



Global Knowledge®

Expert Reference Series of White Papers

# Tough Love: When IT Security Hurts Your Business

# Tough Love: When IT Security Hurts Your Business

Hank Marquis. FBCS CITP, Global Knowledge Practice Leader

---

## Introduction

As IT commoditization continues to increase audit and control activities, IT gets better at identifying and documenting the causes of significant outages. IT organizations are using ITSM (IT service management based on ITIL) to make the source of many IT failures clear, and they use Business Service Management (BSM) to understand what the customer impact might be for any changes proposed.

ITIL, and even more so BSM, is all about taking one's cue from the business and what is best for the enterprise, and creating processes that confirm business impacts before making any changes. Aligning with business means understanding the business and helping understand the ramifications of decisions.

In an increasing number of cases, these ITIL efforts show the source of the outage to be action from the security department, and the BSM processes show the impact to be devastating in some cases. Unfortunately, it seems as if, in many companies, security staffs do not take advantage of existing IT processes, nor do they understand the impact on the business of the systems they police.

It appears that ITIL and BSM concepts can help security departments make better decisions, too.

Generally, companies need security oversight for their information technology investments, services, and corporate systems. However, some security departments today are stand-alone groups of dedicated workers who "know what's best" and then go do it – with increasingly disastrous consequences for the business. Sometimes this is due to a corporate policy of separation – specifically keeping IT and security at a distance from each other.

One possible cause of the growing friction between IT and security is that many security departments are separate and unequal groups operating outside of IT that "do security to IT." This can distance security from day-to-day IT operations and precludes many interactions with ordinary IT staff, customers, users, and existing IT processes.

At best, the distance between the two entities can make security seem elitist; at worst, this results in major cost, quality, and regulatory liabilities for the business.

Based on my personal experience working with some of the leading information technology organizations in the United States to implement ITIL and BSM, here are three real-world examples to illustrate this burgeoning problem. Also presented are possible solutions for those now facing this serious, sensitive, and hard-to-address issue – an issue that needs to be addressed, however uncomfortable it may be.

## The Best of Intentions

At a hospital in New Hampshire, a well-meaning IT security practitioner decided that the passwords in use by healthcare workers were “weak” after he visited Microsoft’s website and used their free password “strength” checker.

He had the best of intentions – data privacy laws are tough. One of the regulations to which the hospital is subject is the Health Insurance Portability And Accountability Act Of 1996, or HIPAA. The maximum fine for a HIPAA breach is \$100 per violation and up to \$25,000 for all violations of an identical requirement or prohibition during a calendar year. But don’t think that the penalty is limited to this. Oregon’s Providence Health System agreed to pay more than \$95,000 in state fines and \$7 million to \$9 million in victim credit protection services relating to loss of patient information. And there can be jail time as well – an employee of a Seattle cancer center, Richard W. Gibson, earned the dubious distinction of being the first person sentenced to jail time for HIPAA violations.

To improve security and avoid such potential HIPAA violations, our erstwhile security practitioner decided to change all passwords to a “stronger” scheme of his own design. While he had the best of intentions, the problem was that the password scheme he came up with produced passwords “stronger” than required; so strong, in fact, that users could not remember them. Instead, users wrote them down on yellow sticky notes and stuck them to their computer monitors.

This single act by a security practitioner in order to prevent HIPAA violations set the stage for more potential HIPAA violations than the previous “weak” passwords allowed!

This could have been prevented if he had worked with business customers to establish any security requirements beyond the baseline required (in this case) of HIPAA. Then, after establishing a baseline of security per HIPAA regulations, he should have taken his cue for any additional appetite for security from the business – the customers and users of the systems. This story had a more or less happy ending as this is just what he did.

He should not have made arbitrary decisions regarding security enhancements. By negotiating with customers, he could have determined how much security the business was willing to risk, and more importantly, how much additional security the customer needed, if any.

As in this example, these types of mistakes can expose the organization to significant liabilities and losses beyond simple cash penalties and incarceration. Put another way, security practitioners don’t always “know what’s best” for their users, customers, or the business, and sometimes they get it wrong.

## Trumping IT

Another example of security gone awry with significant consequences is that of a major outsourcing service provider located in Ohio. The service provider's security department pushed a mandatory software update "patch" to a major customer application.

Security practitioners felt the patch was so important that they decided to skip testing and deploy the patch immediately – against the advice and over the warnings of IT staff and management who had very efficient ITIL Change and Release Management practices and procedures in place. IT had to acquiesce to security, because in this company, as in most, security department mandates trump.

As fate would have it, the patch went in, and the system went down. It seems that the application builders relied on the "undocumented feature" the security patch "fixes" in order to operate. While they tried to determine a solution, the system no longer represented a security risk – it was now a business risk, because customers couldn't use it. Since the service was not usable as contracted, the service provider could not rightfully charge for it, yet they needed to spend to support and restore the service. On top of everything, this flagship product, in use at a major retailing and credit organizations, was no longer operational, which had a dramatic impact on customers.

