FIFTH THIRD BANK

The Evolving Cyber Threat Landscape:
How to Combat It Through Awareness

September 20, 2019

Grant Jacoby
SVP – Information Security Strategy and Innovation

Agenda

- Welcome and Introduction
- What We're Up Against – The Evolving Cyber Landscape
- Specific Threats We Face
- Treasury Management Solutions And Other Best Practices
- Fifth Third Cyber Defense and the Fifth Third Cyber Fusion Center
- Q & A

What We're Up Against:
The Evolving Cyber Landscape

The Web

Intricate organic linking of sites for information sharing

VS

Things spiders weave with aim of capturing prey

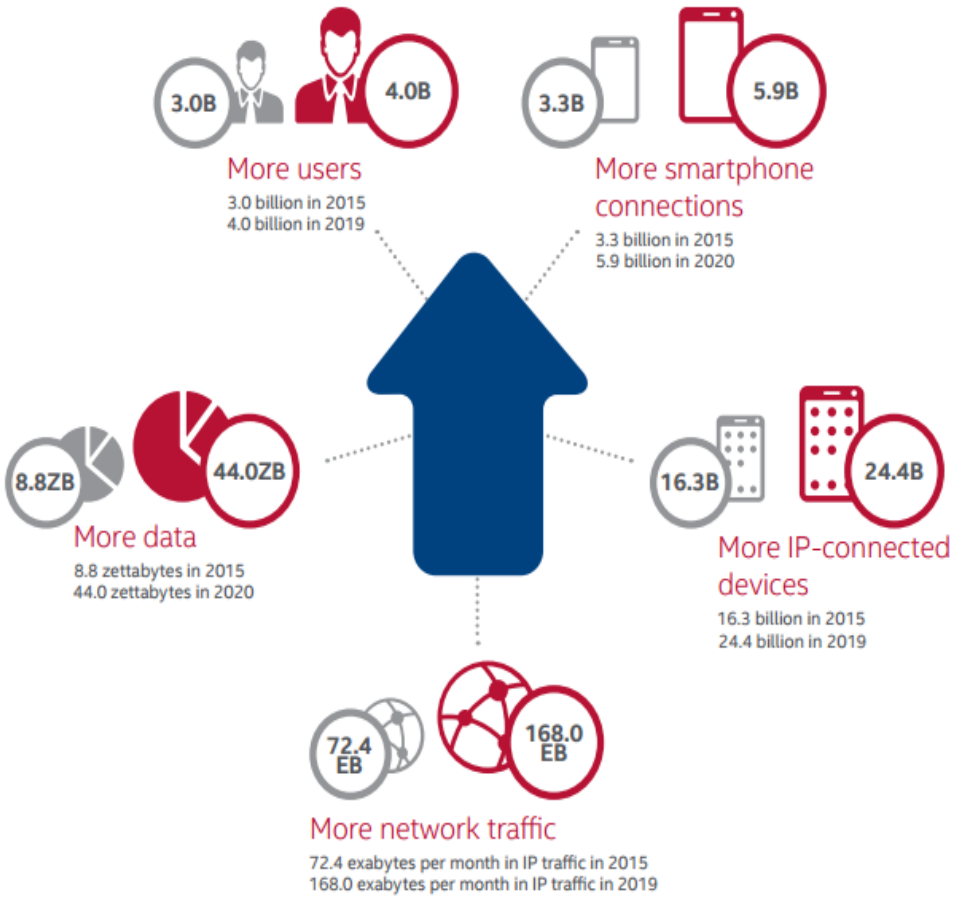
The Internet was built for connectivity, speed and technical innovation – not security and protection.

For criminals, the digital world has become a low-risk, high-reward offering with a borderless reach, assured anonymity and defenseless victims who can't find them.

As society innovates, so do the bad actors.

