Vulnerability of Financial Institutions to Cyber Crime

Presented by Damian Donaldson MSc. Information Security, CISSP, CISM

The Importance of Cyber Security to Financial Institutions

- Financial Institutions depend on information in order to function.
- Clients are provided not just with financial services, but also security services.
- Providing clients the assurance of confidentiality, integrity and availability of their financial information is a key function of financial institutions.
- Information systems and technology are critical for the operation of financial institutions.
- Information is a valuable commodity. Financial information is especially valuable to criminals.

Why target Financial Institutions?

- Financial Institutions are attractive cyber crime targets.
  - There is a lot of money to be made.
  - Technology has made cybercrime more rewarding and less risky for the criminal than traditional criminal activities.
- Example: The Carbanak cybercrime group made headlines in February 2015. They compromised the technology infrastructure of financial institutions using malware and were estimated to have stolen tens of millions of US dollars (exact amounts stolen still not known).
- Example: The Bangladesh Bank heist in February 2016 in which US$81 million was stolen after credentials for the SWIFT system were compromised and used to initiate fraudulent fund transfer requests.

Vulnerabilities in Financial Institutions

- Technology vulnerabilities
  - Technology hardware and software have flaws.
  - This affects every industry (not just financial sector)
  - Organizations cannot always respond to fix these flaws as quickly as they should due to cost and resource constraints.
  - Over time technical defences have improved.
  - Good governance processes needed to mitigate risks.
- Fleshware vulnerabilities (human weaknesses).
  - Attackers have found it is much easier to hack the humans (staff and clients).
  - Exploit emotions, lack of knowledge, greed etc. – Social Engineering.
  - Use technology to trick humans (Phishing emails, banking malware, ATM card skimming, etc.).
  - Improving security awareness is key to making the situation better.

Vulnerabilities in Financial Institutions

- Cyber criminals have many avenues of attack.
- They can attack the financial institutions directly (requires more planning, coordination, resources and technical skill).
- They can attack persons who interface with the financial institutions
  - Individuals likely have less protection and “softer” defences than institutions
  - Every person with an ATM card, credit card, Internet/mobile banking password is a potential target and source of revenue for the cyber criminal.
- The use of technology to increase points of customer contact, facilitate the conduct of business at any time and from anywhere has expanded the borders of the institutions and presents cyber criminals with a much larger attack surface.

Examples of Cybercrime attacks

- Fraudulent email (Phishing)– used to trick persons into giving up account details, passwords, PIN numbers. Email looks “official” and may contain a link to a legitimate looking website, or have an attachment the recipient is urged to open.
- If the recipient clicks the link, they may be taken to a fraudulent website which looks legitimate and invites them to enter their sensitive details.
- If the recipient opens the attachment, that attachment may turn out to be a malicious application which secretly records things they type and helps attackers get sensitive information which can be used for fraud (banking malware).
- Card skimming/cloning
- Money laundering via money mules (lotto scamming, work from home scam, mystery shopper scam, relationship scams).

Examples of Cybercrime attacks

- Hacking of Internet facing systems still takes place
- Attackers scan for vulnerabilities in Internet facing systems.
- They then exploit these vulnerabilities with technical tools to gain privileged access to the systems.
- The attackers then manipulate the system to gain further access to the organization’s network, or initiate transfer of funds from the institution.
- This kind of attack has become more difficult to execute as technical defenses have improved.

Challenges in dealing with Cybercrime

- Institutions face all kinds of risk. Cyber Security risk is just one such risk. Some institutions prioritize other issues ahead of cyber security. Hence resources and attention are focused elsewhere.
- Sometimes cyber crime activity is not detected in a timely manner. Many organizations don’t realize they have been victims of cyber crime until very late.
- Cyber crime investigations can be very complicated. It is sometimes difficult to identify who the criminal is and where they are. Attackers can be anywhere and can use computers all over the globe to aid in their attacks. Jurisdictional issues come into play. Sometimes resources from multiple jurisdictions are required just to complete an investigation. That presents its own challenges.

Digital Forensics and Evidence

- Succesful prosecution of Cyber Crime cases depends on the availability and quality of digital forensic evidence.
- Forensic tools and techniques need to be used to gather digital evidence in a manner that preserves integrity, and facilitates investigation and reporting.
- Many organizations are not in a position to properly generate, capture or preserve the kind of digital evidence that would be useful in an investigation or for successful prosecution.
- Systems and personnel must be prepared beforehand to assist with the investigation of cyber crimes before there is an incident.

Conclusion

- Financial Institutions make attractive targets for Cybercrime because that is where the money is.
- Often times it is the people who work within and do business with institutions that are the most vulnerable links in the security chain.
- Technology alone cannot solve the cyber crime problem.
- Awareness is critical.
- Investigating and prosecuting cyber crime incidents can be complicated endeavours.
- Institutions have to prepare themselves for incidents before they happen.

Thank you!