Moments of Truth -

By Adam Lipson

Your web site has been hacked. Confidential new product information is being used by a competitor. A senior executive accepts a job with your most feared competitor. Your manager tells you a third party security audit will commence in 30 days.

Most companies confront difficult IT security challenges only after being faced with a crisis or "moment of truth." Some examples of these moments of truth include:

- Virus Protection: The lack of good workstation protection practices enabled the Code Red virus to infect more than 25% of individual desktops and laptops within an enterprise. In order to remove the virus and repair the damage, the company needed to devote approximately 2 hours of IT support per desktop and experienced a complete day long shut down of its e-mail system. Across a company of 1,000 employees, this translated into 2,000 hours of technical support, and untold loss of worker productivity.
- Disgruntled Employees: Another company believed that a senior executive terminated for cause may have taken confidential sales data, but they needed to prove it. Their only option was costly investigation and, once the theft proven, time-consuming litigation.
- Intellectual Property Loss: A competitor was able to break into a company and obtain valuable intellectual property – because of a weak network security perimeter.
- Web site Defacement: A company's Web site was defaced. and an article in the newspaper about the defacement caused the stock price to drop.
- Company Audit: An annual security audit revealed significant vulnerabilities in infrastructure security. Addressing the numerous citations proved far more expensive than a proactive program for protecting systems and networks.
- Third-Party Interfaces: A company granted a new partner a feed to a sensitive database without adequately checking its security practices. It opened up the enterprise to all of the vulnerabilities of the partner's network

These are just a few examples of the many crises that cause companies to take action. In fact, reacting to these will consume a lion's share of a company's IT security budget. R*eactive* security will never result in complete security. While it is true that an organization cannot foresee every conceivable cyber-security risk, a preventive strategy immunizes a company against the most likely threats.

Smart Security Does Not Need to Cost More.

A well-rounded security program addresses more than just the perimeter technology. A holistic approach must include processes, people and integration in all facets of work. A complete and effective framework includes:

- Well-maintained security policies – Since most attacks occur from within the enterprise, specify a standard for what is acceptable, who enforces the policy and the consequences of violation. Well maintained policy will reduce the risk of loss.
- Regular user awareness training and education – Let the users know how they can contribute to protecting the corporate IT assets. Educating users on sensible security practices can result in reduced IT security risk.
- Continuously monitored network perimeter protection – Manage the security perimeter and host based security including log review and incident evaluation. This gives your business the opportunity to react appropriately to security breaches.
- Up-to-date system hardening baselines – Implement and maintain consistent system builds on all hosts, routers, firewalls and applications that include security best practices. Up-to-date hardened configurations are more resilient to attacks.
- Diligent user authentication, authorization and revocation processes – Good security is as much about allowing easy access to those who should have access as it is about not allowing unauthorized user access. Sensible policy and practice of user authentication improves overall security posture.
- An effective, well-rehearsed disaster recovery/business continuity plan – Put disaster recovery and business continuity plans in place. Routinely evaluate and test plans. This can prepare your company for the worst case scenarios. While requiring effort and expense, this can save your company from downfall.
- A current and effective malicious code/virus protection program – Malicious code/viruses results in billions of dollars of loss annually. A virus protection program must be included in any credible security program.

- Up to the minute monitoring of emerging threats and newly discovered vulnerabilities – New threats and vulnerabilities appear on a daily basis. An effective security program must include a program to address emerging security threats.

The Illusion of Security

More than 60% of security breaches come from internal sources. Simply installing a network perimeter firewall only creates an illusion of security for it only protects from outside attackers. Even the best firewall cannot prevent the more common internal attacks, nor can it assess damage. Moreover, most valuable information assets reside in applications and databases. A properly configured firewall can prevent unintended network services from penetrating a perimeter. However, they do nothing to harden a server operating system or secure an application from attacks that occur beyond the firewall.

Security is no better than the weakest link. A good "security chain" includes nine security domains:

	TECHNOLOGY	PROCESS	PEOPLE
INTERNAL	INTERNAL PENETRATION TEST	HOLISTIC ASSESSMENT	HOLISTIC ASSESSMENT
PERIMETER	EXTERNAL PENETRATION TEST	HOLISTIC ASSESSMENT	HOLISTIC ASSESSMENT
EXTERNAL	HOLISTIC ASSESSMENT	HOLISTIC ASSESSMENT	HOLISTIC ASSESSMENT

Even an effective security program built on process, people and integration can be undone by a naive user writing her username and password on a sticky note pasted to their monitor. The best IDS (intrusion detection system) will prove useless if the people monitoring it are not alert and well-trained in appropriate incident response procedures. A terminated employee can continue to access sensitive information if the human resources department fails to inform the account management group to close all system accounts for that person.

Simply performing security perimeter reviews does not constitute a credible security program. An effective information security program identifies, evaluates and mitigates security risks in all nine security domains. It includes policy, architecture, business assessments and on-going management within all nine of the security domains.

Call to Action

Making sound business decisions requires good data. The same principle holds true for security. A coherent security program begins with an understanding of the quality and magnitude of a company's information risks. Knowing that burglars usually come in through an open window means there is no point in locking the front door if you've left the windows open.

If you are an executive with responsibility for technology or security, ask yourself the following questions:

1. Do I understand my true IT security risks? When was the last time we conducted a thorough security *risk* assessment that covered technology, processes and people? Was the last security assessment merely a "check box" of the perimeter security?
2. Do we have a ***documented*** security framework that includes the nine security domains listed above? Can we benchmark the framework against an industry standard? Do we execute according to the framework?
3. Do I believe it? Can the IT staff show me a ***written*** policy for disposal of desktop computers with sensitive information? Can my security personnel to show me how they seek out current information on new attacks (e.g., Nimda or Code Red), geo-political threats, and emerging vulnerabilities against core corporate technologies Does the server support group use ***documented*** hardening baselines for consistent, secure builds of new platforms?

If the answers you receive left you with an uneasy feeling, then dig deeper. Start with a security risk assessment. If you have the experience, you can do this internally. Or, you can go to an outside security consulting firm if you don't have the in-house capabilities or available resources to assess all nine security areas. Once you understand your risks, only then you can build or upgrade your security framework.

About the author: Adam Lipson is the Executive Vice President of Client Services & Product Development at Vigilinx (http://www.vigilinx.com), a leading full service provider of digital security solutions,