Anything connected to the network is a target for hackers and exploitation

The Growing Cyberattack Surface



Source: McAfee Labs, 2015

The New York Times

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

By Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber Sept. 7, 2017

Equifax, one of the three major consumer credit reporting agencies, said on Thursday that hackers had gained access to company data that potentially compromised sensitive information for 143 million American consumers, including Social Security numbers and driver's license numbers.

Huffington Post

MyFitnessPal Security Breach Affects 150 Million Users, Under Armour Reports

By Carla Herreria 03/29/2018 08:59 pm ET

Hackers breached MyFitnessPal, a popular calorie-counting app and website, and acquired private data from about 150 million users.

The New York Times

All 3 Billion Yahoo Accounts Were Affected by 2013 Attack

By Nicole Perlroth Oct. 3, 2017

Verizon Communications, which acquired Yahoo this year, said on Tuesday that a previously disclosed attack that had occurred in 2013 affected all three billion of Yahoo's user accounts.

Uber Data Breach Exposed Personal Information of 20 Million User

By BLOOMBERG Updated: April 12, 2018 3:02 PM ET

A data breach in 2016 exposed the names, phone numbers and email addresses of more than 20 million people who use Uber Technologies Inc.'s service in the U.S., authorities said on Thursday, as they chastised the ride-hailing company for not revealing the lapse earlier.

Increasing in Numbers, Sophistication, and Destructive Nature

70% of ransomware attacks targeted small/medium-sized businesses in 2018

Global ransomware attacks could **cost $193 billion** [5]

In 2018 a full 43% of login attempts worldwide were actually fraudulent [14]

12,449 data breaches confirmed in 2018, a 424% increase over previous year,[11] **and second-most active year for data breaches**

62% of business users report they have access to company data that they probably shouldn't see[15]

Organized criminal gangs now joined by North Korea in **targeting banks**[11]

Cyber criminal **extortion gangs promise salaries averaging $360,000 per year** to accomplices [19]

U.S. Government has identified cybersecurity as "one of the most serious economic and national security challenges we face as a nation"

6 months time to breach discovery

Over 80% of all phishing attacks targeted victims in US. [17]

The average total organizational **cost of a Data Breach** against a US company in 2017 was **$7.35 million** [6]

A malicious insider causes 90% of a business's networks to fail.[13]

Hackers Attack **Every 39 Seconds**[12]

The largest ever DDoS attack in history reached 1.7 Tb per second, in 2019.[21]

93% of data breaches occurred in **minutes or less** [4]

78% of people claim to be aware of the risks of unknown links in emails. And yet they **click anyway**.[10]

BEC Attacks increased by 130% in 2018 [3]

Half of the 2018 cyber-attacks involve supply chain partner [9]

The number of **email phishing attacks skyrocketed 250%** during 2018 [18]

It's a Business…

Hacker threat has expanded beyond opportunistic individuals using common techniques…to nation-state actors and professional criminals

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.

Source: Matthew J. Schwartz, (2019) “Cybercrime Gangs Advertise Fresh Jobs, Hacking Services”, bankinformationsecurity.com

Cybercrime costs are unprecedented

From the start of 2017 through the first half of 2018, cybercrime groups generated billions of dollars worth of profit and have caused gross losses of more than $1trillion.[1]

$1,000,000,000,000

61% of data breach victims in 2016 were businesses with less than 1,000 employees.[2]

Many small financial firms have the "wealth" commensurate with small or medium enterprises but typically don't have the same levels of security…making them lucrative targets for hackers.

Individuals with over $5MM in net worth will have a nearly 90% chance of experiencing cybercrime loss with an average amount of $75k by 2020.[3]

[1]*Cyber risk is growing. So how can we prepare. (1/17/18). World Economic Forum. www.weforum.org*
[2]*Verizon. (2017) Verizon 2017 Data breach Investigation Report*
[3]*Rubica*

The Cyber Threat Landscape:
Specific Threats We Face

The Hackers Playbook

Paths or tools that adversaries use to attack their target

Phishing attacks	Unsecured wireless networks	Removable media	Mobile devices	Malicious web components	Viruses and malware
Email campaigns crafted specifically for a target. Often contain links directing recipients to malicious sites or attachments infected with malware.	If attackers are able to gain unauthorized access to a wireless network, they can observe traffic, data, and deny services to legitimate users.	USB devices can easily introduce malware into an information system.	Rogue or modified apps can be downloaded by unsuspecting individuals, opening up the mobile device to the threat.	If an unsuspecting individual visits a malicious web page, he can possibly make his systems or networks vulnerable or lose sensitive information	Tools used in order to launch certain types of attacks. Many of these tools are openly available on the Internet.

