Global Information Assurance Certification Paper

Building a Security Practice within a Mixed Product-R&D and Managed-Service Business

GSLC Gold Certification

Author: Evan Scheessele, evan@swics.com

Adviser: Jim Purcell

Submitted: June 30th 2007

Outline

1. Introduction

.....

3

2. Virtu-Publishing Corp.....…….... 4

3. Strategic Tension: Embrace it or be Irrelevant…. 5

4. Know Thy Technology First…….. 7

5. Alignment with Senior Management…….. 10

6. Know Thy Customer……. 14

7. Style of a Security Leader…… 16

8. Concluding Perspectives…….. 20

9. References……. 23

1. Introduction

Information-rich technology businesses offer their security staff more challenges today than ever. Where business is driven by active technology development and technology is delivered to customers in the form of a managed-service, security takes on a scope that impacts the business's fundamentals. This paper addresses the challenges and best practices related to delivering overall security (here referred to as a security practice) within a complex business. The template business examined in this paper hosts both highly complex networked-product R&D and 24/7 outsourced managed services.

Where a business is both actively developing technology and introducing new technologies to the market as a managed-service, both sides of the business - development and delivery - have unique security perspectives and requirements. Building up both sides, in simultaneous coordination, is a particular challenge to a security leader, requiring strategic perspective and daily flexibility. Here we describe the individual challenges, how those challenges are necessarily related to greater business goals, and the necessity of coordinated security development. We also describe best practices for the coordinated construction of an integrated security practice, specific lessons learned, and overarching strategies for the future of such businesses.

2. Virtu-Publishing Corp

Our model for this paper is Virtu-Publishing Corp, a hypothetical start-up engineering and solutions company developing "Web 2.0"

applications for the emerging micro-publishing market. The core of Virtu-Publishing is its world-wide network of kiosks for authors and editors to upload and download manuscript drafts. The system depends on secure physical hardware (under constant revision), software running locally on the kiosks, network services, and centralized software in Virtu-Publishing headquarters. Each element presents its own security challenges, ranging from hardware design, to pure software to pure traditional IT. In a customer-facing consolidated sense the solution is sold as a managed-service, where for Virtu-Publishing's customers pay monthly service charges for access to the high-bandwidth network and certain unique features related to the publishing-industry. Unsurprisingly, Virtu-Publishing's hypothetical customers of 2007 have high expectations for security: especially regarding their unpublished manuscripts.

Virtu-Publishing Corp is consumed with challenging security work on two sides of a balance. There is both the work of further developing its technical solution, and the work of servicing its existing, paying customers. The development side of the business, Virtu-Publishing R&D, is immature, sprinting most of the time and changing priorities more often than an established business with proven product lines. As seems always to be the case with fledgling high-tech businesses, requirements and market direction are still in flux, so project consistency is mostly absent from the R&D side of the business.

Virtu-Publishing Operations is the department that is customer-facing, and accordingly runs the IT and networking to deliver the managed-service 'product' to the market. Given Virtu-Publishing R&D's

shifting priorities and inconsistent delivery of features, Operations must be especially nimble servicing customers and managing expectations. This tension between development and service leads into our first observation about security in the dynamic technical-plus-service industry. Mind and respect the business's realities.

3. Strategic Tension: Embrace it or be Irrelevant

The hybrid-business environment described above leads to this paper's first and most basic security leadership perspective to appreciate. It is that security may be important to the business, but it is likely no major department's first order of business. Unless security is a business's named primary objective, (and for Virtu-Publishing, like most technology business, it is not) then neither R&D nor operations is going to put major capital toward security practices. Development engineers, operations delivery teams, and even the business's executive management will be focused first on their core commitments. Those core commitments are typically growing revenue, reducing unnecessary costs, and managing investors' expectations. Security is typically appreciated but considered a second-order priority. Security has the especially difficult challenge here in a hybrid business in that R&D and operations both will consider it to be the other's responsibility to ensure security deliverables are accomplished. It is simply the nature of fast-moving teams and security that R&D will see security as processes and procedures that are to be delivered in the operation of the managed-service, and operations will expect that R&D will build a secure product from the beginning.

