Deloitte.

The Future of Security
Evolve or Die

Ken DeJarnette
Principal
Deloitte & Touche LLP

November 2011

Contents

- Evolve or die
- Six trends to consider
- Evolving risks and challenges face off against opportunity
  - Social media: Don’t “friend” your enemies
  - Mobile devices: Multiplying avenues of attack
  - Cloud computing: Cloudy with a chance of infiltration
  - Software vulnerabilities: The soft underbelly of your IT environment
- Conclusion : Evolution is a process, not an event

Evolve or die

- The ***business environment*** is evolving as competitive conditions and customer needs evolve, giving rise to new business models, processes, and ways of working.
- The ***IT environment*** is evolving to support new business models and users who adopt new tools to keep them connected and productive.
- The ***threat environment*** is evolving as the business and IT environments evolve to create new exposures, vulnerabilities, and avenues of attack.

Are your security and risk management capabilities evolving to keep up?

Six trends to consider

How vulnerable organizations are prone to attack by cyber threats

Six trends to consider

1. **Targets of choice, not chance:** Attackers increasingly target specific companies, products, services, and individuals.

2. **Involvement by organized crime:** Low risks and high rewards lure organized crime to cyber crime and supporting activities.

3. **State-sponsored cyber threats:** Financial, political, and strategic ends motivate state-sponsored operators to compromise systems and steal intellectual property.

4. **Growing insider threats:** Insider incidents have risen due to economic conditions and “insider access” accorded to non-approved third parties.

5. **Legislative initiatives:** New cyber legislation with private-sector implications may increase penalties for non-compliance.

6. **Global implications:** Global operations may need rethinking, given attacks such as Aurora and the complexity of dealing with international investigations.

Evolving risks and challenges face off against opportunity

Four risks in 2011 and beyond

Social media: Don’t friend your enemies

- Many corporations are still working to develop a coherent social media strategy, but most agree that this new channel will be increasingly important for attracting and interacting with their customers.
- The rapid adoption and growth of social media are driving many companies to react quickly.
- Many organizations focused on understanding the business value of social media are losing sight of the risks associated with adoption.
  - New avenues for attack
  - Social engineering opportunities
  - Brand and reputation vulnerability

Adversaries can use data extracted or derived from social media sites and various public information sources to build profiles of executives and board members for identity theft or actual attacks, for instance, via account access or spear-phishing.

Social media: Steps to consider

- **Get smart**. Understand the features and dangers of social media sites and collaboration tools and foster awareness of their limitations and risks.
- **Create boundaries.** Policies governing the use of social media and collaboration tools, and for data loss prevention and user education, are essential.
- **Educate your workforce.** Training can promote proper use of social media and collaboration tools and limit inappropriate data sharing.

Mobile devices: Multiplying avenues of attack

- Almost all corporations are dealing with increasingly mobile workforces and customer bases who have made laptops, tablets, and smart phones pervasive.
- Mobile devices present relatively easy, low-risk points of entry to attackers, who can remotely monitor them for passwords, account numbers, and personal identification data.
- The proliferation of mobile “apps” complicates the enforcement of enterprise security standards.
- Mobile devices are especially vulnerable when traveling internationally, especially in geographies where governments are less active in enforcing laws against cyber criminals or may themselves be involved in state sponsored cyber espionage.

While many of today's smartphones can be configured to lock down [Internet] browser access, limit downloading of third-party applications, and improve control over other functions, the policies must balance protection and productivity.

Mobile devices: Steps to consider

- **Lock it down.** Configure mobile devices to minimize the chance of their being scanned, sniffed, or tampered with.
- **Leave it home.** Consider restricting users' primary mobile devices to domestic use, and issue temporary devices with minimal data and/or limited functionality for overseas travel.
- **Employ dynamic policies.** Policies such as application white lists are essential, as is considering mobile devices' security capabilities and limitations in purchase decisions. Be wary of the performance tradeoffs (which can be considerable), however.

Cloud computing: Cloudy with a chance of infiltration

- Scale-to-market and economic considerations are driving increased business demand for cloud computing, which is gaining market acceptance before technology and security are mature
- Security concerns have led corporations to take a conservative approach to cloud (particularly ‘public’ cloud) adoption. The exception is within the Technology, Media, and Telecommunication industries where early adopters (many of whom are moving in to the provider realm) are leading the way
- Responsibility and governance questions are as critical as technology concerns, but should be addresses like any other business risk
- Inherent risks are exacerbated when data in the cloud resides in a foreign country or moves across international borders

Providers typically do not accept the business and financial risks that cloud computing poses to the enterprise.

Cloud computing: Steps to consider

- **Contemplate risk.** Include risk as a key factor in deciding which applications and data to move to the cloud and what type of cloud is most appropriate
- **Understand the configuration.** Know where the cloud components and your data will be housed and who is responsible for which functions and risks
- **Apply your standards.** To the extent possible, apply your standards to service providers, and remember that you can outsource functions but not risks
- **Trust but verify.** Due diligence when selecting service providers and the right to assess their security capabilities on a periodic basis are important

Software vulnerabilities: The soft underbelly of IT

- Faster development cycles and the proliferation of applications have created more vulnerabilities
- Social networks and mobile platforms have made the problem more pervasive
- Highly evolved underground economies have developed to make exploiting these vulnerabilities easier and more prevalent
- Most security teams are out-resourced by well organized criminal elements, state sponsored attackers, and communities of “hacktivists” who are increasingly effective at coordinating their efforts

Attackers have almost unlimited time, skills, and resources to devote to creating and exploiting vulnerabilities.

Software vulnerabilities: Steps to consider

- **Incorporate good offense into your defense.** Employ cyber intelligence to understand what threats are developing and what attacks may be targeted at your organization
- **Anticipate and defend.** Anticipating failure enables you to develop damage control, system resiliency, rapid recovery, privacy protection, and notification and public relations plans
- **Define normal to identify abnormal.** To monitor for unknown threats, it is possible to develop heuristics that can detect unusual code or activity
- **Exercise vigilance.** Develop baseline metrics and maintain situational awareness of network activity, monitoring for unusual spikes or traffic destinations

Conclusion

Evolution is a process, not an event.

Evolution is a process, not an event

- Security functions must accelerate their own evolution to match the speed at which the environment is evolving
  1. Gather intelligence from a variety of sources
  2. Transform that intelligence into actionable information
  3. Treat security as discipline, not a department, so the organization can better act on the information

- Security functions need to control the dialogue better so that agendas are not dominated by regulatory requirements and media hype

- Take a risk-based approach to formulating a measured response and allocating resources according to the value of assets and assessment of threats

- It's not a matter of security "doing more," but rather evolving in ways that make sense for the organization given the environment, and continually balancing benefits against costs and risks

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.