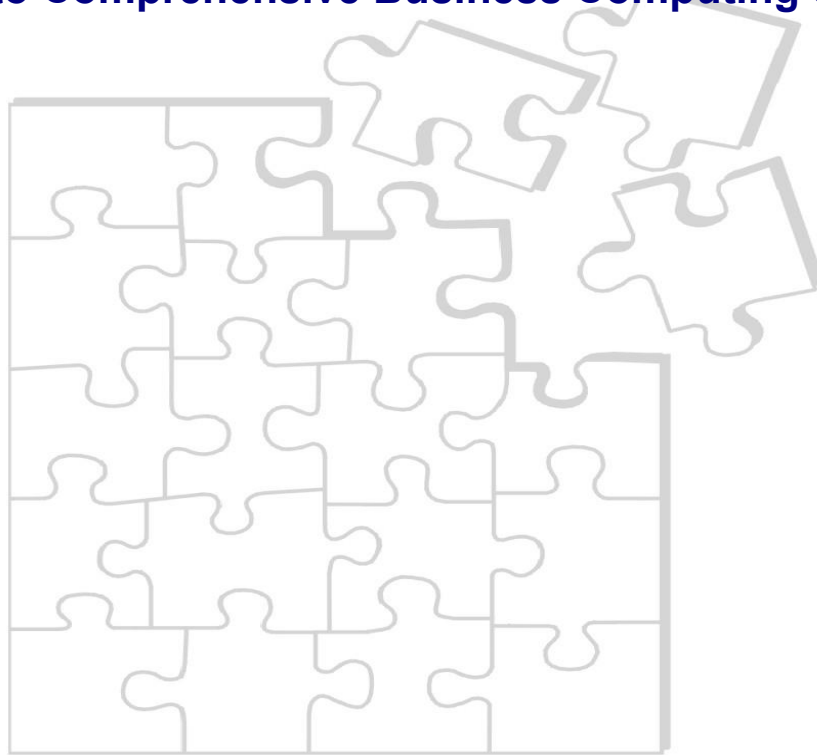




The Secret to Comprehensive Business Computing Security



Introduction:

The convergence and integration of operations and security management is an emerging and evolving reality for many enterprises today. Reasons for this convergence are being found in and documented by industry expert opinions and vendor-sponsored research, and solution-provider marketing collateral. Theory and market-speak describe the driving forces of complexity, technological sophistication and market pressures. However, to date there has been little discussion and information gathered from those directly involved in actual day-to-day IT and security operations.

We address that gap with this report based on interviews with those who are actually involved with and have experienced the challenges and benefits of integrated security and operations management. Interviews with IT staff and individuals were supplemented with a review of available literature and case studies to document the experiences, the solutions and the benefits being realized. The following presents what we learned along with the opinions of the IT operations staff we interviewed and researched.

Table of Contents

The biggest threat to business computing security 1
What’s driving all of this risk? 2
Just because a security control is simple to do, does not mean it will get done!..... 5
Moving beyond the security-operations blame game..... 7
Achieving operational security 8
Investing when there is “no ROI for security” 11
Conclusion 13

The biggest threat to business computing security

Every organization with networked computers has at least some level of awareness of the significant risks and threats to the private and proprietary data that resides in their infrastructure. Yet far too many enterprises, agencies, institutions and individuals have still found themselves the subject of leading stories and fodder for the news media because of successful data intrusions. All manner of data and information that should be secured with the most stringent protection methodologies and tools have found their way into public data streams via the internet or as the result of residing on lost, stolen or discarded endpoints – such as laptops, desktops, servers, and mobile devices.

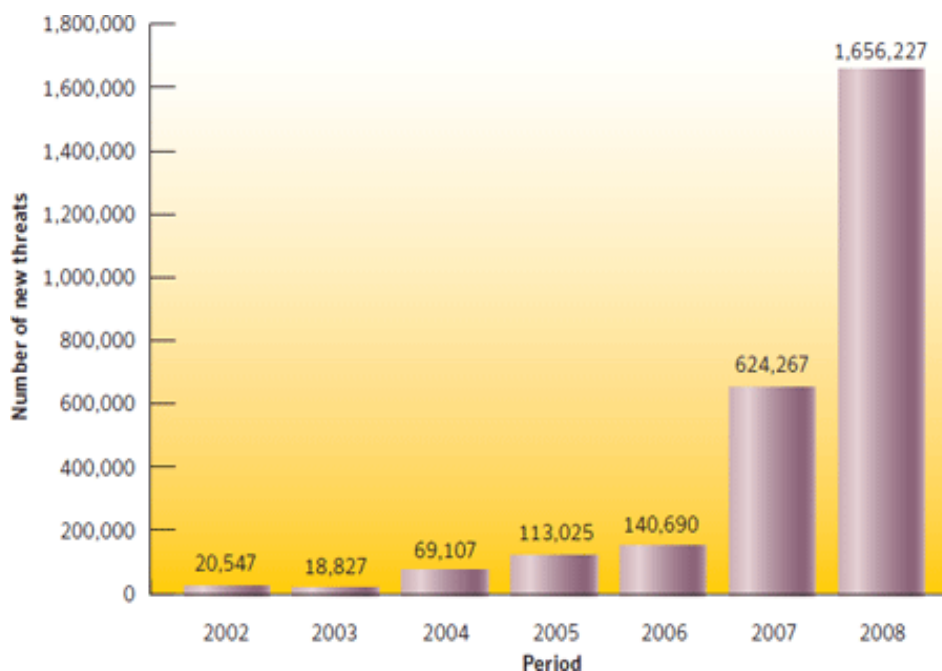
The threat to the endpoint and the supporting infrastructure has many forms as well as multiple sources. Many threats come from external sources with nearly all aided and enhanced by recent architectural innovation. A threat can be an attack made and enabled by a networked application. It can result from weak server (e.g. blades not properly maintained) or endpoint infrastructure management (e.g. missing a virus definition update). It can be the loss/theft of the device.