Social Engineering

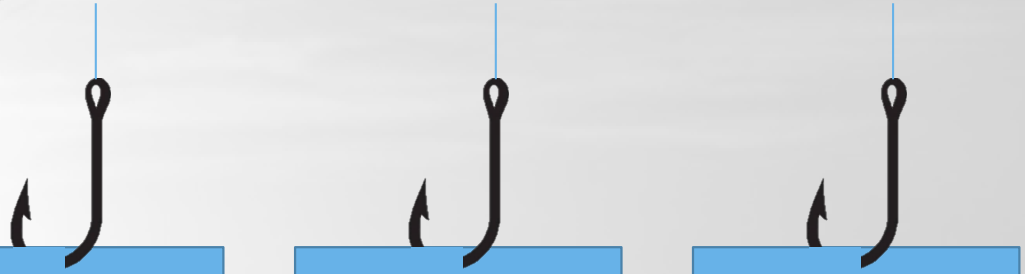
The art of manipulating people so they give up confidential information.

Hacker Playbook – Phishing

Cheap cost and high success rate drives the cybercriminals' favored method-of-choice

Results of successful phish:

- Download malware
- Remotely control your computer
- Load ransomware
- Account takeover
- Alter/delete files
- Send emails on your behalf
- Direct you to illegitimate websites
- Steal personal information



91%

Of successful cyber attacks start with phishing[1]

66%

Of all malware infections were installed via malicious email attachments[2]

1:14

Employees get tricked and 25% of those get duped more than once.[2]

One successful phishing event is one too many

[1]*91% of Cyber Attacks Start with a Phishing Email. (7/26/17). DigitalGuardian, www.digitalguardian.com*
[2]*Verizon. (2017) Verizon 2017 Data breach Investigation Report*

Social Media – a hacker's favorite target

600,000 Facebook accounts are compromised every single day.[1]

- Users of social media such as Facebook, Instagram, and Snapchat face a 46% higher risk of account takeover and fraud than those not active on social networks.[2]
- Pharming/Typosquating/Spoofing – Tricking users into believing they are interacting with legitimate sites and services.
  - In 2010 the official site of the 2018 Winter Olympics was registered. Since then more than 100 similar domains have been registered, only 3 were legitimate.[3]
  - Suspiciously registered domains can outnumber brand-registered domains[3] **20:1**

[1]Dascalescu.A, (3/29/18). 10 alarming Cyber Security Facts that Threaten Your Data. www. heimdalsecurity.com
[2]Javelin Strategy and Research. (2017). 2017 Identity Fraud Study. www.javelinstrategy.com
[3]Proofpoint.(2018).The Human Factor Report 2018

Hacker Playbook – Social Engineering

Exploit our natural curiosity, desire to be helpful, love of a good bargain, and our time constraints

Business Email Compromise

- 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 vs johncsmith@gmail
- Tactics:
  - Sense of urgency
  - Use rules to forward emails to hidden folders
  - Wait until executives are on vacation
  - Use fake chains using subject lines with "Re:" or "Fwd:". This technique grew more than 50% year over year.[1]
- Other variations:
  - Impersonation of supplier with longstanding relationship

The number of attackers using legal language increased 1,850% year over year.[1] The subject "lawyers call" was the most popular.

