Strategic Approaches to Cyber Security and Digital Forensics

Presented by:

Maureen Hayden-Cater
President
First Global Bank Limited

What is Cyber-Security?

- Cyber security involves protecting personal and business information by preventing, detecting, and responding to attacks on the systems, networks and data in cyber space.
- Increasingly critical threat to global financial institutions. Large firms are prime targets for activists, organized crime, and cyber terrorists.
- An attack on an institution can have a devastating effect on the firm's reputation, costing significant amounts of time and money to repair.

What is Cyber-Security?

- Still not as well understood by many company heads as it should be

Password
123456
klossner
" I DON'T THINK YOU UNDERSTAND THE CONCEPT of CYBERSECURITY."

http://blog.lumension.com/6053/cyber-security-awareness-month-lumension-style/

Cyber-Security and Financial Institutions

- Interconnection of financial institutions is crucial to the financial system's functioning, but it's also an area of vulnerability
- This risk increases as these institutions connect with third-party vendors and service providers to expand offerings and improve efficiency
- Risks can include anything from fraud to espionage, disruption of operations, and destruction of information

Considerations for Financial Institutions

- How do we balance secure online transactions and excellent customer experience?
- How do we protect sensitive business information while encouraging collaboration?
- How do we ensure that our systems aren’t compromised by third party suppliers?

Shifting Role of Cybercriminals

- Cybercrimes not just committed by amateurs
- Criminal organisations (or hostile nations) have embraced digital technology as an important weapon
- Attacker who has gained access to a company network may sell the access credentials
- Organisation may be targeted as a means to get to another organisation via a linked system

