RIS Retail

Posted Date: 9/5/2010

Gearing Up for the Holidays? So Are Cyber-Criminals

By Michael D. Peters

The holidays typically are the peak season for merchants. Yet at such a critical time of year many retailers still leave themselves vulnerable to significant e-commerce fraud – and the corresponding lost revenue and damaged brand reputation -- because they don't enforce or implement information security best practices throughout the year.

While cyber-crime statistics have been historically hard to track, the FBI's joint report with the Internet Crime Complaint Center (IC3) showed that in 2009 complaints of online crime increased significantly by 22.3%. There isn't any reason to expect that 2010 will show a dramatic decrease.

With those statistics in mind and Holiday 2010 quickly approaching, here are three strategies retailers can implement to avoid the unwanted attention of cyber-criminals this year.

1. Evaluate Technology Usage – selecting the right technology and effectively using it makes all the difference not only in performance, but more significantly, towards preventing cyber-crime. So many organizations that have lost sensitive personal information or have suffered security breaches later recognize that they potentially could have prevented it. Considerations include:

- Data Protection: the protection of critical information assets, the very soul of our electronic business world.
- Online Transaction Security: the various technical controls in use protecting the transfer of business data, customer data, and identities.
- Cloud-based Application, Server, and Data Security: the latest, greatest thing in computing has added a new layer to balance security and business as never before.
- Application Layer Protection: holistic methodologies of protecting applications within the application layer from threats that open us to unauthorized access and attacks or may expose our private information.
- Information Security Architecture: describe how the security controls or security countermeasures are positioned and how they relate to the overall IT Architecture while

serving the purpose in maintaining the system's quality attributes, among them confidentiality, integrity and availability.

2. Unending Vigilance –the internal and supporting organizations that exhibit a "caring, can-do culture" with respect to information security and data protection help protect against security breaches. Considerations include:

- Cross-Channel Risk Management: you'll have either financial loss or reputational loss — sometimes both, and the better approach is to reduce business risks through the cooperation of technology, business and compliance efforts.
- Emerging Threat Evaluation: any credible business person or security practitioner will keep tuned into the threat-scape, collaborate with business peers and other resources to be better prepared for tomorrow's zero-day threats.
- Security Configuration Management: the monitoring, change detection and enforcement of established security configuration policies.
- Business Continuity and Disaster Recovery Strategy: involves planning for keeping all aspects of a business functioning, including IT or technology systems, in the midst of disruptive events.
- Security Business Process Development and Management: holistically refers to the established process whereby information security standards are implemented and maintained organization wide.

3. Responsible Governance – delivering regulatory and compliance evidence will significantly benefit the bottom line while bolstering information security. There is a distinctive difference between organizational intentions regarding governance and data security and how they actually protect it, creating a wide threat gap. Considerations include:

- Change Control: the formal process used to ensure that changes to a product or production system are introduced in a controlled and coordinated manner that reduces operational and security risks.
- Regulatory and Industry Compliance: specific audit requirements may vary between the different compliance requirements and industry regulations, but all consider data protection key.
- Information Security Policies and Procedures: the foundation to all of the technology deployed and the utilization whereof.
- Security Audits: describes the measurable technical and security assessment of a system or application.
- Cross-Channel Security Best Practices: defines the application of current best practice methodologies coupled with proactive security procedures reducing threat opportunities to business.

By Michael D. Peters is Chief Information Security Officer CrossView Inc.