The objective of a savvy security manager in this reality is to embrace the natural tension between R&D and operations, and not impose an artificial structure on the business for the sake of security. Good security requires neither a refactoring of a business's organizational structures, nor an excessive imposition on any one department over another. The business's primary functional drivers are to develop new and competitive products, and to successfully deliver those products to its managed-service customers. As such, security is going to have to fit into both of these strategic silos of the business, not exist independently, attempting to get a practice up and running in a vacuum.

The key to adapting to an operations-versus-R&D dynamic of a small, dynamic technology business is to work within both spheres independently, fostering trust and managing expectations with each department's leaders, and when necessary participate in shuttle diplomacy. Security can sometimes be a simplifying concept, reducing business complexity to finite requirements. For example, a control must exist on the Virtu-Publishing network to detect unauthorized intrusions. Such a control will require infrastructure and process in Virtu-Publishing Operations, but also will dictate certain product-design considerations in Virtu-Publishing R&D, such as for registering network ports used in the applications.

An independent security leader needs support from both departments to build a successful practice, and only with strong partners on both sides of the business can the leader work out solutions to security problems requiring both technical and operational changes.

4. Know Thy Technology First

In Virtu-Publishing's hypothetical case, there are a variety of technologies in use to enable the novel distributed micro-publishing solution. Selections range from local and wide-area networking, various operating systems across kiosks and datacenter servers, middleware for hosting core business logic, databases, and various pieces of custom-written code for Virtu-Publishing's market-differentiating applications, leveraging likely several different programming languages for logic and presentation. An independent security leader within such a complex business needs as many tools at their disposal as possible in order to be successful. One powerful enabler is a thorough knowledge of the business's technologies.

Foremost, understanding the technology enables credibility and an ability to speak with immediacy to the issues from the point of view of the respective sides of the business. Without a solid working knowledge of the technology differentiating the business from competitors, the security manager might as well be considered integral to only the managed-service side of the overall business. And while a lot of good security can be delivered through traditional 'OpSec' processes and procedures in a business's operations, in a dynamic business like Virtu-Publishing there are too many additional variables to allow for short-sidedness.

Similarly, if security leadership's focus is too deep "in the code" the operations side is left at a deficit. Operations security requires diligence and the constant striking of a balance between effective security and "too much" security where the network or

infrastructure becomes unwieldy, unreliable or both. Knowledge of operations technologies allows for the necessary credibility to drive efficient operational security improvements and knowledge of where the most effective and affordable balance should be struck.

The security manager's objective should be to become a serviceable architect of the business's overall technology stack. This means working closely with R&D and operations leads to understand how the solutions are developed and the pieces integrated. Examples of good starting points are:

- What are the fundamental design requirements driving the architecture?
- What programming-languages are used for software development?
- How is software regression-tested, packaged and deployed?
- How many separate pieces of software comprise the various parts of the solution?
    - What might be the least-understood link?
- How are off-the-shelf components, both hardware and software, integrated into the solution?
- What operating system or firmware-characteristics do and pieces of "black box" off-the-shelf hardware present?
- What network protocols does the solution use to communicate internally?
- What kinds of internal logging does the solution provide?

Notice that none of the above is a security-specific question. Such inquiry helps lead to a deep understanding of how the business's core technology works, why it was designed a certain way, and how it is likely going to need to be handled by the operations team. These are kernels of knowledge that an overall security practice can align with for more effective communications and establishing dependable expectations.

Technical security knowledge sometimes can even be a requirement with regard to specialized customer requirements. For instance, if FIPS-140-2 certification is a customer expectation of the key cryptographic modules in a business's solutions, then the security manager will greatly benefit by understanding many of the intricacies of cryptography.

5. Alignment with Senior Management

As mentioned above, Virtu-Publishing's executive management is focused more on the numbers than on the hackers. This is not though a realization to confront, but rather an opportunity to make security matter to leaders using their own language. The key here is finding management's pain and showing security's return-on-investment (ROI).

Even in a small or start-up organization alignment with senior management can be challenging. The reason is probably not lack of accessibility, but rather the inherently different spheres of work and context. Security is inherently about technology (mostly) and business is mostly about finance - in practice the two fortes intersect only

occasionally. The solution is simply to span both sides of the business. A successful security manager in a hybrid business must work to be a trusted, if quiet, partner in the circles of business administration. It may sound like quaint advice, but the best way to know what is going on and stay aligned with the pulse of the business is to attend meetings. Inviting oneself is occasionally awkward, but if otherwise necessary, the exposure and passively-formed relationships by simply being present in the top conversations translates directly to access and respect.