Enterprises, non-profit organizations, and governments, all are responding to the increasingly varied threat landscape by consolidating siloed security monitoring and post-event analysis tools into more comprehensive security suites. Even as their organizations reap the resulting benefits, IT staffs interviewed for this paper remain concerned about the exponential growth in the threat landscape.

The bad guys seem to never sleep, producing over 1.6 million new malicious code signatures in 2008 (Figure 1).¹ Security managers interviewed for this report all noted that they have given up on tracking traditional metrics such as port scans and automated attacks because, as one interviewee stated: “there are simply too many script-kiddies out there.” A study conducted by the Verizon Business RISK Team² reported “90 confirmed breaches within our 2008 caseload encompass an astounding 285 million compromised records.”

It is no longer sufficient to focus solely on high-priority patches and signature updates to lower your organization’s risk profile, the volume and value of enterprise data at stake is too great and the range of attack risks is too vast. The interviews and research indicate the need for a more comprehensive, integrated view of the environment to be taken.

Figure 1: New malicious code signatures (Source: Symantec Corporation)



What's driving all of this risk?

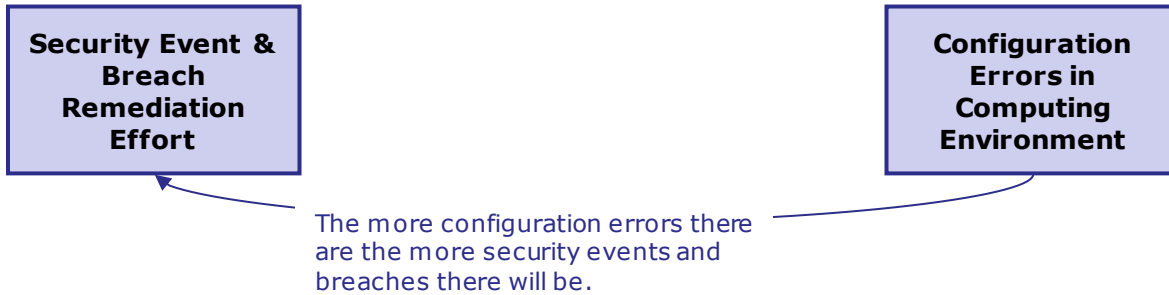
Some argue that the most pressing security problem for today's enterprise results from an under-developed or under-provisioned ability to detect vulnerabilities and automate patch deployment to remediate those vulnerabilities. We, as well as a number of those interviewed, don't entirely agree with that position. If your security remediation and patching process is very active, it can be an indication that you have deeper issues that are not being addressed.

One of the deeper issues is likely the result of the fact that more configuration errors in the environment results in a direct increase in the likelihood of security breaches (Figure 2). Our interviews appear to bear this out. Most of those interviewed expressed the opinion that better insight into configuration data would improve their risk posture. For example, one systems manager recalled that during a project to automate application performance and usage monitoring, they discovered over 600 active user accounts for employees that had left the organization years before. This discovery prompted an internal effort to integrate security, configuration and application management teams. Another, operations manager specifically mentioned that an unexpected benefit of using Symantec's Altiris solution* (purchased to automate their deployment and migration tasks) was a noticeable drop in the number of security-related events that required operations intervention. The Verizon study² also appears to support

* Symantec recently rebranded the Altiris solution suite as "Symantec Management Platform"

this conclusion, showing that errors (miss-configurations, omission, programming errors etc) either enabled or contributed to 67 percent of breaches.

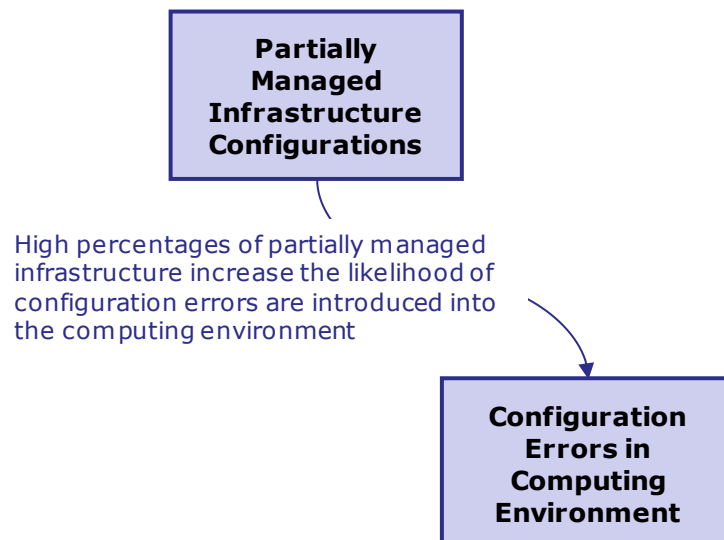
Figure 2: Configuration errors impact security breaches



The same Verizon study² also noted that known vulnerabilities and configuration errors are introduced by several means. Some are the result of issues with code quality, others result from device miss-configuration issues introduced during initial deployments, while others derive from configuration or access control changes introduced during migrations, upgrades, patching, problem resolution fixes, etc..

