

2009 Security: Where do you stand?

Needless to say, 2008 brought all of us some serious challenges—with ramifications that will carry forward beyond 2009. The bail-outs, fraud, bank failures, ponzi schemes and identity thefts of 2008 will be followed by sweeping new regulation and increased governmental oversight.

Beyond obvious regulatory requirements, information security now plays a key role in retaining consumer trust. The global economic crisis combined with increasingly sophisticated targeted attacks on financial institutions present a scary combination of *motive* and *opportunity*, making information security of paramount concern for 2009.

Warning Signs

So how do you know how your information security program stacks up? Below are a few red flags that may indicate opportunities for improvement:

- You do Risk Assessments solely for compliance purposes and not to improve the business. You make updates looking in the rearview mirror rather than through the windshield of active risk management.
- Management doesn't have the meaningful information they need to exercise oversight responsibilities.
- Your Internal Audit does not have the technical knowledge to assess the effectiveness of IT controls.
- There is confusion over definitions. Many organizations mistake a "penetration test" for a "Risk Assessment" or an "IT audit" for a "general controls review."
- You spend more time on security compliance *activities* than on overseeing and managing IT risk.
- You spend too much time on reacting to symptoms rather than addressing root causes. An example of this is time you spend putting out fires caused by unpatched systems instead of improving the update process. Or worse, scrambling to do a forensic analysis after a suspected system compromise without retaining the evidence through event logging.
- Your employees have introduced new IT risks without management awareness (e.g. computer viruses, USB devices, PDAs or inappropriate Internet activity).

In this difficult economy, all businesses are looking for ways to lower expenses and do more with less. Considering the increased risks and expanding regulation, now is not the time to neglect security. The good news is that most information security programs can be improved significantly without tremendous capital expenditures but through more effective risk management techniques and oversight.

Steps for Improvement

- **Establish Governance** – Senior management needs to take the protection of information assets seriously, allocate appropriate resources, oversee the security program and set the tone of protection for the organization. It starts at the top, and designating the right person to be the Chief Security Officer (CSO) is critical.



The CSO should have enough knowledge to understand IT security concepts and the internal clout to enforce the management-approved policies across departmental boundaries.

- **Manage Risk** – Management and the board need to approve the organizational appetite for risk and how threats are managed. This includes clear and concise documentation of the organizational threats, how the threats are mitigated and where exposure remains. Most would prefer to protect a few critical systems extremely well, rather than protect everything poorly. To do this effectively, IT assets need to be classified and prioritized to determine the adequacy of controls.
- **Process vs. Activity** – Risk should be evaluated on a routine basis, not simply when the Risk Assessment is updated annually. When looking at new products/services, technology, vendors and even employees, you should include threats and mitigating controls in your evaluation and selection process.
- **Increase Awareness** – A culture of protection and healthy paranoia should exist among employees. This is accomplished through ongoing training and education—not only on “what” the security policies are, but on “why” the policies exist to protect the institution, and “how” to respond if there is suspicious activity.
- **Quality Testing** – Key security controls need to be tested on a regular basis and when change occurs within the environment. There are a variety of methods to effectively test the *technical, administrative and physical controls*. Tests can range from security vulnerability assessments and disaster recovery exercises to test technical controls, to tabletop exercises and social engineering testing methods to test administrative and physical controls.

No doubt, 2009 will be the year where management oversight will be required to appropriately allocate resources, as well as achieve compliance. The focus will not be on the IT-related compliance activities that are being performed, but on how overall IT risks are managed. An effective Risk Management program combined with Governance will go a long way to improve the overall security posture to meet the challenges ahead.

By: Jeff Olejnik, President
Assurity River Group, Inc.
4500 Park Glen Road, Ste. 120
Minneapolis, MN 55416
952-230-6488
jolejnik@assurityriver.com
www.assurityriver.com