Cyber-Security Today

a current look at the security threat landscape

Presented by:

Claudiu Popa, CISSP CISA CIPP CRMP

President, Informatica Corporation

on the agenda

1. Intro
2. Impact
3. Who
4. Where
5. What
6. How
7. Trends

who are we?

history	Established 1989, systems integration & networking Specialized in data protection since 1996
industry focus	All sectors Particular expertise in FI, healthcare and public
competencies	Certified risk and security professionals only Deployed across Canada
differentiators	Assessment methodology incorporates global standards Extensive proprietary content
approach	Risk-based, top-down methodology Defense-in-depth, security by design Focus on processes and controls

how do we know?

security project management	SPM ensures that PMI-compliant project management practices are in use in IT projects
merger and acquisition support	Specifically designed for all situations involving corporate transformations and technology acquisitions
security scenario and risk mitigation	Anticipate disasters and mitigate risks using structured brainstorming and strategy consulting with certified auditors
communications & incident planning	Prepare for incidents and disasters before they occur with a complete package of predefined emergency practices
secure internet presence	periodic and continuous Internet monitoring for organizations with an active online presence and extensive content
evaluations of 3rd parties and technologies	evaluate 3rd party agreements, SLAs, employee and contractor documentation and new technology acquisitions

what is the impact?

1. On people
2. On processes
3. On technologies
4. On the economy
5. On the bottom line

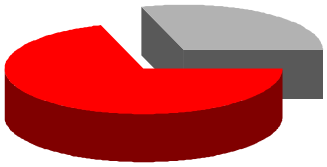
by the numbers

- CEOs: Compliance #1 cost influencing profitability
- IT: 42% of firms not doing enough to implement security
- Managers: 68% have too much PII to handle securely
- 40% of IT & Compliance practitioners pessimistic about future
- Estimated cost of remediation per compromised record: **$182**
- Minimum number of compromised data records since January 2005: **354,550,351**

- 2007 NYSE/Ponemon survey
- 2008 Verison Data Breach survey
- 2010 Privacy Rights Clearinghouse

who is behind the attacks?

- 73% hackers, organized crime, Internet-borne threats
- 18% insiders, gruntled or otherwise
- 39% included business partners, 3rd parties, suppliers, vendors, etc



73%
external sources

where are the attacks focused?

- weak, basic controls
  (87% preventable using basic / reasonable controls)
- weak, complex controls
  (detectable using best practices monitoring and auditing)
- processing and tracking mechanisms
  (monitoring and logging often overlooked)
- emerging technologies
  (opportunistic attacks up to 85% of intercepted breaches)

- 2010 Informatica Research

what is being targeted?

- personal information
- physical assets
- access credentials
- unmonitored data or systems
- proprietary corporate information
- trade secrets
- backup data
- potentially embarrassing info

how is it done?

- social engineering / pretexting
- intelligent polymorphic swiss army rootkits
- zero-day attacks
- smartphone & mobile computers
- corporate identity theft
- domain name hijacking
- backdoors and built-in malware
- workplace surveillance and monitoring
- **a growing list of application security attacks**

where to look for signs of trouble?

1. visitor management, access control, physical zones
2. clean desk/clear screen, recyclables, fax room
3. disclosures, privacy policy, data classification
4. network jacks, password prompts, unsecured laptops
5. wireless presence, removable storage, USB keys, backups
6. segregation of duties, principle of least privilege
7. generic/shared logins, security tied to sensitivity
8. secure development, promotion, SDLC practices
9. adherence to standards, legislation awareness
10. remote access, online application complexity

best practices

- security and privacy awareness
- technology hardening
- testing and risk assessments
- mobile and remote security
- effective incident management
- cohesive controls
- proper visibility and monitoring
- proper physical security

challenges and directions

1. Making centralized information risk management useful
2. Understanding and implementing incident management
3. Implementing convergence without exponential risk increase
4. Making secure access control and easier pill to swallow
5. Enabling proper business continuity with focus on compliance
6. Adopting consistent security across partner and customer web

disruptive technologies for the next 18 months

1. identity and access management
2. secure virtualization
3. pattern-based malware detection
4. centralized threat management
5. unified compliance management
6. smartphone and mobile computing security

trends & discussion

- industry standards moving towards government regulation
- PIA/TRA analysis migrating towards holistic risk management
- unified compliance processes combine standards and legislation
- privacy focus to drive compliance pressures to drive security spending
- organizations with mature risk processes to streamline & leverage

activity

- security project management
- risk & threat assessments
- awareness, education & policy

contact

- www.SecurityandPrivacy.ca
- twitter.ClaudiuPopa.com
- LinkedIN.ClaudiuPopa.com