

Key Information Security Trends for 2009

By Jonathan Gossels & Philip Cox – ISSA member, Sacramento Valley, USA chapter

A look at information security trends from cloud computing and virtualization to compliance and the changing role of security departments.

When we look back at 2008, we see the establishment of virtualization as a foundation for many datacenters and increased awareness of compliance requirements spurred by an increase in compliance enforcement. As with other years, high profile security breaches dot the past year, but more on the mind is how to weather the financial storm that looms for the upcoming year. While we cannot answer the financial storm question, this article attempts to give a glimpse into the critical trends we see occurring in 2009.

The cloud

When you look to the future, for 2009 you see a haze which is better known as "The Cloud." Cloud computing is poised to revolutionize IT infrastructure, architecture, and operations. The buzz around the technology is undeniable, but the buzz can have a sting to it – from a security perspective. Cloud computing offers some fabulous technological and cost-saving benefits. What if you no longer had to worry about capital expenditures for your data center? What if you did not have to worry about backups, fault tolerance, managing hardware, or software licenses? How much time, effort, and cost savings could you realize? It would be a dream for most CIOs and IT managers, it just makes sense. Except for the most mission-critical applications, it is easy to see the attractiveness of having no data center, no hardware costs, and a vastly reduced IT staff. If anyone is skeptical of the business proposition, consider that Amazon is closing in on 500,000 developers using its cloud business.

However, this world of bliss does have two significant drawbacks: accountability and security. With the cloud, you do not control/own any of the hardware; that is part of the ben-

efit of cloud computing, but it means someone else does. So now you have taken some level of accountability and a chunk of security responsibility and transferred it to another entity. This means an increased risk for your company or organization which must be mitigated in some manner. From where we sit, the only avenue for this risk mitigation is contractual, and the current SLA/contracts typical of most cloud providers do not provide adequate coverage for the increased risks involved. Thus, while the cloud has great promise, there are security risks that MUST be mitigated in some manner. As with all technology, organizations must proceed with caution, understanding that when something seems too good to be true, it usually is. The key, of course, is selecting a cloud computing vendor that has built its systems, practices, and controls in strict conformance with pertinent standards, as well as ensuring contracts provide adequate protection. The issues of application integration, privacy, compliance, and security are huge and only simplistically understood at this time; do not look for easy answers any time soon. All of us will be wrestling with these issues for years to come.

Virtualization

For those who are not enthralled with the cloud, or who cannot use it because of the associated risk, the core technology of the cloud is available for you to use directly – virtualization. The expansion of virtualization technology is undeniable. Even relatively conservative organizations have aggressively adopted virtualization to realize the promise of reducing hardware, real estate, and utility costs. What began as an effort for an enterprise to transform 1000 servers into 100 servers each supporting 10 virtual systems does not end there. The move afoot among the various virtualization vendors is to get a virtual toe hold in each architectural computing layer

as evidenced by virtualized applications and desktops. What started as a data center efficiency effort is turning into an all out enterprise streamlining (and yes, centralization) initiative for many organizations.

We have all seen this type of central computing architecture with remote dumb terminals many times before (main frames, Sun diskless workstations, NEC X-Terminals, etc.), but it is the technology advances in the "motion" (e.g., VMotion, XenMotion, etc.) part of the story underlying virtual infrastructure that is so compelling. The cost-effective combination of hardware and virtualization software technology allows relatively seamless failover and high availability. This will encourage CIOs to move a large portion of their environments into the virtual world in the coming years. It will just make sense economically and functionally.

When companies bring virtualization in-house, they avoid the responsibility issues with the cloud and to some extent the security issues (at least the risk of another organization having access to their data). However, they have the added risk associated with a technology they may not understand. Many of the current virtualization solutions have design security problems (i.e., plaintext communications) that can be used to compromise the infrastructure, and if you do not understand that, you can design an environment that puts you at increased risk when compared to a traditional environment. More than ever, security has to be an up-front consideration in designing a virtual environment, and each virtualization technology has its own set of security issues that must be addressed.

Compliance drives the security agenda

For many organizations, the security agenda is now set by outside compliance requirements. Those requirements typically stem from a combination of regulatory, contractual, and demonstrative business needs.

HIPAA compliance

Many companies are feeling the pinch of regulatory and contractual requirements. In past years, organizations handling electronic protected health information (EPHI) felt that they could pay lip service to the requirements as very few audits were being conducted. The lack of enforcement has a trickle down effect from covered entities to service providers and the whole industry appeared to treat compliance as an option. Some well-publicized audits have led to more scrutiny by Health and Human Services and that has led health organizations and service providers to look more closely at their compliance state. The trouble with HIPAA (like most regulations) is that there are many ways to interpret the rules and there is very little guidance regarding best practice. Organizations have had good success in solving these problems by using the ISO 27002 code of practice to establish metrics and practices to meet the intent of the regulation. The result is a security and compliance program that fits the organization's risk profile and can stand the test of an auditor's scrutiny.

PCI compliance

The Payment Card Industry Data Security Standard states that all organizations that store, transmit, or process payment card data are required to comply with its requirements. This statement is especially meaningful to merchants, service providers, merchant banks, and card issuers. However, many organizations are exposed to or store payment card information but do not fit neatly into one of PCI's defined categories. The struggle for these organizations has been to determine whether compliance is necessary, whether non-compliance is an option, what the risk associated with non-compliance is, and what compliance actually means in their business context. As in so many areas of security and compliance, the answer lies in assessing business risk with a clear understanding of PCI requirements. The challenge is to determine a path that mitigates real risk and achieves compliance where necessary. Expect better definition of business classes in PCI's future, but until then, all organizations will need to decide for themselves or with the help of an expert partner how to practically achieve and maintain compliance.