The standard organizational best-practice for security managers continues to apply: if possible, especially in a complex, hybrid high-tech business, security should report to and tune-in to top-level business executives. In no better way can a security leader cultivate the strategic concept of the business' s security practice.

With access to and credibility from a business' s senior leaders, the security manager' s opportunity to grow an effective security practice comes from selling a vision of return-on-investment. Preparing a statement of security ROI is admittedly difficult, but necessary for effective investing in security controls. Security is nothing more to most executives than another technical investment. Buying servers enables one improvement, hiring developers facilitates another - investing in security simply delivers one more benefit. Nothing sells an investment to upper management better than articulating, in financial terms, the reward, or financial return. For broad security - the development and evolution of a whole business' s security practice - use rough ROI. Rough here does not mean dispensing with financial calculations, rather it means that everyone will agree it is

unreasonable to attempt to predict with precision what returns are possible. The point is simply that ROI is the right tool for security managers to justify security expenditures.

One side insight about security ROI is that some elements may be non-obvious but still worth including in the presentation to senior management. One is that peoples' time has value and may be accounted for. This goes both ways too: for instance in our Virtu-Publishing example, on the in the investment side the security manager may rightly want to recognize R&D developers' time redirected to code reviews, or in operations the time for staff to invest in review network log files. On the return side though are opportunities for time to be saved: for instance a potential drop in time to develop bug fixes due to better initial code, or time saves reviewing firewall logs due to automated consolidation and correlation services. Staff's time still matters in small businesses, where headcount reduction due to automation may not be anticipated.

Another non-obvious return on security investment worth capturing is value to marketing and sales. For some executives the linkages are easily identified, but to the security manager it may be a challenge to incorporate the kind of 'spin' to relate under-the-covers security investments to product features or other soft customer benefits. Still, the argument is worth investigating, especially in complex hybrid businesses where elements of security have a meaning across the entire solution.

A final insight for establishing effective alignment with senior business leaders is to hook security into business planning by finding

the 'pain' of each management chain. This idea is somewhat stylistic, but it means identifying, for each of the business' s verticals, the executive' s key drivers or challenges to success - then cultivating an understanding of how some part of the security practice directly relates to and supports the vertical' s goals. The alternative is that security may be for each division leader just one more thing below their personal priority line.

6. Know Thy Customers

Such as with the Virtu-Publishing service, where the 'product' is both a tangible experience and a managed-service, knowledge of customers' expectations for security is critical to effectively prioritizing security investments. Ivory-tower engineering of any complex solution' s security controls and features is not as helpful as starting with an understanding of the market and what managed-service customers already expect. For instance (although this likely would not be the case for Virtu-Publishing) if Common Criteria certification was a standard customer requirement, then early design of the business' s security practice would reflect it. [Similarly, 'Know thy Partners' may also be relevant. If for instance Virtu-Publishing' s kiosks were to support credit-card transactions, then PCI compliance would be an obvious requirement.]

Also a view of the future - what customers know is coming down the road in terms of emerging technologies or competitors' offerings - will assist in guiding priorities. Customers neither live entirely in a

vacuum, nor perpetually in the 'now' - especially where a managed-service is at play and commitments to monthly payments are under consideration. Savvy customers will place a company's offering onto their own perceived continuum of poor to good security, or existing, present security stretching toward way-off "coming soon" security. Such considerations may sound more akin to marketing than security management, but where security direction plays both into product design and details of operations, security emerges visible enough to demand consideration of the customer's likely response.

The specific practice of risk assessment plays an additional and somewhat novel role in aligning security priorities with customers' needs. Risk assessment is often seen as an internal process, for understanding an organization's security gaps, but in the context of a managed service risk assessments are additionally valuable if cast to include customers' perceptions of threats and impacts to the utility they derive from the service. Well-regarded risk assessment methodologies such as CERT's OCTAVE are standardized and relatively objective in their approach, leading to meaningful internal and customer-driven inputs into security practice prioritization.