The issues with code quality tend to be exacerbated when a high percentage of the computing infrastructure is managed in an ad-hoc manner (Figure 3). According to a recent Symantec survey³, 54 percent of respondents actively manage less than 60 percent of their IT assets. With so much of the environment being left to 'its own devices' eventually even the best perimeter-based security solution will struggle to monitor for an ever increasing number of signatures that target the unmanaged weak spots in the network.

Figure 3: Partially managed infrastructure impacts configuration errors



The situation will only become more difficult over time as the number of networked computing systems skyrockets as virtual servers populate enterprise datacenters and the mobile revolution accelerates with the attendant proliferation of netbooks, smartphones, virtual desktop interfaces, etc. These will combine to dramatically increase the number of devices accessing enterprise information and applications.

Similarly, the study's comments about new deployments, migrations, upgrades, problem resolution fixes and patches touch on another deeper issue – the fact that known vulnerabilities and configuration problems are being introduced into systems at an increasing pace. Simply put, as infrastructure changes more frequently, the more vulnerabilities flow into the business' computing environment.

Yet infrastructure change itself cannot be shunned or cast in the role of the enemy of secured operations. Doing that only perpetuates a view of the IT organization as a hindrance to achieving business goals. Realistically, we all know that the pace of infrastructure configuration and access control changes is not going to decrease any time soon. The amount of employee churn in today's business environment only adds to the rate of change. Business users will always require new applications and new features which evolving technology and technologists willingly provide using n-tiered web applications and service oriented architectures that enable more rapid software development and upgrades.

However, this frenetic pace of change is one more reason why layered perimeter-based security products and automated compliance monitoring do not provide the whole story when managing business computing risk. The study conducted by Verizon² confirms this by reporting “87 percent of breaches could have been avoided through the implementation of simple or intermediate controls. All of these were the standard, run-of-the-mill practices that we in the industry see and use everyday.”

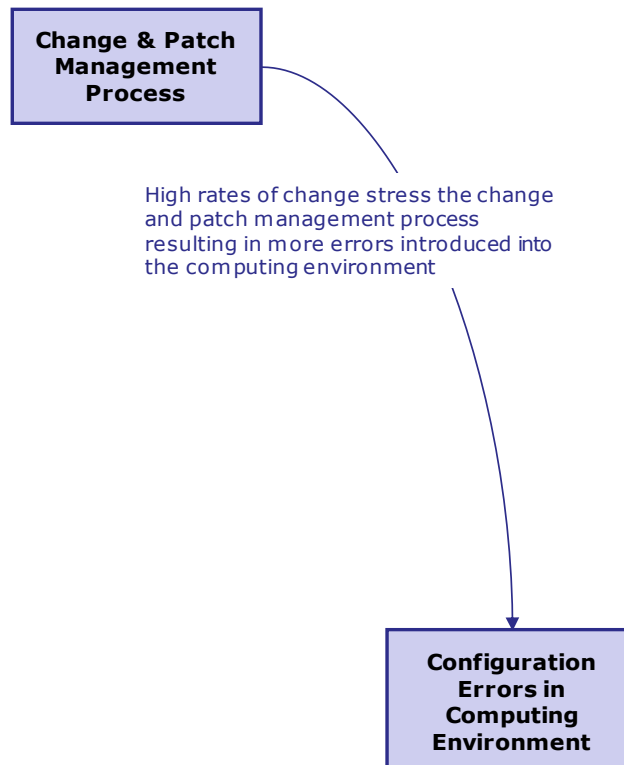
While the report did not specifically outline each of the controls, research from the IT Process Institute (ITPI)⁴ indicates that IT controls and maturity of processes do improve the overall performance of the IT organization. They also indicate that some IT controls improve operational performance more than others. Two of the top three controls are:

- Providing technical personnel with accurate information about current configurations.
- Thoroughly testing all changes before release.

Additionally, our interviews showed that experienced operations managers were well aware of and knowledgeable about best practices that **should** (emphasis added) be followed. For example, one interviewee stated that he was “tired of being a fix-it hero” and that he was more interested in “preventing these problems by configuring things the right way the first time.”

Others discussed the need for weekly or daily meetings between operations and security teams to determine the best process for introducing updates, patches and migrations in a secure manner. In other words, infrastructure change itself is not the root cause of security vulnerabilities. It is a highly stressed change and patch management process that introduces security vulnerabilities (Figure 4). It is the infrastructure changes implemented by multiple, disconnected, ad-hoc change processes with compliance controls implemented on only the ‘important’ fraction of the infrastructure that creates a vulnerable computing environment.

Figure 4: Changes impact configuration errors



For example, if IT staff use different patching mechanisms every time, or use different ways to implement configuration changes, or depend upon manual compliance checklists, or have an incomplete understanding of which systems require specific updates, or rely upon inaccurate infrastructure inventory – the result is that the required ‘simple or intermediate controls’ are not being actively implemented or followed.

Just because a security control is simple to do, does not mean it will get done!