This example did not have a happy ending and reflects the worst-case scenario. The cost of playing this trump card extended beyond mere lost profits to include loss of credibility, market image, and goodwill. It also crossed into the area of corporate responsibility and shareholder value.

If the security department had worked within established IT processes instead of trumping IT with self-imposed timetables, the ITIL-based Change and Release Management activities already in production may well have discovered the flaw and developed an alternate solution.

## Dysfunctional Mandates

In New York City, at one of the world's leading financial management and advisory company's security department, analysts pen mandates based on flawed understandings of current applications. Example mandates include blocking certain network ports, applying certain directory permissions, and so on.

When these flawed mandates reach IT, system administrators have no choice but to modify them before applying in order for them to function at all. If they actually carried out the instructions as provided, entire applications would fail. Consider applying read-only access to a software configuration file that requires read/write access in order for an application to operate. As you can imagine, entire business processes come to a screeching halt when this happens, but happen it does.

Security analysts ill-informed about the structure and capabilities of the applications they police not only compromise the quality of their work, but also create tremendous, additional work for an already taxed IT department.

If security practitioners could engage with IT, these problems would quickly resolve. Sound Configuration Management based on ITIL could quickly identify this dependency, and BSM mappings would show the impact. But as in many security departments, this one follows a concept of separation – security and IT are separate by design.

## The Zen of IT and Security

The theme running through these examples is one of a critically important organization making decisions in an information vacuum, unaware of the systems they monitor and unwilling or unable to rely upon the people and processes they police.

While these acts can appear arrogant, more often than not they are born of ignorance, not malice. This ignorance arises from working in a department outside the auspices of day-to-day IT operations, being unaware of existing IT policies and processes, and taking cues from their own understanding of security versus working with the business to establish security requirements.

These security faux pas are not random, seldom-occurring events. These few simple examples illustrate a growing problem within the IT security world.

How very Zen that through acts seeking to improve security in order to prevent problems, security practitioners often create problems.

## Day of Reckoning for Security Departments

Why is this coming to a head now? The reason lies in the work done by IT to support the increased regulatory tracking and control required by information technology commoditization. While by no means perfect, the audit trails made possible by ITIL adoption and now appearing in many IT organizations highlight the causes of failures – as in the case of my examples. And, the adoption of BSM principles means it is easier for IT to understand and quantify the impact on the business of these failures.

Accelerating IT commoditization is breeding increasing regulation over IT. In order to conform to regulations such as HIPAA, Sarbanes-Oxley, and others, IT has had to amend its ways to clean up its act. They have chosen ITIL and BSM as the means to do so, and by implementing controlled, cross-functional processes they are seeing results. As a result, few still consider IT a collection of independent technical groups where each works in a vacuum with total disregard for other groups. Yet many security departments still operate under the old model, and many security practitioners continue to state the absolute requirement for a dedicated and separate security group outside of IT.

Within best-of-breed IT service management frameworks such as ITIL, security is an integral and critical part of every aspect of IT. As formal IT service management adoption accelerates, stand-alone security departments find themselves more and more at odds with how the business and the rest of IT think it should operate.

IT has had to integrate its “silos” into a cohesive team and has chosen ITIL and BSM to develop an end-to-end, customer-focused view. Similarly, perhaps security should no longer be a standalone group outside of IT, but rather integrated into and along with the other IT service management processes.

I’m not alone in this assessment. An article in CSO [*Chief Security Officer*] quotes Gene Kim, CTO of Tripwire and co-founder of the IT Process Institute, an independent research organization that exists to support the membership of IT audit, security, and operations professionals, as saying, “. . .What ITIL does so well is to show how security doesn’t live by itself; it lives within the overall IT operational context. . . A significant proportion of security-related Sarbanes-Oxley audit deficiencies relate to change control – yet for years, security practitioners have fought shy of the issue. . . the day of reckoning is here.”<sup>1</sup>

These are strong words from a globally recognized authority on security, audit, and IT. Kim was not predicting possible future events; he was describing actual current events.

Consider Thomson Financial (part of The Thomson Corp.), which began implementing formal IT service management several years ago, and now has a very different security organization as a result. According to Tim Mathias, vice president of IT security and CISO at Thomson Financial, security at Thomson Financial today is now a matrix function, with security responsibilities distributed around IT. “Having these [security] people actually embedded within the organization gives my team much greater visibility into what’s actually going on – more so than we could achieve otherwise,” says Mathias. “We’ve seen a significant shift of attitude within the various units: security is now seen as a business enabler rather than as a bunch of people who just say ‘no’.”<sup>1</sup>

Integrating security into IT operations clearly has benefits, and now that generally accepted IT practices like those in the ITIL are commonplace, it is easier to integrate security into day-to-day IT operational activities than ever before. Most IT departments already have processes in place to manage changes to the infrastructure, and security should leverage the work and investments made by IT to their benefit.

