Information Security

A report from the battlefield

By Robert Younce

Industry Trends

- *Frameworks* are becoming the trend in all industries to stabilize the risks of informal IT and security operations
- While frameworks have been great in outlining security requirements, their adoption mainly by IT lack the effective oversight required to be successfully implemented and sustained.
- In addition, the influence of IT, business and security on corporate objectives are not cohesive with one another until very late in these adoptions, if at all. This negatively impacts the capabilities and effectiveness of all three independent objectives.
- Overall, many companies lack the maturity required to be successful in many of the basics of the framework. This is not industry specific either, effective use of frameworks is a major gap primarily because the processes and technology are expensive and complex.

Industry Trends Continued

- *Security* is an organizational objective and the security functions, such as breach management, should no longer be limited to just IT, it should be operated by the COO or similar role where risk and impacts cannot be influenced by competing goals and support for security function is optimal.
- With all of the breaches that have been occurring, security can no longer successfully protect organizations sensitive systems and information, unless it has more prominence in the environment/organization.
- It has also become an agenda item for most Board of Directors which is driving framework adoption. Security should not be centric to technology either, it should also influence business operations, mergers and acquisitions, and should be considered in every other facet of the business.
- In many instances security has been tightly interwoven with the CIO who will always have competing objectives. While conceptually, it makes sense given the technology requirements, it can be heavily influenced by the behavior and personality of that CIO role

Industry Trends Continued

- *Metrics* are the easiest way to represent how technologies and processes work in the environment and in many cases those metrics do not describe the real security effectiveness of the environment.
- This means security is not being represented clearly to leadership. Many metrics that are measureable to the leadership end up being inconsequential data that do not represent how the environment is really operating.
- It appears more of a show of how current technology is working, but not how Data Loss Prevention tools are finding credit cards or social security numbers being discovered or leaving the environment.
- Metrics should represent operating and system events.

Industry Trends Continued

- *Security operations teams* are too small to handle a fully functioning security environment.
- This is not directed at IT or business, this is a reality of having the bandwidth to understand the full environment (security control, audit control, risk and business, etc.), design and sustain operational requirements, and then successfully oversee and monitor throughout all IT and security processes.
- Control technologies are too complicated for a small team to manage and should be spread throughout the environment or be outsourced which would add additional complexities.
- This requires proper process designs, accountability by teams, and more.

Industry Trends Continued

- *Secure Web/Internet* is still a major problem in every environment.
- There are not enough teams in place to successfully secure web development through-out most industries, otherwise web application firewalls would not be as necessary as they are.
- Although static and dynamic web application vulnerability scanning are not required, it could be leveraged to reduce simple errors and overall coding improvement.

Industry Trends Continued

- *Communications channels* that exist between IT and business are starting to become more formal and understood.
- With today's business leaders being more technology savvy there is more ability to achieve objectives outside of IT.
- This speaks volumes to the critical fact that security cannot be limited to IT.
- In the more effective environments, a key individual was in place to help keep all parties up to date with what was occurring in the environment.

Industry Trends Continued

- *Integrating security technologies* in the environment has been a serious challenge and problem for long time.
- In addition to the integration, the planning required to sustain the technology by the staff is woefully underestimated.
- IT is hiring teams to operate these expensive security technologies for themselves when in many instances business operations may be able to leverage similar technology.
- Overall, security is left to an understaffed team without the required knowledge to effectively manage a single technology, not to mention multiple disparate devices with a high technology to staffer ratio.
- Without an integration plan and vision, many technologies die on the vines after hundreds of thousands of dollars are invested.
- In most instances security technology is brought in to address a control gap and are not designed with workflows for IT and business to effectively handle its usage. In addition, in many instances the workflows themselves need a business operator and an IT operator to be successful with the tool.

Industry Trends Continued

- *Threat intelligence, analysis and response capabilities* are a major focus in an effort to prevent breaches, minimize technology exposures and make sense of smaller event data sets.
- Until all company event data is communally submitted to a private cloud with all other companies where scientific analysis can be applied, threat intelligence will improve slowly.

Industry Trends Continued

- *Remediation management* is an up and coming branch of a tactical IT team used ensure issues can be resolved effectively and timely.
- This is not simply vulnerability scanning, but also addresses audit / regulatory compliance issues, business events, threats, and issues identified during risk assessments, etc.
- An effective group can make managing and responding to issues more aligned and controlled to limit repetitive issues from being reported to business and IT.
- Remediation management should be part of the company's overall governance structure to ensure transparency, and prioritization of remediation.

Industry Trends Continued

- *The knowledge of where critical data exists* (modified, stored and moves) is almost always incomplete or informal.
- An environment where this is known and understood, has much more effective processes and controls.
- The ability to effectively perform security functions and respond to appropriate events in the environment is severely hindered by a limited knowledge of where data exists in an environment.
- It can also impact budgets by overspending on technology be may be unnecessary. In many instances, though, you still want to have layers of controls to management threats throughout the environment.

Industry Trends Recapping

- *frameworks are helping*
- *security is not just an IT centric issue*
- *metrics are not where they should be*
- *security teams are siloed*
- *web security is still maturing*
- *communication is still a basic gap*
- *technology integration is weak*
- *threat analysis is gaining momentum*
- *Minimal or decentralized remediation management*
- *Minimal understanding of critical data flow diagrams and storage repositories*

Is your head spinning yet?

- Overall these risk areas have not changed in many years, only the potential attack methods and mechanisms to identify them.
- The action plan to resolve these concepts and concerns stem from the ability of organization leaders to know what their capabilities and maturity are in these areas and how transparent the effectiveness of security is being portrayed.

Questions?