It is not that the run-of-the-mill security best practices are particularly difficult in themselves. The problem comes from the number of times each different task has to be done and the limited

amount of time available for IT staff to do it. What typically happens is that time constraints and competing priorities trump completing simple ‘good security hygiene’ tasks.

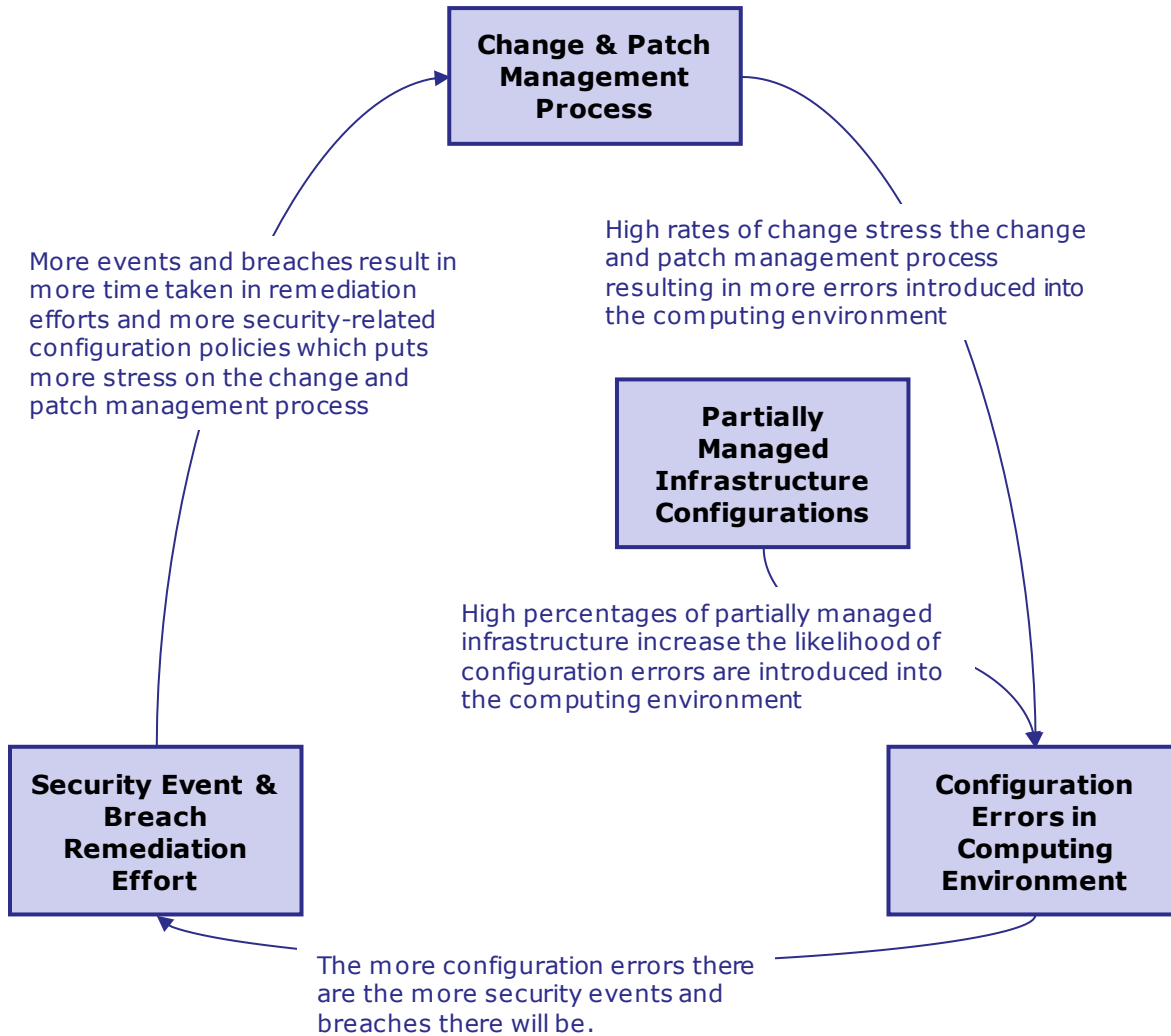
For example, any IT operations manager will tell you that a basic step in installing new software is to disable or change the default usernames or passwords supplied by vendor software. Yet this simple task often does not get done. Indeed, one of our recent interviewees noted that this was one of the strongest points of contention between the operations and security teams. He noted, “IT operations staff want to get patches up and running as fast as possible so they just accept the default installation options, but a lot of the time the default options take us out of compliance.” Basically they are faced with a classic tradeoff -- taking the time to do things securely or meeting their business demands for low cost (aka minimal IT time spent) and high agility (aka get it deployed fast).

When hygienic controls and best practices are short-circuited every day during normal IT operations it means that known vulnerabilities and configuration problems are introduced into the business computing environment. This results in higher security risks, higher potential for actual breaches and increased operational costs in terms of detection, response and remediation activities.

However, the solution often takes even more time away from the operations staff, as the interviewee went on to state, “what we are trying to do is work with them to review all the options before deployment.” Eventually this creates a self-reinforcing cycle (Figure 5), where an increasing number of security events and breaches result in more operations time taken in remediation efforts and more security-related configuration policies which puts more stress on the change and patch management process.