Taking risk assessment and leveraging its findings into security planning, action and delivery is primarily an operations duty. Although some aspects of the security practice inevitably dictate certain elements of product design, (for instance physical security of a Virtu-Publishing kiosk or user authentication in kiosk software) mostly the execution of the practice is consumed in the delivery of managed service. Here standards like ISO/IEC 27001:2005 have immense structural

value, establishing a tactical frame of reference for operations security, and also great value in explaining security defense-in-depth to customers. ISO-27001 is an objective standard for overall organizational security, which along with its established credibility over years of refinement allows strong assertions to customers about exactly how secure is the managed service.

7. Style of a Security Leader

The concept of style may at first seem mostly irrelevant to a discussion of building a security practice. Beyond traditional approaches to security practice such as enterprise security governance, style is part of the effective leader's toolkit of intangibles that help make the difference between delivering adequate security and being positively market differentiating. For instance, Virtu-Publishing is a hip, fast-moving and exciting company of young, risk-taking talent. One challenge for its security leader is to accommodate the business's progressive culture and not falling into security's traditional (stereotypical) "No" approach.

The best starting place for refining how a security manager can be an effective leader is to partner deeply: one security manager cannot do it all by him or herself. One goal should be to grow responsible tactical leaders for elements of the security practice. Define scope for these domain leads and actively seek to win management buy-in for each delegated individuals' security responsibilities. Closely related is the importance of building ownership and responsibility within the

direct or indirect security 'staff'. If nothing else, the security manager should sponsor an informal - but recognized - forum for the business's security planning, investigations, development and hot topics. Hybrid businesses are complex business - everyone is R&D and operations may rarely have opportunity to cross collaborate or share notes about security challenges. For certain fast-moving businesses often lack low-stress forums for clarifying "dumb questions" and synchronizing knowledge across domains. A lot is inevitably being asked of everyone, even those who never thought of security before, and an open forum allows for greater awareness and personal investment.

There are two corollaries to the above structural thoughts. The first is simply that clear and ample communication is more effective than an air of secrecy. Good security is built on the technologies of keeping secrets, but the practice of business security depends much more on knowledge of process and procedures, aligned expectations and an ability to react rapidly. Open communication as a standard way of operating a security practice works better than operating security in its own closed vault. Communicate effectively and frequently. The other concept related to security organizations is that *morale matters*. Security in personal practice, say with developers performing code reviews, or network engineers configuring access control lists, is often dependent on trust. Where relationships are strong and employees feel rightly empowered, then commitment to security practices follow. Morale is the obvious but rarely considered root of quality, consistent performance. In this way the security practice is no different than other skill practices in business, but it bears repeating. Accordingly, security is in many facets a complicated field, and mistakes are made.

When mistakes are identified with a 'spin' toward learning lessons and improving the core practice, staff typically grows more dependable and independent. In never serves to over generalize, but in security as in other skill fields, encouragement and education build morale far more than admonitions. In other words, be practical about non-disastrous mistakes, and seek continuous improvement.

In working across functional groups, between Virtu-Publishing R&D and Operations for instance, intentional introduction of one group's themes into the other's context builds better understanding. For instance, use knowledge from a business's operations side, such as account-management, to educate R&D about what *really* matters to customers. (Or at least what paying customers say matters to them.) In the same way, use R&D depth of experience and specialized details to arm operations with knowledge of new tools and technology. Similarly, operations staff can better see and appreciate how operations will evolve by knowing the R&D roadmaps for security improvements, and operations attention to quality language and metrics for security can better arm R&D engineers to understand the implications of otherwise arbitrary design decisions.

"That which is measured gets done" is a mantra in many management circles, and it remains a valuable stylistic tool for security managers. Most often, good security is impossible to verify: one cannot easily measure, nor especially sell to upper management, the absence of loss of business. Therefore, meaningful positive metrics are critical for communications and continuous improvements to practices. Logs exist to be reviewed for exceptions, alarms to be responded to in

some manner, and statistics to be compared against expected baselines. These are basic expectations that a security manager has to continuously sell into an organization to reap the benefits of the knowledge of the performance of a security practice. Otherwise the security manager must wait for incidents and disasters to prove the worth of the practice, by which time heroics and tremendous risk to the business are more likely than a clean response and resolution.

