Published on *The National Law Review* https://www.natlawreview.com

10 IT Risk and Security Trends to Watch

Article By:

Risk Management Magazine

IT risk and security remains an ongoing business problem that demands vigilance. The following are 10 trends to watch for in the coming year.

1. Information Risk Management (IRM) Outsourcing

Outsourcing in the IRM domain can help companies create a program that is more effective, more agile and cheaper. All IRM activities can be outsourced, and those firms that rely on full-time, domestic hires to reboot their programs will face higher costs going forward, which may prove unsustainable.

2. Information Security Management System (ISMS) Certification

Over the next five years, ISMS (ISO 27000) certification will become a de facto best practice. The United States will soon catch up to its peers as American firms recognize that ISMS certification is essential to effective risk mitigation.

3. Compliance

Signs point to an increasing frustration with the legal and regulatory impositions on enterprises amid growing concern that investment benefits will not be achieved by misdirected or vulnerable compliance efforts. At the risk of losing momentum and knowledge, many will look to reorganize and find staff able to address these challenges. A better alternative is to establish information security road maps that track progress and report results to senior management.

4. Business Agility vs. Best Practices

Partially as a consequence of achieving compliance, tension has built up between the drive for agility and market share versus the need to follow best practice and process disciplines. Efforts to resolve this tension can result in costly business interruptions. To prevent this, firms must identify critical services where failure would cause significant, highly visible business outage, and enforce best practice and process disciplines in these areas.

5. Mobile Computing

Mobile computing is gaining momentum due to its inherent advantages: agility, accessibility and collaboration. But in order to ensure that this trend can continue unimpeded, security must be enhanced. Data encryption, user authentication and transaction non-repudiation are all needed. In order to succeed, firms will need to get ahead of the curve in defining standards and developing secure mobile applications-and then provide continual security assurance.

6. Strong Authentication

Whether communicating with fixed workstations, notebooks or mobile devices, the use of strong authentication techniques is a growing trend. This can include device confirmation in combination with out-of-band authentication (e.g., a separate account access PIN transmitted to a user's registered cell phone that needs to be entered by the user to complete a login or financial transaction).

7. Continuous Security Testing

Both external intrusion and inside abuse are often in progress long before the activities are detected. Periodic network security assessments no longer suffice. Advanced enterprises are now adopting solutions that support continuous testing and provide sustained network security assurance.

8. Insider Fraud and Abuse

The insider threat still represents the greatest security risk. The FBI reports that insider fraud and abuse costs billions of dollars. Data loss/leak prevention (DLP) solutions respond to this threat by stopping careless users from inadvertently exposing sensitive information.

As a countermeasure, smart organizations are working to gain greater insight into authorized user behavior by asking, for example, what employees are actually doing with their given privileges. This is coupled with analysis to establish patterns of behavior. Alerts are raised if a user departs from established rules or normal patterns. While security logs only show that users are accessing the resources to which they are permitted, insider surveillance provides the virtual equivalent of a physical security camera.

9. Cloud Computing

Cloud computing typically supports an internet-based service outsourcing model, giving enterprises a way to move publicly accessible information out of their own computing infrastructure. As an outsourced service, some responsibility and risk shifts to the service organization. For example, the provider must supply secure communications, secure access and internal restrictions to isolate customer data. However, there have been situations in which the cloud customer believes all responsibility shifts to the service.

On the contrary, consistent with all security guidelines and regulatory compliance, the customer retains ownership responsibility. The cloud provider indeed has custodial responsibilities, but this is usually limited to establishing access and data isolation between customers.

10. Social Networking

Social networking is gaining ground for intra- and extra-enterprise collaboration. As with all new and potentially risky technologies, the knee-jerk reaction will be to deny and ban these services. This will only delay the inevitable and lead to a late, hurried response.

Firms should embrace social networking early on and work on the information risk and security management requirements. End-users will represent the primary risk because as they become more comfortable with using these tools in their personal communications, they will likely lose their security and risk awareness over time in the workplace social networking environment.

Brian Cummings *leads North America IRM Advisory services for Tata Consultancy Services.*

National Law Review, Volumess I, Number 43

Source URL:https://www.natlawreview.com/article/10-it-risk-and-security-trends-to-watch