This often brings enterprises back to blaming IT operations – even as operations teams are under constant pressure to ‘do more with less’ and are consistently being maligned for having expensive labor costs, and using anywhere from 60 to 80 percent of their budget to ‘simply’ maintain systems. These pressures drive IT operations staff to skip compliance steps, ignore run-of-the-mill best practices, and workaround configuration controls in an effort to respond rapidly to the myriad of business, change, and security requests that flow onto their to-do-lists every day.

Figure 5: Security and operations cycle



Moving beyond the security-operations blame game

In the end, neither operations nor security teams benefit from ‘blame game tactics’ that delay effectively analyzing the bigger picture. Both teams can benefit by increasing their span of awareness to include an examination and understanding of external dependencies and influencers that negatively impact their specific responsibilities and tasks.

Looking at these relationships also moves the focus from assigning blame to addressing root causes. During our interviews we found that causes are often the result of actions that make perfect sense in themselves to one particular group, but inflict risk or damage in the context of overall enterprise operations. For instance, responding to a new mandate, the security team implements a more restrictive security policy for controlling automated file access. However, if

IT operations does not integrate this policy change into how it manages the file, the server it is located on and how other applications and services access that file then it is likely going to create a backlog of compliance events that IT must remediate and/or increase the risk of application or service failure due to an inability to access the file.

Simply sending an email to IT administrators notifying them of the policy change does not guarantee that all the additional work to integrate the policy change into daily operations will get done. Remember that when the operations team's workload exceeds the available operations team's resources, hygienic tasks always take a backseat to clearing the backlog of events and remediation work. Creating a collaborative environment where both teams can be effective is at the heart of achieving operational security.

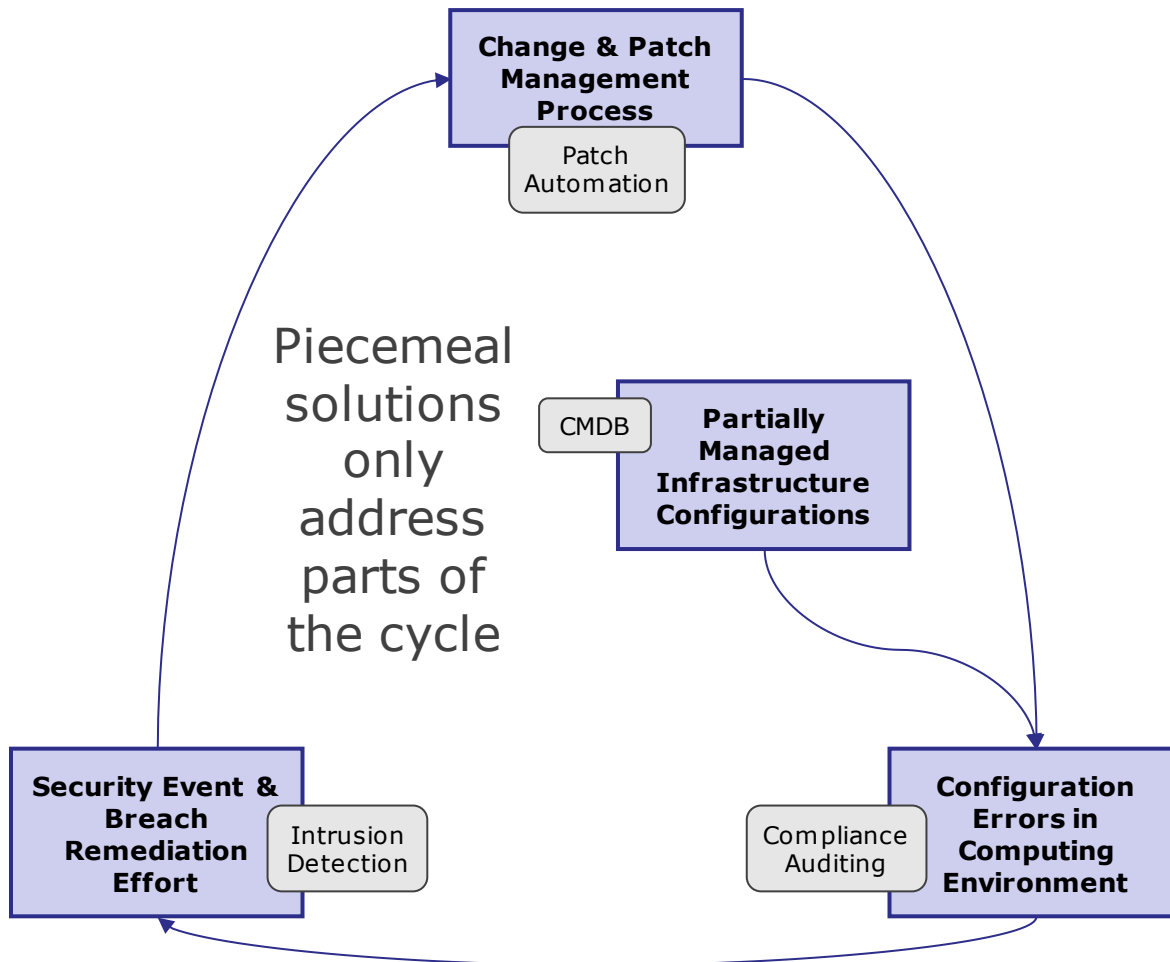
Achieving operational security

Operationalizing security requires forging a closer working relationship between the operations and security teams. The teams must work together to create feasible security plans and procedures for enforcement that can be followed on day-in-day-out basis. Acceptance and application of those enforcement procedures is critically important for success because they will only work if administrators consistently follow them as they go about their daily tasks.

