Cyber Crime & IT Fraud

Could your organisation survive if it lost $20,000? $50,000? Or $1 million overnight?
Contents and Outline

• Overview
• History
• Categories of Cyber Crime
• Types of Cyber Crime
• Prevention and Cyber Security
• Current Case Studies
Overview

The 5 most cyber attacked industries

1. Healthcare
2. Manufacturing
3. Financial Services
4. Government
5. Transportation

“Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual” – Interpol

1. The Computer as a weapon
   - Using a computer to commit real world crime
   - Cyber terrorism and credit card fraud.

2. The Computer as a target
   - Using a computer to attack another computer
   - Forms of Hacking, DOS/DDOS attack, virus/worm attacks
History

- **1820** - First recorded cybercrime
- **1978** - The first spam e-mail
- **1982** - The first virus was installed on an Apple computer

**2003-2004**

- Script Kiddies
  - Bragging rights or intellectual curiosity

**2005 - Present**

- Organized Crime
- RANSOMWARE
- CLICK-FRAUD
- IDENTITY THEFT
- Motive: Profit

**2016 and beyond**

- Highly organized criminal syndicates
- Brazen, complex, and persistent for profit
- $USD500 billion annually
Types of Cyber Crime

1. Hacking (credit card)
2. Denial of Service Attacks
3. Identity theft
4. Virus Dissemination
5. Computer Vandalism
6. Cyber Terrorism
7. Online Fraud
8. Software Piracy
9. Forgery
10. Malicious Code
11. Malware
12. Phishing
13. Spam
14. Spoofing
15. Defamation
### Why Do Breaches Occur?

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>42%</strong></td>
<td><strong>6%</strong></td>
</tr>
<tr>
<td>Mis-configured system or application</td>
<td></td>
</tr>
<tr>
<td>Configuration Errors</td>
<td>Installing applications</td>
</tr>
<tr>
<td>“Weak” defaults</td>
<td>suspect malicious</td>
</tr>
<tr>
<td>Easy passwords</td>
<td>Clicking links</td>
</tr>
<tr>
<td>“Bugs”</td>
<td>Phishing Emails</td>
</tr>
<tr>
<td>Input validation</td>
<td>Watering Hole attacks</td>
</tr>
<tr>
<td><strong>31%</strong></td>
<td><strong>6%</strong></td>
</tr>
<tr>
<td>Vulnerable code</td>
<td>Targeted attack, exploited</td>
</tr>
<tr>
<td><strong>15%</strong></td>
<td>Undetermined</td>
</tr>
</tbody>
</table>

*Source: IBM Security Services 2013 Cyber Security Intelligence Index*
Prevention and Cyber Security

- Firewalls
- Operating system is up-to-date
- Up-to-date anti-virus and anti-spyware
- Use a pop-up advertising blocker
- Use strong passwords
- Secure wireless network
- Reputable websites and mobile applications
- Avoid clicking on unexpected or unfamiliar links
Why is it so dangerous?
• Causes significant business disruption & data loss.
• A single compromised device puts a whole network at risk.
• Significant growth in new ransomware variants increases the risk of zero-day attacks.

Prevention
• Properly monitored End-point Anti-virus.
• Operating system and application patch management to avoid exploits.
• A Multi-layered email security system.
• A web security/web filtering system & firewall.
• Email and web use training.

Mitigation
• Backups should be regular, comprehensive and stored in a secure non-network accessible location. Many businesses have their backups encrypted too, resulting in complete data loss.
2017 Threat Study
Internal Threats

Stolen Credentials | Malicious Insider | Social Engineering

Why is it so dangerous?
• Staff are able to bypass most security measures taken.
• User accounts often have access to significant amounts of sensitive data.
• Requires little or no technical knowledge.

Prevention
• Implementation of Multi-factor authentication
• Restrict data egress channels. (USB, file transfer)
• Comprehensive exit process, performed immediately on employee termination.
• Clean desk policy.
• Staff training.

Mitigation & Detection
• Segregation of duties to minimise severity of data breaches.
• Network/file monitoring for abnormal behaviour.
What training do staff need?

Passwords
• Prevent reuse of passwords from external accounts, and sharing of passwords.
• Prevent insecure password storage. (post it notes on computer, stored on network drive).
• What constitutes a secure password. Enforce or suggest increased password complexity.

Emails, files and the web
• Identifying malicious emails, attachments and links.
• Identifying malicious files and common file types for malware delivery.
• Identifying malicious websites.
• Safe & work appropriate web browsing practices.