To SAS-70 or not to SAS-70

The financial industry continues to rely on SAS-70 audits for proof of partner security practices. These assessments have the potential to provide real value, but too often they do not address the security requirements organizations care about. In performing security reviews of a partner organization, it is not unusual to hear claims of "SAS-70 compliance" or that the assessment is unnecessary in the face of an existing SAS-70 audit. Typically the SAS-70 has been designed to highlight the organization's strengths and deals only indirectly with security. SAS-70 reports can yield useful information about business practices, operations, and security, but they are no substitute for an in-depth security assessment that focuses on the business needs of the consuming organization. Unfortunately, many companies fail to grasp this fact.

Changing role of security departments

Another trend to look for is the evolution of security departments away from operations and toward technology thought leadership, policy development, verification activities like application vulnerability testing, and enforcement. With the exception of security operation centers at very large companies, over and over security hands-on activities are being pushed into lines of business or other IT operations groups. In stark contrast, two growing areas of responsibility are the management of partner security and communication of the enterprise's security program to prospective customers and other third parties.

Increasing focus on partner security

In 2009, look for increasing depth and rigor of the security assessment of business partners and a corresponding increase in the resulting requirements. While it has been customary for organizations to allow relatively broad access to sensitive

production data by production support personnel, expect requirements for tightened access controls, increased monitoring, and better auditing controls. The financial community, in particular, is beginning a cultural change by requiring partners to implement controls that meet or exceed their in-house controls.

Inconsistent long-term partner management

Inconsistencies are prevalent in the long-term management of partner security. While the best organizations take a life-cycle approach to managing their service providers by conducting periodic reviews, requiring notification when business or technology requirements dictate, and conducting risk assessments of the service and relationship, many use a “set and forget” approach with their partners. It is important to establish and maintain partner management programs; such programs are required in virtually every security standard or regulation. However, a majority of organizations are not yet paying adequate attention to what may represent both operational and regulatory risks.

Threats are everywhere

It is not unreasonable to expect that most new web applications would be secure, but they are not:

- Unauthorized rogue users should not be able to access data intended only for authorized users
- Authorized users should not be able to perform inappropriate actions on their own accounts
- Users should not be able to obtain any information about the accounts of other users
- Users should not be able to perform any actions on the accounts of other users

Most web applications are rife with easily exploitable problems, mostly caused by the same basic mistakes (e.g., failure to validate input).

There appears to be three reasons why web applications are not getting better: in today’s extreme time-to-market-driven development process, security requirements are rarely formalized, security is often ignored at the design phase, and developers receive inadequate training in secure coding practices.

Web applications are not the only culprit. Browsers, plug-ins, infrastructure components, and desktop applications can all put companies at risk of external attackers exploiting weaknesses inside a company’s hardened perimeter. The first step is to recognize the threat and take vulnerability management across the enterprise seriously. The best organizations are proactively assessing the threats associated with external web applications. Product solutions are evolving that address both directly attacking web applications and various forms of data leakage. This is a space to watch closely in the coming year.

Plug and play

Another sweeping trend is plug-and-play security. Since 2007 the industry has been swamped with security appliances that perform useful functions and require minimal skill to install and manage. Examples include devices that ensure that only healthy and up-to-date computers can connect to a network, identity enforcement, policy-based network access control, malware filtering, email security, bandwidth management, secure remote access, and even SSL traffic inspection. Looking at nominees for the *Rookie of the Year* award category for a leading security magazine, many of the candidate companies offer security appliances of one type or another. In this space, “set and forget” is exactly what makes the appliance approach so attractive – low ongoing costs.

The demand for this technology is fueled by the complexity of monitoring the state of security in the enterprise. More security systems are being integrated with one another. For example, identity systems and network monitoring systems are showing not only that connections are being made and packets are being sent, but by whom.

Conclusion

2009 will be a year of making it on the “skinny.” Budgets will be tight, but we’ll still need to get the job done. Regulatory compliance will be mandated more and more, and the use of virtualization to reduce costs will make inroads in many traditional datacenters. Keeping things secure will be an ever daunting task, and many will seek external expertise to augment their internal staff. Those who have established an efficient system, will reap the rewards, while others will find the ad-hoc method of system security will be nearly impossible to maintain in the coming year.

About the Authors

Jonathan G. Gossels, ISACA/CISM, president and CEO of SystemExperts, a consulting firm specializing in computer and network security and compliance, plays an active, hands-on role advising clients in compliance, technology strategies, managing complex programs, and building effective security organizations. Jonathan brings a business focus to this work, balancing all technical initiatives with business requirements and impact. He can be reached at jon.gossels@systemexperts.com.



Phillip C. Cox, CISSP, PCI QSA, CISM, NSA IAM/IEM, is a principle consultant with SystemExperts. He is an industry-recognized consultant, author, and lecturer with an extensive track record of hands-on accomplishment. For the past several years, Phil's technical focus has been on Microsoft technology, in particular, security issues related to UNIX-Windows heterogeneous environments. He may be reached at <mailto:phil.cox@systemexperts.com>.