For example, explaining how changes to a company’s firewall might lead to security issues, Marcia Wilson, CEO at Wilson Secure, a company that provides network security assessments, describes how integrating security with formal Change and Configuration Management yields benefits. She says, “The solution for these two problems is to require Change Control approval for all firewall changes. The approval process must include someone at a high-level of authority.”<sup>2</sup>

She is basically describing the checks and balances that most IT organizations that have adopted generally accepted ITIL practices already include. Rather than handle security incidents as special cases, skipping important, business-impact reviews and analysis, it makes more sense to integrate security changes into the existing IT workflow. Sound, existing processes like those espoused by the kind of Change Management required by, for example, Sarbanes-Oxley, include oversight and escalations that take into account business impact and urgency. These existing IT processes can address security issues quickly while still taking the time to make sure security related changes introduce no inadvertent results.

Security can also gain important knowledge from an understanding of IT operations, something many security departments simply don't possess. Marcus J. Ranum, world-renowned expert on security system design and implementation says, "It's ridiculous to think that you can secure something that you don't understand, but a lot of [security] practitioners try. I've seen sites spend hundreds of thousands of dollars trying to deploy IDS [Intrusion Detection Systems] or whatever, but they never bothered to learn what their network is being used for to begin with."<sup>2</sup>

## Time for Change

To be fair, security practitioners often find themselves in difficult situations. If they don't act swiftly enough, the results can be bad. As shown in this article, if they act too swiftly, the results may also be bad.

Fundamentally, security decisions are judgment calls made by individuals following a process. However, the more sources of information and the richer the understanding of tolerable risks, the better the judgment will be.

To meet the burdens of regulatory audits for program and change management companies have invested millions to transform their IT operations with ITIL and BSM. It is time to reap the benefits of these investments by integrating security into day-to-day IT operations and aligning both IT and security with business priorities. Such a move can improve security decision-making dramatically in at least three areas:

- Understanding customer risk tolerance and security requirements
- Managing security-related changes to the infrastructure through existing IT processes
- Gaining awareness of how IT infrastructure, systems, and applications actually function by participating in day-to-day IT operational activities

The new IT emerging in the wake of IT commoditization is coming as a real shock to many security professionals. IT has migrated away from its old role as technology gatekeeper to a more business-driven and customer-supportive role. So, too, must security change. Security must evolve from a stand-alone department acting as gatekeeper to just another normal, but important, aspect of day-to-day operations within IT.

Experts in the security field often cite that the leading security mistake made by companies is not integrating security awareness into employee education and workplaces, and that a security awareness program can be one of the most effective and least expensive steps a company can take toward protecting its information resources.

It is beginning to appear that another security mistake made by companies is not integrating their security with ITIL and BSM processes. Perhaps leveraging the ITIL and BSM process and control investments made by companies can be another effective and inexpensive step a company can take toward protecting its information resources.

## Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

[ITIL v3 Foundation Exam Prep Boot Camp](#)

[How to Get Started with ITIL](#)

[How to Create an ITIL Service Desk and Incident Management Process](#)

[How to Measure and Justify IT Services](#)

For more information or to register, visit [www.globalknowledge.com](http://www.globalknowledge.com) or call **1-800-COURSES** to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

## About the Author

Hank holds advanced certification in ITIL, ISO-20000, COBIT, Six Sigma, and Project Management. He is a senior member of the American Society for Quality, and has over 25 years of IT experience managing, organizing and optimizing IT infrastructures and organizations. He has extensive experience helping IT executives implement IT governance and operational frameworks. He held operational management positions at MCI, was CIO at e-commerce financial services provider Celexis, served as VP of Marketing and CTO at management software company Opticom and rose to senior management at Compuware. Hank has helped dozens of companies develop and implement ITSM best practices. He currently leads the Business Service Management practice area for Global Knowledge, and you can contact him at [hank.marquis@globalknowledge.com](mailto:hank.marquis@globalknowledge.com).

## References

- <sup>1</sup> Wheatley, M. "The Skinny on ITIL." CSO Online. 6 January, 2006. IDG Communications, 2009. [http://www.cso.com.au/article/158369/skinny\\_itsm?fp=8&fpid=4](http://www.cso.com.au/article/158369/skinny_itsm?fp=8&fpid=4)
- <sup>2</sup> Schweitzer, D., Sc.D. "Security Faux Pas." 15 October, 2004. Vol. 26 Issue 42. Page 8. Sandhills Publishing, 2009. <http://www.processor.com/editorial/article.asp?article=articles%2Fp2642%2F21p42%2F21p42.asp>