Human Nature is the Vulnerability

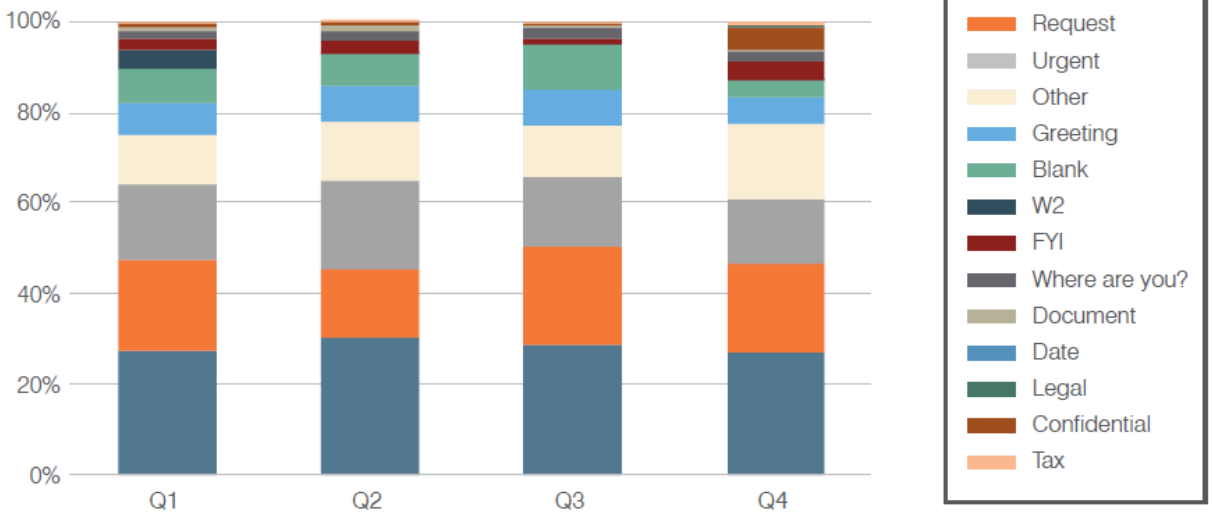
Business Email Compromise (BEC) attacks jumped by 80% over the past quarter.[2]

[1] *Proofpoint.(2018).The Human Factor Report 2018*
[2] *Townsend, K. (8/28/18). Email Impersonation Attacks Increase by 80%. Securityweek.*

BEC - Email Fraud

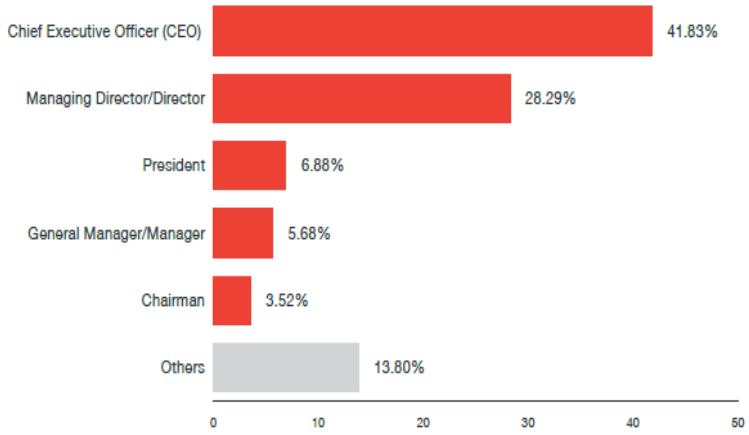
From: CEO
To: CFO
Subject: Payment

Top Email Fraud Subject Lines by Quarter[1]

