Cybersecurity Threats, Trends, and Strategies

ICCCFO Conference – Spring 2018
Cyber Risk Trends and Threats
Cyber Risk Trends

- Hackers love what small businesses have to offer!!!
  - Companies with 1 – 500 employees are largest targeted segment for cyber attacks*
  - Many are less equipped to protect against an attack
- Phishing and spam have continued to trend upward, most opportunistic attacks
- Digital extortion

*Symantec 2017 Internet Security Threat Report
Passwords

- 81% of hacking-related incidents leveraged the use of stolen and/or weak passwords (63% previous year)
  - Tricking victims to disclose password
  - Default credentials
  - Common passwords
  - Data breaches (Yahoo, LinkedIn)

Verizon 2017 Data Breach Investigations Report
Internet of Things (IoT)

● All things physical connected to the Internet
● New platforms create new cyber attack opportunities
  • Smart home devices (e.g., security systems, thermostats, lighting)
  • Embedded devices (e.g., DVRs, smart TVs, webcams, wireless access points, digital assistance, smartphones, printers, routers)
  • Automobiles, robotics, cloud pets, vacuum cleaners, pacemakers
  • ATMs, electronic signs
Cyber Threats – Email Scams
Cyber Threats – Email Malware Scams

● Sender is spoofed to be a known entity (i.e., Google, Microsoft, FedEx, IRS, FBI, Help Desk, CFO, Netflix)

● “Most of us are not suspicious of Word, Excel, or Adobe files

● Attachment executes script (i.e., PowerShell, JavaScript, Macros) to download malware (i.e., keylogger, ransomware)
Cyber Threat Trends – Macro Malware

Dear Kevin,

Please see the attached Word Document …

Best Regards,
ACME Company
Cyber Threat Trends – Macro Malware
## Cyber Threats – Email Malware Scams

### Top 10 malicious file extensions, January – September 2017

<table>
<thead>
<tr>
<th>File Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office</td>
<td>38%</td>
</tr>
<tr>
<td>Archive</td>
<td>37%</td>
</tr>
<tr>
<td>PDF</td>
<td>14%</td>
</tr>
<tr>
<td>Other Ext.</td>
<td>6%</td>
</tr>
<tr>
<td>Binaries</td>
<td>4%</td>
</tr>
<tr>
<td>XML/HTML/JS</td>
<td>1%</td>
</tr>
<tr>
<td>Apple</td>
<td>0%</td>
</tr>
<tr>
<td>Image</td>
<td>0%</td>
</tr>
<tr>
<td>Scripts</td>
<td>0%</td>
</tr>
<tr>
<td>Android</td>
<td>0%</td>
</tr>
</tbody>
</table>

Source: Cisco Security Research
Cyber Risk Trends – Business Email Compromise (BEC) Scams

- Attacker targets executive manager or business owner
- Attacker gains access to victim’s email account or uses a “look-alike” domain to send a message tricking an employee into performing a wire transfer
- Difficult to detect because email does not contain a malicious attachment or URL
From: [redacted]
Date: March 23, 2016 at 10:25:39 AM CDT
To: [redacted]@law.com
Subject: Wire Payment

Mark,

Are you in the office? I'm in a contract meeting til 5pm and i need you to take care of an invoice payment before the cutoff time today.

I'm very busy, Email me.

Chairman Emeritus

[redacted]

Phone [redacted]

Fax [redacted]

[redacted]
Cyber Risk Trends – Business Email Compromise (BEC) Scams

- Average payout for a successful BEC attack is $140K US
- The FBI urges businesses to adopt two-step or two-factor authentication for email

Trend Micro Security Predictions for 2018
Ransomware

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ~ 415 USD.
Your Bitcoin address for payment: 1LyjW9wyajpS3j9RitZDip6cDcZ7jMG5

You can also make a payment with PaySafeCard or Ukash.
In case of payment with PaySafeCard or Ukash your total payment is £ 400.

Payment verification may take up to 12 hours.

Support
Message Center

Try to decrypt your file here
You can test the decryption service once for FREE.
Case Study – Targeted Phishing Attack
Case Study – Targeted Phishing Attack

Someone has your password

Hi John,

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
- Saturday, 19 March, 8:34:30 UTC
- IP Address: 134.249.139.239
- Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.
Case Study – Targeted Phishing Attack
Case Study – Targeted Phishing Attack

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQCAytYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xlXNlc3NvbnRlbnQuY29tLy1RZVlpbHJkVGp2WS9BQUFB...

Someone has your password!

Hi John,

Someone just used your password to try to sign in to your Google Account john.potato@gmail.com.

Details:
- Date: 19 March, 03:30 UTC
- IP Address: 134.248.139.239
- Location: Ukraine

Google stopped this sign-in attempt. We want to make sure you stay safe. If you're the one who tried to sign in, do nothing.

If you didn't try to sign in, choose an action:

- Change Password
- Report abuse

Best,
The Gmail Team

http://bitly.com/gblgo0k
Case Study – Targeted Phishing Attack

Fake Google Website
Strategies for Establishing a Cybersecurity Program
Cybersecurity Controls – Layered Defense

- Employ a data backup and recovery plan for all critical information
- Vulnerability management program – patch promptly
  - Operating systems (Microsoft, Linux, MacOS)
  - Applications and web plug-ins
  - Firmware and embedded devices (IoT)
- Use strong authentication (e.g., complex passwords, two-factor, multi-factor, biometrics)
Cybersecurity Controls – Layered Defense

- Encrypt your sensitive data
- Endpoint protection (i.e., malware protection)
  - Firewall
  - Remote access
- Log and monitor security events
- Don’t forget physical security
- Make people your first line of defense – training
Threat Intelligence and Collaboration

- Wipfli Website and Cybersecurity Newsletters
  - www.wipfli.com/cybersecurity

- Regulatory bulletins and alerts (US-CERT)

- Data breach intelligence reports (Verizon, Symantec)

- FBI (www.fbi.gov)

- NIST (www.nist.gov)

- Industry peer groups, conferences, webinars
External Dependency Management

- Must have a strategy to identify, monitor, and mitigate the risks of third-party relationships (based on complexity of the relationship)
- Due diligence for vendor selection
- Ongoing vendor monitoring program
  - It is important to ensure vendors have adequate controls for protecting customer information
  - It is important to understand what a breach at a vendor’s operation means to your institution – vendor responsibilities
Cyber Incident Management and Resilience

• Have enhanced incident response plans – tabletop testing
  • Have arrangements with vendors who can work with your institution to implement incident response—a proactive approach, not when an incident has occurred
  • Work with regional crime taskforces
  • Ensure plan includes how you will notify customers

• Ensure there is periodic tabletop testing of your incident response program

• Ensure employees know how and when to escalate an event—ongoing employee awareness program
Cybersecurity Testing/Training

- IT Risk Assessment
- Perimeter Vulnerability Assessment/Penetration Testing
- Internal Vulnerability Assessment
- Social Engineering Testing
  - Email spoofing
  - Pretext calling
  - Physical penetration
Questions
Contact Information

Mark Scholl
Partner
Wipfli LLP
815.626.1277
mscholl@wipfli.com

Certified Ethical Hacker (CEH)
Certified Information Systems Auditor (CISA)
Certified Information Systems Security Professional (CISSP)
Microsoft Certified Systems Engineer (MCSE)