Finally, specifically for developers, an important stylistic consideration is to provide consistent information-security advice and guidelines. The vast majority of developers are not security savvy outside of narrow software domains, although contemporary trends, such as SANS's Secure Programming Skills Assessment are starting to improve this position. The root goal of software development security in hybrid-business is to keep one's chances of exploit-free code high and receive prioritized security features on schedule with primary marketing-driven features. Mostly, developers are motivated by delivering functionality, performance, elegance, and code that is bug free. The key here is that even the best developers need consistent requirements to reliably delivery good security in code. Security cannot simply be mandated. Hard, objective requirements are more easily digested into software development lifecycles, and more immediately measured. Also, consistent, measurable security objectives, allow a consistent story from design to delivery for customer communications and marketing collateral, and even those in-depth customer conversations that inevitably precede major managed-service deals.

8. Concluding Perspective

Building a security practice amid the extraordinary chaos of an innovative high-tech managed-service business takes attention to detail, patience and good people. Mostly, good people. Effective and flexible security practices come only from an accumulation of many individual efforts and contributions. Still, in the end such accomplishments may be overshadowed by greater business pressures, market shifts or business change. Risk seems to persist outside of the security domain, regardless of how well a security manager implements a risk mitigation plan. Regardless of such external factors though, success will be dependent on the efforts and commitment of people, and these thoughts reflect on that theme.

Grass-roots security awareness is more valuable than training. This statement is not to say that training is inappropriate: indeed if credible security training is available, affordable and applicable it should be pursued across the breadth of the business. Still, a grass-root approach to the business's necessary themes of its security practice costs little and returns across many domains. Grass-root education means making approachable themes of security be an every-day pat of doing business - letting security be soaked up by the personnel and processes that make up the business's entirety. Grass-roots also means letting others take individual lead of security domains, letting security leadership develop in multiple locations, in effect becoming fault-tolerant. This idea is not immediately actionable, but it is a goal and a frame of reference for considering whether a security practice is maturing with a business.

Finally, an old management maxim is to “stroke what works”, that is, seek to use positive reinforcement with staff. Management styles vary of course, but security is not black-and-white, and often the right course is not evident before the fact. Mistakes do get made, and in business, if a security practice is built with checks and oversight, usually security mistakes do not lead to disasters. Generally, reinforcing lessons-learned and rewarding constructive efforts are more efficient than punishing or replacing those who make mistakes. This is true too in the security domain, and is especially relevant in hybrid-business security due to the higher replacement cost for talented engineers in terms of dollars and time to bring someone new up to speed. Security in high-tech is complicated and a tough balance to strike: when the security team’s efforts hit the business’s mark for security, recognition and approval set a long-lasting tone. Reward good security contributions. Nothing breeds quality efforts in security work better than recognition and reward for efforts well done.

References

National Institute of Standards and Technology (2007). *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*. Retrieved June 30, 2007, from http://csrc.nist.gov/cryptval/140-2.htm.

Berinato, S. (2002). Calculated Risk - Guide to determining security ROI. *CSO: The Resource for Security Experts, 5*. Retrieved June 30, 2007 from http://www.csoonline.com/read/120902/calculate.html.

Brightsight (2007). *Common Criteria*. Retrieved June 30, 2007, from http://www.commoncriteriaportal.org/.

PCI Security Standards Council, LLC (2007). *Home - PCI Security Standards Council*. Retrieved June 30, 2007 from https://www.pcisecuritystandards.org/index.htm.

Carnegie Mellon University (2007). *OCTAVE Method Implementation Guide*. Retrieved June 30, 2007 from http://www.cert.org/octave/.

International Standards Organization (2005). *Information technology - Security techniques - Information security management systems - Requirements*. Retrieved June 30, 2007 from http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103&ICS1=35&ICS2=40.

Wikipedia Foundation, Inc. (2007). *Defense in depth*. Retrieved June 30,

2007

from http://en.wikipedia.org/wiki/Defense_in_depth.

Carnegie Mellon University (2007). *Governing for Enterprise Security*. Retrieved

June 30, 2007 from http://www.cert.org/governance/.

SANS Institute (2007). SANS Software Security Institute. Retrieved June 30,

2007 from http://www.sans-ssi.org/.