The Evolving Cyber Threat Landscape and How to Defend Against it

Tom Scarborough
Sr. Director, External Security Programs
August 18, 2020
Today’s Agenda

• Introduction and Overview

• Top Cyber Security and Fraud Threats
  – Business Email Compromise
  – Ransomware

• Best Practices on How to Combat Each

• Discussion and Q&A
Ever Changing Threat Landscape

Source: https://www.idc.com/mea/events/64869-cybersecurity-day-2017
It’s a Business…

The threat from “hackers” has expanded beyond opportunistic individuals using common techniques…to nation-state actors and professional criminals who are building and running large criminal organizations…
And we’re fighting for the same resources

Network Administration, Programming

Must have at least 10 years experience working with an above field, not a combination of fields. This is not negotiable. Must have at least five years experience working in a team-based cooperation environment. We don’t want freelancers. Must have strong work ethics and a willingness to work full-time for this organization. Life’s too short not to be rich. Must be able to bring innovative approaches to the operations and think out-the-box regularly. Must have a very good ability to document your workflow and formulate articulate reports on your duties. Candidates with multilingual skills were desirable. Must have a winning attitude.

The Hackers Playbook
Common Tactics Used by Cyber Criminals

- **Phishing attacks**
  - Email campaigns crafted specifically for a target. Often contain links directing recipients to malicious sites or attachments infected with malware.

- **Unsecured wireless networks**
  - If attackers are able to gain unauthorized access to a wireless network, they can observe traffic, data, and deny services to legitimate users.

- **Removable media**
  - USB devices can easily introduce malware into an information system.

- **Mobile devices**
  - Rogue or modified apps can be downloaded by unsuspecting individuals, opening up the mobile device to the threat.

- **Malicious web components**
  - If an unsuspecting individual visits a malicious web page, he can possibly make his systems or networks vulnerable or lose sensitive information.

- **Viruses and malware**
  - Tools used in order to launch certain types of attacks. Many of these tools are openly available on the Internet.

---

**Social Engineering**
The art of manipulating people so they give up confidential information
Business Email Compromise (BEC)
Business Email Compromise (BEC)

Compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds

The History of BEC:

• Became prominent in ~ 2012 - 2013
• Used to primarily target bank employees
• Saw a significant shift in 2015/2016 timeframe to target employees of the victim organization
• Many new “flavors” added in recent years
Business Email Compromise (BEC) – Social Engineering

BEC Overview:

• Used to obtain access to a business email account and imitate the owner’s identity, in order to defraud the company and its employees, customers or partners.

• Focuses efforts on employees with access to company finances, payroll data and other personally identifiable information.

• Fraudulent request comes from a compromised executive’s email account. Email address closely resembles a familiar one: johnasmith@gmail.com vs johnncsmith@gmail.com

• Tactics:
  – Sense of urgency
  – Use rules to forward emails to hidden folders
  – Wait until executives are on vacation or traveling on business
  – Use fake chains using subject lines with “Re:” or “Fwd:”. This technique grew more than 50% year over year.¹

BEC losses grew by 37% in 2019 alone, accounting for 40% of total cyber crime losses.

¹Proofpoint.(2018).The Human Factor Report 2018
Business Email Compromise: How it Happens

**Step 1: Identify a Target**
Organized Crime groups target US and European businesses, exploiting information available online to develop a profile on the company and its executives.

**Step 2: Grooming**
Spear phishing emails and/or telephone calls target victim company officials (typically an individual identified in the finance department.)
Perpetrators use persuasion and pressure to manipulate and exploit human nature.
Grooming may occur over a few days or weeks.

**Step 3: Exchange of Information**
The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

**Step 4: Wire Transfer**
Upon transfer, the funds are steered to a bank account controlled by the OC group.

---

FIFTH THIRD BANK
**Real life examples**

Hi Jason,
Please kindly provide me with the ending balances in all my accounts as of yesterday and current balances for today. I have been very busy all day. Please regard this note in timely manner.

Hello Kelly,
Hope all is well with you and that you had a wonderful Independence day, I have some transactions which I will need you to complete today. I want you to update me with balance in my account because I need to complete a wire transfer to another institution for an urgent business purpose. Kindly email me the information required for outgoing Domestic wires. I also like to inform you that we can only get in touch through the email for now because I am meeting at the moment.