Several of our interviewees are 'making do' with an ad-hoc approach to operationalizing security, depending upon developing and maintaining personal relationship between specific team members. For example, one company dedicated a single person to be responsible for responding to security patching and change requests. Other company dedicated a member of the security response team to coordinate and approve workflows for patches and updates.

One of the limitations of ad-hoc communication between security and IT teams is that it fails to address conflicting pressures and priorities across teams, which fuel the self-reinforcing cycle outlined in Figure 5. Additionally the ad-hoc approach allows operations and security teams to continue using siloed, compartmentalized tools focused on simplifying a specific operational task without truly automating the security-related aspects of the task. While each of these tools will individually provide significant benefits to each group, without individual effort to incorporate security-related aspect enterprises they will only rarely leverage the benefit across the entire cycle (Figure 6).

Figure 6: Piecemeal solutions only address parts of the cycle

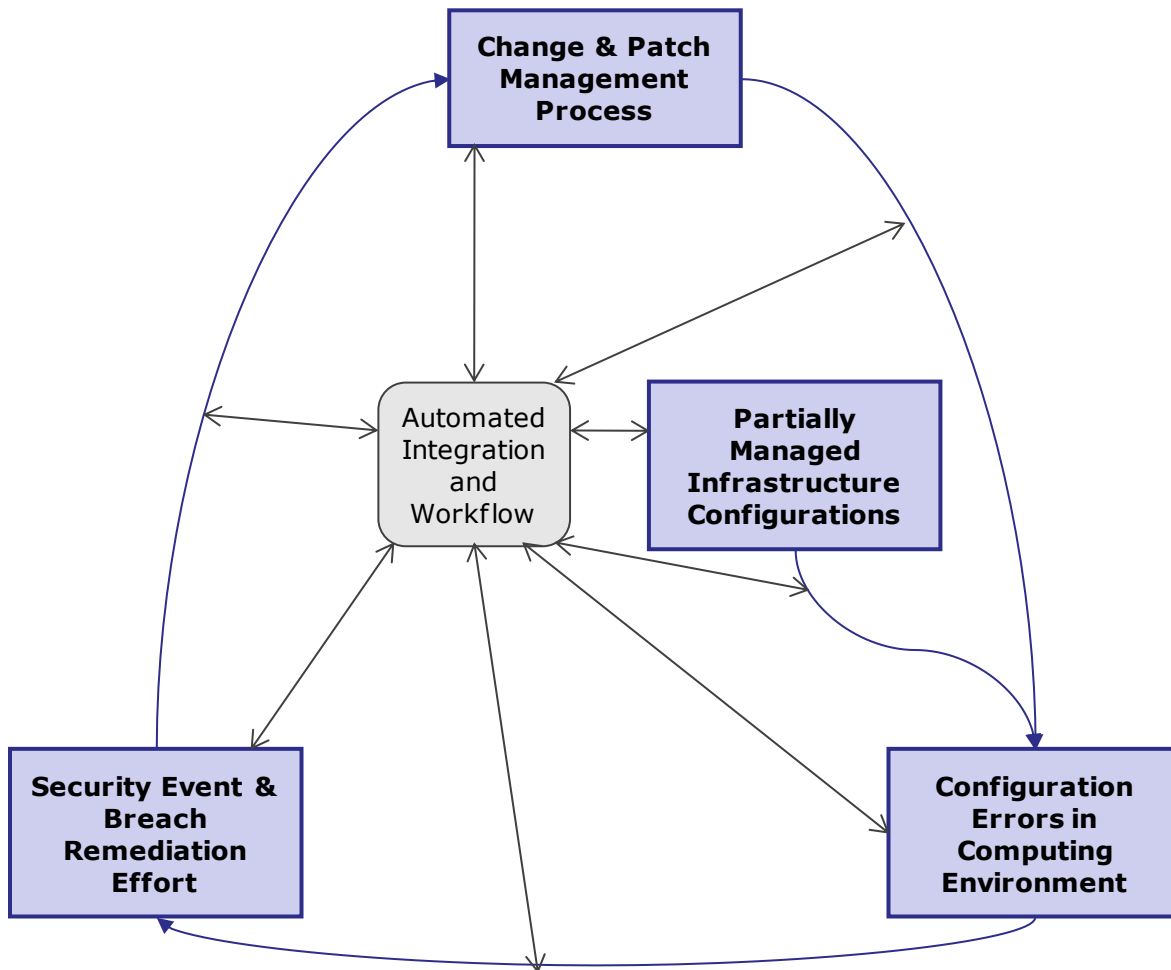


Another approach emerging in a few IT organizations eliminates the security and operations organizations entirely by merging responsibilities for security and operations tasks into a single job description. One interviewee shifted the culture of his team by demanding cross-training for existing staff and making ‘security-oriented mindset’ a requirement for all new technical hires. Thus, security implementation, its management and impact becomes an integral part of IT’s day-to-day working process. The resulting culture shift resulted in a dramatic drop in the number of ‘all hands on deck’ security issues which improved staff productivity and minimized unplanned downtime and service disruptions. It also minimized the time spent on coordination activities, communication gaps, and finger-pointing that occurs when separate groups have related responsibilities. The combined efficiency gains resulted in a significant shift in how the team spends its time. The team now spends most of time on implementing preventative measures and investigating how to securely adopt new technologies to benefit their user community.