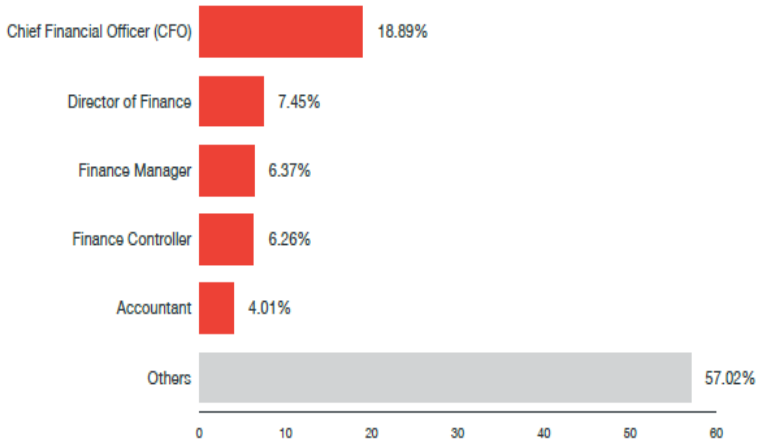


Distribution of most common email subjects in BEC attacks

Percentage of BEC attack attempts that spoof specific positions, 1H2017[2]



Percentage of BEC attack attempts that target specific positions, 1H2017[2]



[1] *Proofpoint.(2018).The Human Factor Report 2018*
[2] *Trend Micro. (2017). 2017 Midyear Security Roundup: The Cost of Compromise.*

FIFTH THIRD BANK

BEC Techniques

There are three different types of identity deception that criminals use to execute a BEC attack: spoofing, look-alike domains and display name deception.