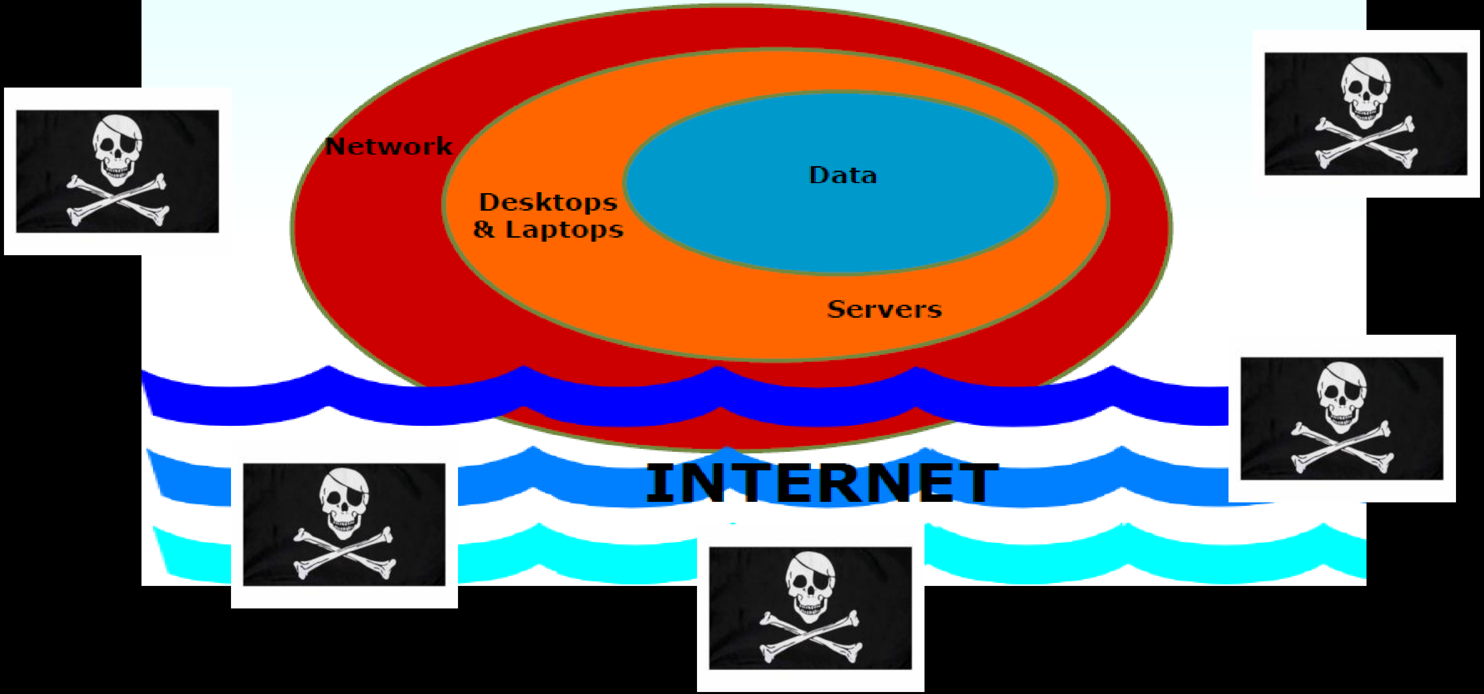
New Technologies, New Threats

- Emerging technologies increase the number of access points
- Mobile banking. Juniper Research estimates the number of mobile banking users worldwide will reach 530 million by next year, up from 300 million in 2011.5
- Cloud computing. The movement of services or data to the cloud mean that firms don’t have control of that data. While institutions may not use the cloud directly, third-party vendors may.
- Bring your own device (BYOD). The devices may not be as secure, or the company may not be able to manage the device as effectively

Why Commit Cyber-Crimes?

- **Access to money** – the impact on financial losses can be millions of dollars depending on the extent of damage
- **Obtaining information concerning intellectual property** – theft of intellectual property can give its competitors a considerable advantage with trade secrets
- **Loss of customer data** – Can result in brand reputation damage, data privacy violations, and other personal liability issues.
- **Identity theft**

Countermeasures: Layered Protection



Response: Prevention

- Understand that cybercrime is here to stay
- Organizations need to be aware of the risks of people, processes and technology and how they can be exploited
- Limit access to the company’s most sensitive data
- Awareness training programmes should be put in place for ALL employees in ALL areas

Response: Prevention

- Budget: Don’t be ‘penny-wise and pound foolish’. Ensure that the necessary funds are put towards IT security
- Monitor systems and behaviors closely to note any abnormal changes
- Educate and train employees constantly

Response: Detection

- CIO’s and CRO’s must keep abreast of changes in technology and risks
- Logging of critical events and monitoring central security incidents and events will strengthen the technology detection measures.
- Information security must be a continuous process and organisations must start to proactively anticipate instead of reactively act on incidents.

Key Weaknesses: Insider Threat

- Current and former employees, contractors, and other organizational "insiders" pose a substantial threat by virtue of their knowledge of and access to their employers' systems and/or databases and their ability to bypass existing physical and electronic security measures through legitimate means
- According to a 2005 (Carnegie Mellon University) study, most insider attacks required little technical expertise.

Possible Solutions

- Monitoring privileged user activity
- Correlating IT access and physical access
- Conducting frequent background checks (know your employee)
- Removing physical access to facilities and critical assets almost immediately upon employee termination

Possible Solutions

To minimize the impact of such attacks, the institution should consider the following :

1. Formalizing procedures (that prevent these attacks from being successful)
2. Continuing security awareness testing exercises (to build a **culture of security** and form the basis of tracking and ensuring continuous improvement)
3. Conduct full penetration assessments (to confirm the resilience of technical controls to prevent these forms of attacks)
4. Providing refresher security awareness sessions
5. Revise security awareness program to include:
    - i. Recognition of threats.
    - ii. Explicit actions to be taken if a threat is identified.
    - iii. Handling of threats in progress.
    - iv. Incident handling and escalation procedures.

Conclusion

- Cyber security needs the attention of all business interests
- In addition to the prevention of incidents, timely detection and an adequate response are critical
- Companies need an effective strategy to counter cyber crime
- New technologies must be taken into consideration when planning for this strategy