This is a fantastic approach and well worth the effort for any team able to implement it. However, we recognize that this will be difficult to achieve with large operations and security

teams where specialization is necessary or where globally dispersed IT teams rely on formalized and repeatable processes and communication between specialists. This is where automation of integration and workflows across security and operations solutions play an important role (Figure 7). Not only does it reduce the backlog of operational work that must get done, but it also enables the organization to more quickly adapt its operations to security policy changes while forging closer working relationships between operations and security teams. Such solutions enable operations to complete the myriad of best practices tasks designed by the security team that should get done, but that don't get done because 'no one has the time to do them.'

Figure 7: Integration and workflows play an important role



When both cross-team workflows and cross-product integration can be automated, the entire cycle can be converted to a positive relationship. The security team will be designing policies that snap into automated workflows without creating time-consuming additional steps for operations staff. Similarly, operations team will focus on gaining better control over more of the infrastructure and providing more accurate infrastructure information to the security team when

issues occur. This change in emphasis helps enterprises operationalize security and provide the requisite checks and balances between the groups, while still allowing some separation of duties.

Investing when there is “no ROI for security”

One of the repeated themes emerging from our interviews focused on the difficulties the enterprise faces when trying to justify the cost of operationalizing security by automating the integration between security and operations tools. As one interviewee at a large gaming enterprise put it “It’ll cost me \$100,000 total to put in the integrated security-operations solution I want, but when I present that to the C-team they tell me that they can get a new gaming system for \$100,000 which would bring in many times that in revenue. Since we haven’t collapsed, as yet, they think we can continue as we have been. But honestly, I don’t want to live through a collapse just to get funding.”

A major hurdle that must be overcome, is when most business executives view security benefits in terms of trying to ‘prove a negative’, i.e. you’ve saved x amount because something hasn’t happened, in this case a security breach that hasn’t occurred. This thinking limits security benefit discussions to pointing at what hasn’t been stolen, or what liability has been avoided. This makes identifying savings and justifying expense a matter of a judgment of risk and value based on the recent experience of the decision-making executives instead of provable calculations. Similarly, no competent operations manager wants to detail all of the best practices that are skipped or work that simply cannot be completed with the available resources. Clearly, the basis underlying the security and operations benefits conversation must change.

In one response, vendor-supplied business cases have increasingly focused on measurable security and administrative metrics. For example, Business Value Analysis (BVA) studies available from Symantec provide detailed labor productivity gains achieved by the security teams:

- AgFirst⁵ was able to reduce the amount of time spent by one IT FTE on security threat management from one week each month to two hours
- State of Michigan⁶ reduced the number of security incidents by 8.5 percent annually

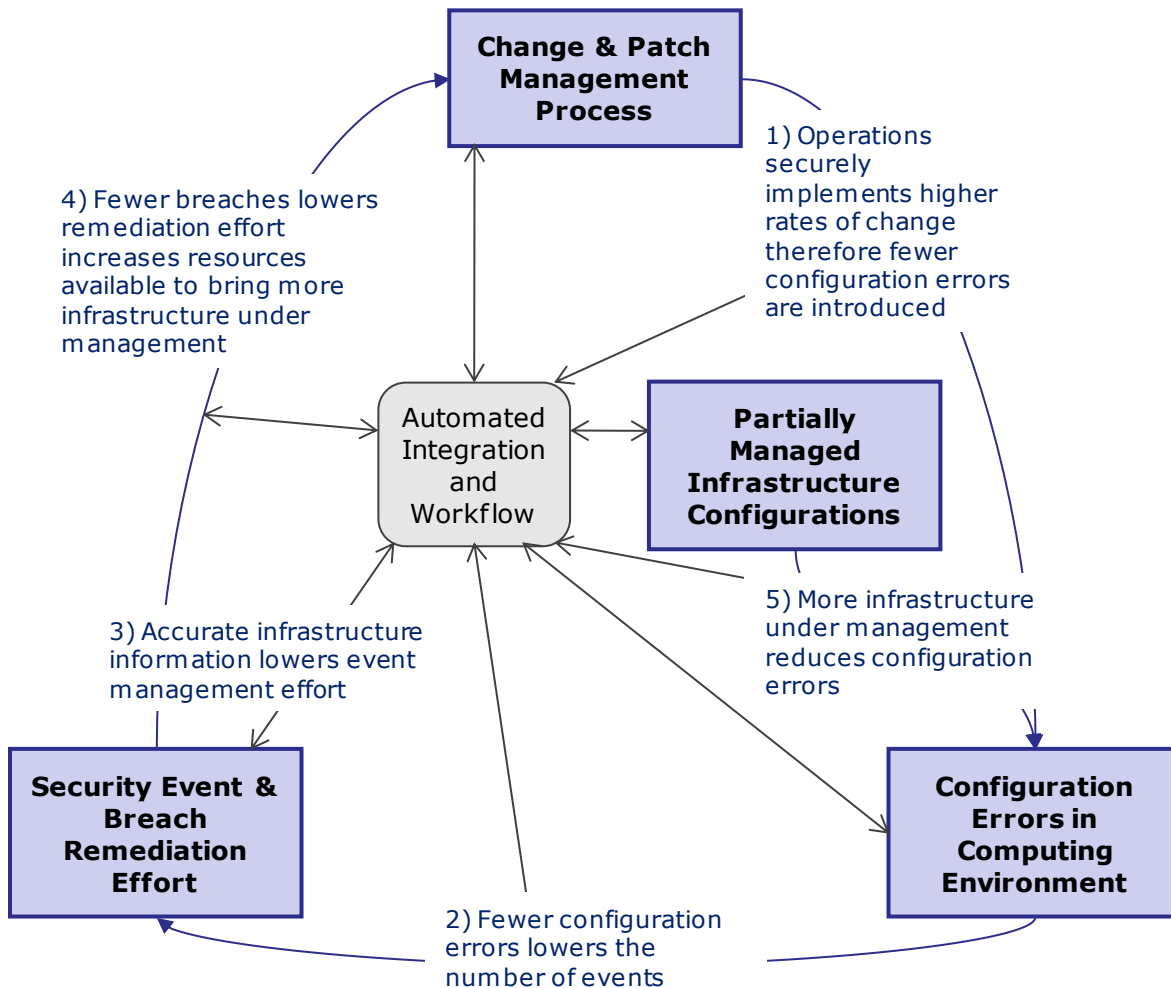
Those same case-studies outlined labor productivity gains achieved by operations teams:

- AgFirst⁵ was able to reduced PC reimaging time from 4 hours to 30 minutes
- State of Michigan⁶ reduced PC reimaging time from 2.5 hours to 15 minutes

What hasn’t been seen yet, and what our interviews and client experience reveals as a problem, is the inability to measure and communicate the benefits of security and operations processes working in concert. How much of AgFirst’s and State of Michigan’s reductions in security incidents were tied to operations’ improvements in reimaging times? What other improvements were achieved because of the move from reactive to proactive mode?

Some interviewees were able to directly link how benefits were recognized across operations and security silos. One CIO noted that when he joined the organization he was “putting out fires all the time” but by consolidating the security and operations responsibilities “we aren’t in that mode now, 55% of my time is spent on strategic planning, on understanding how to bring new technology in to make our employees more effective on the road because we need to find the balancing point between security and usability.” Another commented that once they started automating security policy checks for installing laptop software updates and upgrades, security-related firefighting dropped from a weekly occurrence down to 4-5 hours per month. Four interviewees specifically mentioned the amount of time lost (and recoverable) when different operations managers implemented the same security policy in different ways with different products. Figure 8 illustrates how the relationships and impacts can be traced and tracked.

Figure 8: Benefits across the cycle



The ability to trace and track the relationships between security, operations and business benefits will allow technical organizations to shift to an ROI-based discussion for security and operations investments. For example, if the security team found a way to automate security policy checking that could be readily embedded into an operations change management workflow. This creates a significant jump in operations productivity – with each administrator able to consistently and securely implement the changes without skipping steps.

Finally, the real benefit multiplier takes place when each deployment using that workflow results in fewer rollbacks and fewer subsequent patching or remediation efforts due to compliance audits or security events avoided. As a result, productivity increases for both the security team responding to the events and the operations team implementing the remediation. **The entire cycle now works to lower the total cost of business agility.** This means security and operations teams will have the resources to focus on what the business really needs – investigating emerging business risks and how to securely adopt new technologies to meet business goals.

Conclusion

Our interviews and research underscore a need to evolve from current approaches to security and operations tasks. Business computing and operations must have security-consciousness built into its DNA. Just like DNA, it is a complex structure of intertwining parts. Both operations and IT security have many interconnected tasks and processes that affect each other in complex ways.

A senior infrastructure manager at a law firm put it this way: “We needed a viable solution for enforcing workstation security policies.” The firm has over 7000 employees located in 29 offices worldwide. They found that only way to manage their far-flung infrastructure consistently, effectively and in a cost-efficient manner was to provide their IT operations team a solution that helped them automate configuration management while still permitting the security team to create new security-related configuration policies as needed.

References:

¹ [Symantec Internet Security Threat Report Volume XIV](#), April 2009

² [2009 Data Breach Investigations Report](#), Verizon Business RISK Team

³ [Managing IT in a Difficult Economy](#), Symantec March 2009

⁴ [Leveraging IT Controls to Improve IT Operating Performance](#), ITPI June 2008

⁵ AgFirst Farm Credit Bank, Business Value Analysis Study, October 2008, The Alchemy Solutions Group

⁶ State of Michigan, Business Value Analysis Study, April 2009, The Alchemy Solutions Group



White Paper

This white paper was sponsored by Symantec Software

This document is subject to copyright. No part of this publication may be reproduced by any method whatsoever without the prior written consent of Ptak Noel & Associates.

All trademarks are the property of their respective owners.

While every care has been taken during the preparation of this document to ensure accurate information, the publishers cannot accept responsibility for any errors or omissions. Hyperlinks included in this paper were available at publication time.

About Ptak, Noel & Associates LLC

We help IT organizations become “solution initiators” in using IT management technology to business problems. We do that by translating vendor strategy & deliverables into a business context that is communicable and actionable by the IT manager, and by helping our clients understand how other IT organizations are effectively implementing solutions with their business counterparts. Our customers recognize the meaningful breadth and objectivity of our research in IT management technology and process.

www.ptaknoelassociates.com

July 2009