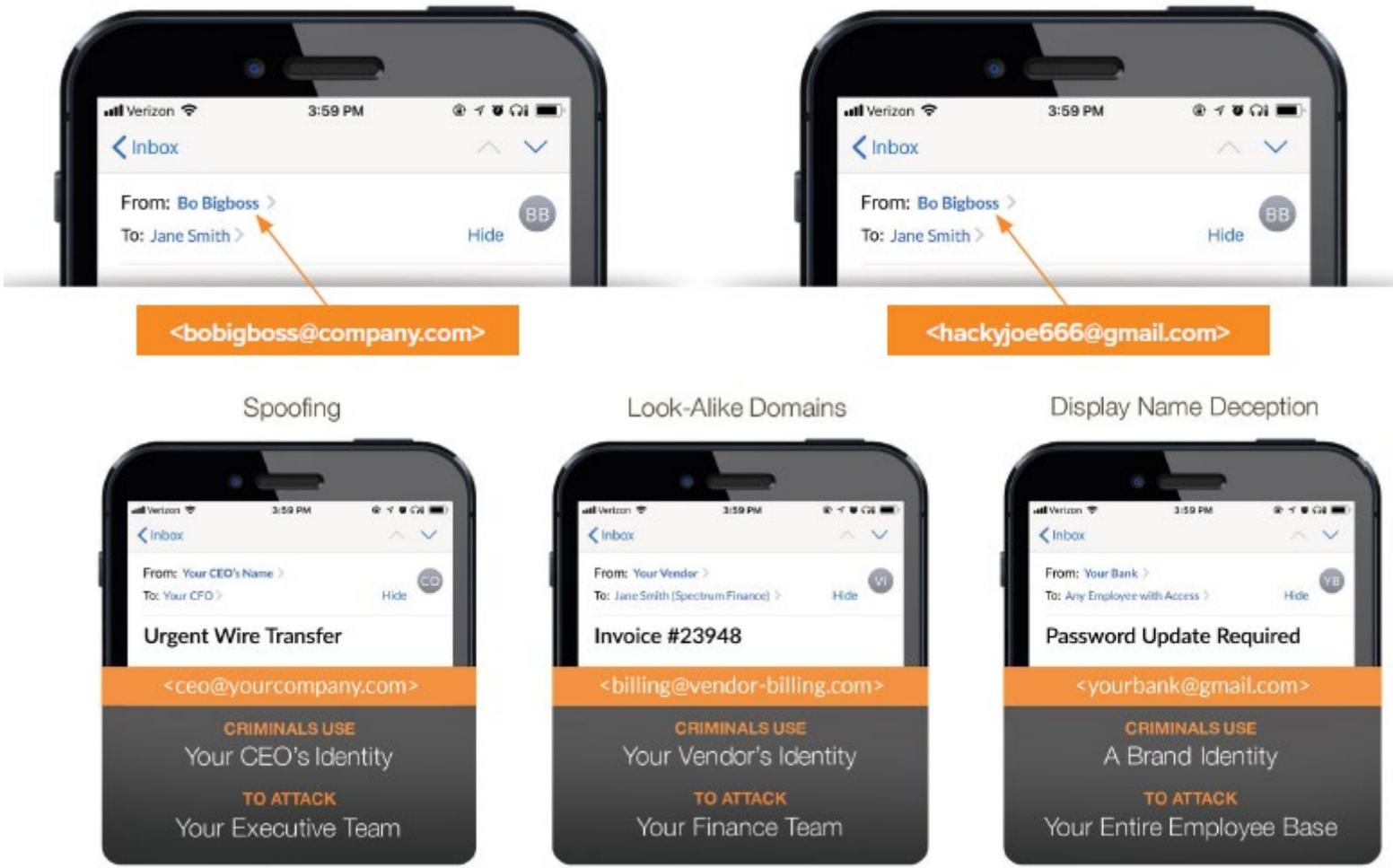


Image: https://www.agari.com/bec/education/business-email-compromise-attack-trends-report.pdf

BEC – The Impacts…

Since May 2013… over **$12 Billion** in losses have been reported!

The FBI reports that between December 2016 and May 2018, there was a 136% increase in identified global exposed losses. The scam has been reported in all 50 states and in 150 countries.

Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 115 countries.

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Jul 12, 2018

Alert Number
I-071218-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update and companion to Business E-mail Compromise (BEC) PSA 1-050417-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data for the time frame October 2013 to May 2018.

DEFINITION

Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) is a sophisticated scam targeting both businesses and individuals performing wire transfer payments.

The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

The scam may not always be associated with a request for transfer of funds. A variation of the scam involves compromising legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees.[1]

STATISTICAL DATA

The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between December 2016 and May 2018, there was a 136% increase in identified global exposed losses[2]. The scam has been reported in all 50 states and in 150 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers

Source: https://www.ic3.gov/media/2018/180712.aspx

Ransomware

Florida City to Pay $600,000 to Hackers After Ransomware Attack

FROM THE MEDIA: The Riviera Beach, Fla., city council agreed to pay $600,000 USD to decrypt its IT systems as part of a ransomware infection. The Palm Beach Post said the attack occurred on May 29 when a police department employee clicked a malicious link in an email. It was was unknown if paying the 65 Bitcoin ransom decrypted all of the hijacked data, but a city spokesperson told The New York Times: "We are well on our way to restoring the city system." He said that the city's website and email systems had been restored, in addition to finance-related systems. Since 2013, at least 169 state and local governments have been impacted by ransomware, according to Recorded Future.

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.

Protect the Money	
❑	Monitor accounts regularly – leverage push notifications
❑	Utilize two-factor authentication sign on
❑	Use TM Products and Services like Positive Pay
❑	Consider adhering to an FBI recommendation for small businesses to dedicate one computer to handle online banking activity.

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

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

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.

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 Bank provides access to insurance products through its subsidiary, Fifth Third Insurance. Fifth Third Insurance is the trade name used by Fifth Third Insurance Agency, Inc., a licensed insurance agency providing insurance services. Insurance products:

- Are Not FDIC Insured
- Offer No Bank Guarantee
- May Lose Value
- Are Not Insured by any Federal Government Agency
- Are Not a Deposit

Insurance products are not offered in all states. Please consult with a Fifth Third Insurance Professional.

