the deployment of critical security patches leads to an increased risk of system compromise. Research shows that the availability of exploit material increases to over 90% within days of vulnerability disclosure⁹. From the risk management perspective, the cost of testing paired with the increased risk of compromise while available patches are delayed, versus the cost of recovering from a failed patch times the risk of a failed patch, has to be weighed up:

$$\{\text{Cost of Testing}\} + P_C \times \{\text{Cost of Compromise}\} \text{ vs. } P_{FP} \times \{\text{Cost of a Failed Patch}\}$$

P_C Probability of compromise
 P_{FP} Probability of issues with a patch

The risk of a patch that causes incompatibilities or disrupts existing business processes after patch deployment drives the commitment of resources into testing. Assuming that the testing of patches identifies potential issues with a patch with 100% certainty, the cost of testing is justified by the averted cost of recovering from a failed patch. Testing can start with the availability of a patch. Upon the availability of a patch the vulnerability is made public and the availability of exploit material increases significantly, which in turn increases the probability of compromise P_C . Furthermore, the cost of compromise and recovery from compromise is typically higher and raises more questions the longer a patch is available but not deployed. Thus, the true cost of testing increases with the increased risk of compromise.

Cost of a Failed Patch

The cost of recovery from a failed patch certainly depends on the type of program being patched. If, for example, a patch of server software on which many services depend has issues, the cost of recovery can become high as compatibility issues are likely. This makes rolling back the patch and recovering from the issue extremely difficult. Therefore, extensive testing is more than justified. However, if a patch for a typical desktop program, for example, has issues, the damage is usually minimal and a roll back is easy and quickly completed. Furthermore, there are alternative programs to provide the functionality. Thus, for many programs, the cost of recovery (times the small

⁹ Modelling the Security Ecosystem, Workshop on Economics and Internet Security 2008 http://www.techzoom.net/papers/weis_security_ecosystem_2009.pdf

probability of an issue with a patch, P_fP) does not justify the expenditure and additional risk of extensive testing. This is especially true as the delayed roll out of the patch poses a considerable risk. Programs on end-points are especially at risk of compromise with the many attack vectors and the activity of the end-users. Server software, on the other hand, is typically better protected as the server does not surf the Internet, receive mails, or open different types of documents.

It is therefore advisable to reconsider the testing procedures and take the different types of programs, and their potential options to recover from a failed patch, into consideration. It is likely that for many programs, the achieved reduction in risk through expedited roll out of security patches more than pays off when compared with the rather small risk of recovering from a patch with issues. Furthermore, the resources saved from this strategy can help to speed up the testing of more complex programs.

Compliance, Security, and Business Risks

Due to increasing security threats and complex regulatory requirements, compliance and security are now recognised as business-critical priorities. Approaching this challenge holistically will add value to any organisation if the process is applied consistently and subsequently provides a transparent overview of the level of security that is present in the organisation.

Patching is a necessity and a fact of life, regardless of platforms, programs, or security tools. The following question therefore arises: How can an organisation balance the need to patch systems with the risks it faces and the need for stability within the organisation?

This answer lies with the implementation of a patching strategy integrated with an organisation's software management and operating system release strategy.

To achieve the desired level of security, the organisation must establish processes for the regular monitoring and correction of issues, ensuring that the risk is minimised and is compliant with the following regulations:

- | | |
|------------------------|---|
| ≡ ISO 9001 (Quality) | ≡ Family Educational Rights and Privacy Act (FERPA) |
| ≡ ISO 27000 (Security) | ≡ HIPAA |
| ≡ ITIL | ≡ FDA (US Food and Drug Administration) |
| ≡ 8th EU Directive | ≡ Sarbanes-Oxley |
| ≡ Basel II | ≡ NERC |
| ≡ Local Privacy Acts | |
| ≡ Privacy Act of 1974 | |

Management should therefore demonstrate support for, and commitment to, information security and privacy. Should a breach occur, at best an organisation will face huge fines. Worse still, non-compliance with regulatory mandates could directly result in loss of productivity, staff, and customers. This, in turn, could cause a negative knock-on effect regarding revenues, stock market value, brand image, as well as industry and consumer trust.

It is common knowledge that deploying patches is a complex process that is difficult to master and maintain. However, by using an integrated risk management process that holistically focuses on the criticality of the risks, organisations will be able to achieve higher long-term business value.

Documenting compliance, security, and risk statements help to:

- ≡ Improve decision making, such as identifying what to patch and determining the business risk of not patching
- ≡ Improve reliability and provide a clear overview of an organisation's compliance, security, and risk status
- ≡ Improve sharing of information with systems administrators, CISOs, and auditors
- ≡ Improve services to business units and suppliers with increased speed, accuracy, and visibility due to prioritised handling of patches
- ≡ Enforce consistent processes organisation-wide

Organisations must manage and identify the risks that exist across the enterprise – including internal compliance, internal controls, and operational risks. It is imperative that these areas work together in alignment to assist the organisation in understanding and leveraging the risks that they are exposed to.

Conclusion

Nowadays, organisations have to be compliant with a growing body of diverse compliance frameworks while investments in compliance do not necessarily reduce the right risks in order to defend against cyber-attacks. To reduce cyber-risks with limited resources, it is important to know the potential targets, the capabilities and limitations of traditional defences, and where to effectively complement defences. Security patches are found to be a primary and effective means to escape the arms race with cybercriminals, as patches remediate the root cause of compromise. This white paper has demonstrated that an intelligent patching strategy is an effective approach for reducing vulnerability risks, as well as for maximising operational efficiency with minimal costs.

About Secunia

Secunia is the leading provider of IT security solutions that help businesses and private individuals globally manage and control vulnerability threats and risks across their networks and endpoints. This is enabled by Secunia's award-winning Vulnerability Intelligence, Vulnerability Assessment, and Patch Management solutions that ensure optimal and cost-effective protection of critical information assets. Secunia's proven, complementary portfolio; renowned for its reliability, usability, and comprehensiveness, aids businesses in their handling of complex IT security risks and compliance requirements across industries and sectors – a key component in corporate risk management assessment, strategy, and implementation.

As a global player within IT security and Vulnerability Management, Secunia is recognised for its market-driven product development; having revolutionised the industry with verified and actionable Vulnerability Intelligence, simplified Patch Management, and automatic updating of both Microsoft and third party programs.

Secunia plays an important role in the IT security ecosystem, and is the preferred supplier for enterprises and government agencies worldwide, counting Fortune 500 and Global 2000 businesses among its customer base. Secunia has operations in North America, the UK, and the Middle East, and is headquartered in Copenhagen, Denmark.

For more information, please visit <http://secunia.com/>

Secunia
Weidekampsgade 14A
DK-2300 Copenhagen S
Denmark

Email: info@secunia.com
Phone: +45 7020 5144
Fax: +45 7020 5145

Copyright 2011 Secunia. All rights reserved.

This report may only be redistributed unedited and unaltered. This report may be cited and referenced only if clearly crediting Secunia and this report as the source. Any other reproduction and redistribution in print or electronically is strictly prohibited without explicit permission.