Kindly email me back with information you will need to complete an international wire transfer with the balance in all my accounts. Am under the weather and I am on my way going to see my doctor.

William,
I am very busy with doctor at the moment, please go ahead and raise the funds and make the arrangement for the wire to go out this morning. I will see you on Friday.

I have some transactions which I will need you to complete today. We need to complete a wire transfer to another institution for an urgent business purpose. I will be very busy all day in a meeting and my phone will not be available but I will frequently check my email for your response.

Good Morning,
How are you doing today? Please kindly let me know the balance in all my accounts as of today and what information do you need to send out domestic and International wire. I will be very busy all day today. Kindly respond to my email frequently.

Thanks.

---

**Fifth Third Bank**
BEC – The Impacts…

Since May 2013… over $26 Billion in losses have been reported!

- The FBI reports that between May 2018 and July 2019, there was a 100% increase in identified global exposed losses. The scam has been reported in all 50 states and in 177 countries.

- Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to at least 140 countries.

Best Practices to Combat BEC:

1. Leverage Dual Approval capabilities whenever possible

2. Know your customer and never accept requests for payments through email or other similar channels
   • Verify legitimacy of payment requests leveraging known good contact information
   • Never trust information received via email

3. Monitor your accounts regularly

4. Educate your employees

5. Use Multifactor Authentication capabilities provided by email providers when possible

6. Limit information shared on social media about your employer and your role

7. Ensure policies and procedures are being followed

8. Leverage appropriate security tools to protect your environment (anti-malware, web proxy, etc.)
Ransomware
Ransomware- Aggressive Rise in the Attacks over the Last 2 years

Causes and Costs:

• TSMC iPhone Chip manufacturer – **System vulnerability (supplier installed infected software on machines w/out running antivirus):** $250M+ in damages

• City of Atlanta – **Vulnerability, brute-force attack to guess weak passwords:** $17M ($6M in software upgrades and security contracts + $11M in new desktops, laptops, smartphones & tablets)

• Baltimore – **Phishing:** $18M+ (10M recovery + 8M in revenue lost, no ransom paid)

• Hancock Regional Hospital- **Vendor login credentials stolen:** $55K paid in bitcoin ransom
Attackers Target Perceived “Soft Targets”

From the Media… All From One Random Week:
• IT Services Giant Conduent Suffers Ransomware Attack, Data Breach
• Ransomware Attack Exposes 1.5TB of Stolen Aerospace Data
• BREAKING: Columbia student information at risk in ransomware attack
• Honda investigates possible ransomware attack, networks impacted
• Elexon files posted online following May’s ransomware attack

And Even More Recently…
• Cognizant
• Garmin
• Carlson Wagonlit

Notable Data Points:
• In 2019, 205,280 organizations submitted files that had been hacked in a ransomware attack — a 41 percent increase from the year before
• From January 2019 through October 2019, over 140 local governments, police stations and hospitals have been held hostage by ransomware attacks
• Since 2013, at least 169 state and local governments have been impacted by ransomware
• We’ve seen an increase in supply chain attacks with some indication that some have been targeted
• Threat actors continue to evolve tactics with increase in stealing of data for threat of release and public shaming
Associated Ransoms Increase Significantly

By The New York Times | Source: Coveware
Best Practices to Defend Against Ransomware:

• Have a sound data backup plan - Maintain up-to-date backups and store offline
• Test your backup plan!
• Segment the network
• Perform regular penetration testing as well as enterprise-wide risk analysis
• Keep anti-virus and anti-malware systems current
• Maintain a diligent Vulnerability Management program
• Filter what comes in and what goes out (proxy)
• End user education on phishing /suspicious emails
• Develop and implement disaster response and recovery procedures
• Exercise and Test!
Cyber Insurance

Cyber insurance is available and can provide services that include:

• Incident response services: Breach coach, legal fees, forensics, notification costs, credit monitoring, public relations

Cyber insurance can provide protection for exposures that include:

• Ransom/extortion
• Business interruption/loss of profits
• Social engineering
• Network liability: Failure to prevent transmission of viruses, etc.
• Privacy liability: Failure to protect private information
• Regulatory proceedings
• Media liability

The Fifth Third Insurance Agency can provide further information and advice on this topic*

Fifth Third Insurance is the trade name used by Fifth Third Insurance Agency, Inc. Insurance products and services are offered through Fifth Third Insurance Agency, Inc., which is a wholly-owned, non-bank subsidiary of Fifth Third Bank, National Association. Banking and insurance decisions are made independently and do not influence each other. Insurance products are not FDIC insured, not guaranteed by a bank and are underwritten by unaffiliated, third party insurance carriers. Insurance products are not offered in all states. Please consult with a Fifth Third Insurance Professional.
Appendix
Business Checklist
Just as the Fifth Third Bank team is committed to protecting both our clients and the enterprise, our business clients have similar obligations. Here are some highly effective actions businesses can take to protect their own network, company, and clients.

<table>
<thead>
<tr>
<th>Protect the Money</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Utilize two-factor authentication sign on</td>
</tr>
<tr>
<td>• Use TM Products and Services like Positive Pay</td>
</tr>
<tr>
<td>• Consider adhering to an FBI recommendation for small businesses to dedicate one computer to online banking activity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secure Your Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Create secure passwords</td>
</tr>
<tr>
<td>• Don’t reuse your passwords. Use a unique password for each account</td>
</tr>
<tr>
<td>• Avoid sharing</td>
</tr>
<tr>
<td>• Create passwords that are long and strong</td>
</tr>
<tr>
<td>• Avoid public Wi-Fi networks</td>
</tr>
<tr>
<td>• Separate work and personal information and actions</td>
</tr>
<tr>
<td>• Surf safely – consider the use of a web proxy</td>
</tr>
<tr>
<td>• Never enter personal or customer-specific information into a public computer.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Practice Good Security Hygiene</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Use an up-to-date browser and apply patches regularly.*</td>
</tr>
<tr>
<td>• Install and regularly update security tools (anti-virus, anti-spyware, firewalls, etc.)*</td>
</tr>
<tr>
<td>• If your company has internet sites, incorporate intrusion detection and vulnerability management tools.</td>
</tr>
<tr>
<td>• Turn off and remove services that are not needed, like USB drives.*</td>
</tr>
<tr>
<td>• Use a mail service that blocks or removes email file attachments commonly used to spread viruses.</td>
</tr>
<tr>
<td>• Ensure only approved company applications are deployed and keep them patched.*</td>
</tr>
<tr>
<td>• Download the free Trusteer Rapport software available on our site to add another layer of security.</td>
</tr>
<tr>
<td>• Install pop-up blockers on your system.</td>
</tr>
<tr>
<td>• Make sure your networking equipment and computers are supported by the manufacturer</td>
</tr>
<tr>
<td>• Dispose of your network, computer and mobile devices safely</td>
</tr>
</tbody>
</table>

*indicates basic system hygiene
Business Checklist, cont’d

### Implement Security Measures

- **Restrict Access to Information**
  - Individuals with access to personal information should have the minimum necessary to perform duties
- **Have a sound Back Up Plan and regularly back up critical data**
- **Implement procedures for verifying urgent wire transfer orders – include dual approval**
- **Minimize the number of individuals who can approve or conduct wire transfers or ACH payments**
- **Be aware of third-party risk – You’re only as strong as your weakest third party**

### Be Prepared...It’s not a matter of if...

- Retain an expert cybersecurity firm that can:
  - Provide initial diagnostics of risks and provide regular checkups
  - Perform “white hat” simulated cyber attack tests to identify weak points
- Consider cyber insurance coverage to cover:
  - Breach response
  - Cyber extortion
  - Network interruption
  - Data restoration
  - IT Forensics
- Adopt an Incident Response Plan and test it!
- Manage a data inventory
- Identify the organizational “crown jewels”
- Establish a procedure employees should use if they think their computer may be infected
- Make sure all employees use good security habits. Establish a security awareness program.
- Regularly check for external accounts imitating the company or people within the company.
Any questions?

Thank you!!