Other
• Preventing social engineering
• Signs a device may be infected & appropriate responses
• When to alert IT staff.
Preventing Network Vulnerabilities

Common issues
- Vulnerable components exposed to the internet e.g. RDP without MFA, PPTP VPN.
- Missing OS & Application Patches
- Misconfigured Firewall
- Poor monitoring and reviewal of server, firewall and antivirus logs.
- Website Vulnerabilities
- Unrestricted Physical and USB Access.
- Personal Device Connection to network
- Exploitable Wireless networks
- Poor Account Segregation

Test
- Network & web vulnerability/penetration testing, particularly for external facing resources
- Misconfiguration Testing
- WIFI Exploit testing
- Review Policy and procedure (automated tools exist to reduce IT labour)

Top 25 Remediations by Risk

<table>
<thead>
<tr>
<th>Remediation</th>
<th>Assets</th>
<th>Vulnerabilities</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. MS16-144: December, 2016 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB3205364)</td>
<td>2</td>
<td>152</td>
<td>22</td>
</tr>
<tr>
<td>2. MS16-001: Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 Edition (KB3124275)</td>
<td>2</td>
<td>54</td>
<td>20</td>
</tr>
<tr>
<td>4. Upgrade tcpdump for Ubuntu 12.04 LTS</td>
<td>1</td>
<td>41</td>
<td>0</td>
</tr>
<tr>
<td>5. Upgrade libpore6 for Ubuntu 12.04 LTS</td>
<td>1</td>
<td>25</td>
<td>0</td>
</tr>
<tr>
<td>7. Ll TIMES (Ubuntu 12.04 LTS)</td>
<td>1</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>
England National Health Service (NHS) Ransomware Attack

Between May 12 and May 19 2017, NHS was hit with a ransomware attack affecting more than 34% of trusts.

**Cause**
- Missing patches & unsupported operating systems (XP).
- Poor user training & response.
- Out of date firewalls and Antivirus.

**Result**
- Estimated 19 000 appointments cancelled, some urgent.
- Significant financial cost & loss of public image.
- Data loss, manual data re-entry and work disruption.
$90k Phishing email – fake CEO
• Finance manager received an email from the ‘CEO’ while the CEO was on leave holidaying in Asia
• The email asked the FM to transfer $90k to a foreign bank account
• There was back and forth between the FM and the ‘CEO’ regarding the details of payment
• FM prepared all of the relevant documentation and took this to the CFO for approval for payment. The payment was made

Issue - Email – was very strange and clearly fake

Result - This was a breakdown of the internal controls, rather than inadequate IT systems.
CASE STUDY C

Incident 1
- Customer Gmail account was hacked, invoice was sent to a customer for $15k with fraudulent bank details
- The customer paid the $15k to the fraudulent bank account
- Client wore the cost and police are investigating
- **Customer is now transitioning to Microsoft Outlook – Being a more secure email provider**

Incident 2
- A supplier email was hacked and the same situation as above occurred in reverse
- The invoice was send to our client for approx. 3K and client paid
- The payment was based off the bank details listed on the invoice (being fraudulent).
- The supplier will wear this cost and our client is not out of pocket
- **A process of checking master supplier bank details has been implemented prior to paying any invoices in order to mitigate this risk**
$12k
- Client was processing a refund for $12k
- A hacker watched on remotely as transaction took place
- The internet banking screen was actually a layover (fake) screen and as such the banking details typed in by the finance manager never hit the internet banking site
- The hacker entered different bank details
- They paid the full 12K to an incorrect bank account without knowing
- While the hacker was in their internet banking, he/she changed the account numbers of saved accounts, including staff super funds and employee bank details
- The bank refunded the money, the account numbers were corrected and an IT review was conducted to identify holes in the IT system
CASE STUDY E

$230k
• Two employees within consolidated group in receipt of an invoice
• Subsequent to receipt of invoice a series of falsified emails were then sent between these two employees
• Legitimate invoice previously received from a legitimate supplier for $230k but now with altered payment details
• Payment approved and processed
• Bank (fraud section) advising that payment had been made to an account with potentially fraudulent activity
• One word different in email address (architecs versus architects) being incorrect
• The emails contains formatting and grammatical errors not consistent with their usual style. They make claims of a suspicious nature. A query of this email directed to either employee of the group would likely have detected the fraudulent activity.
CASE STUDY F

> 1.5 million pounds
  • Overseas client transferring funds
  • Client emails hacked
  • Changed banking instructions
  • Bank did not confirm details verbally
  • Transfer was made
  • Bank responsible
Managing the fall out

Consideration
• Need a policy/risk plan
• Contact authorities
• Employee counselling
• Termination of employment?
• Implement/monitor control systems
• Education
• Purchase cybercrime insurance;
• Engage a Cyber Security Professional to review the security of your systems;
• Educate staff on cybercrime and encourage them to remain vigilant in regard to the risks around emails requesting payment or containing links; and
• Strict use of only official email addresses by all Directors for conducting of entity related business.
• Back up data

Recommendations