Aggressive Rise Last 2 years

- Phishing
- System Vulnerabilities

Local Government Targeted Attacks

38
2017

21
Jan-Apr
2019

According to Recorded Future

Causes and Costs:

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

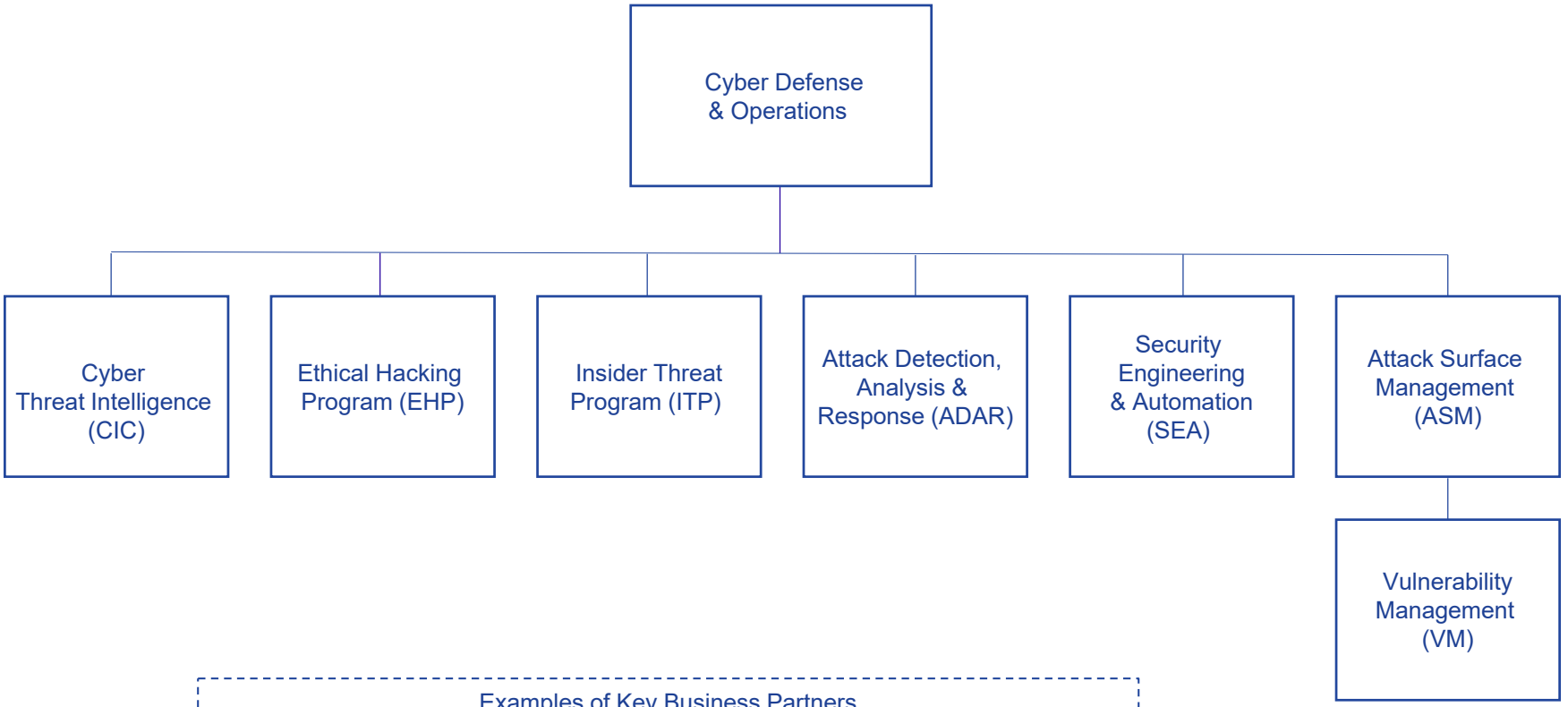
Image 1: Motormille2 via Wikimedia Commons/CC
Image 2: MalwareBytes (RobbinHood ransom note)

Defense Strategies

- Know the threat landscape
- Perform regular penetration testing as well as enterprise wide risk analysis
- Maintain up-to-date backups and store offline
- Keep anti-virus current
- Maintain diligent system/software patching practices
- Implement proper email filtering
- End user education on phishing
- Develop and implement disaster response and recovery procedures

Fifth Third Cyber Defense and the Fifth Third Cyber Fusion Center

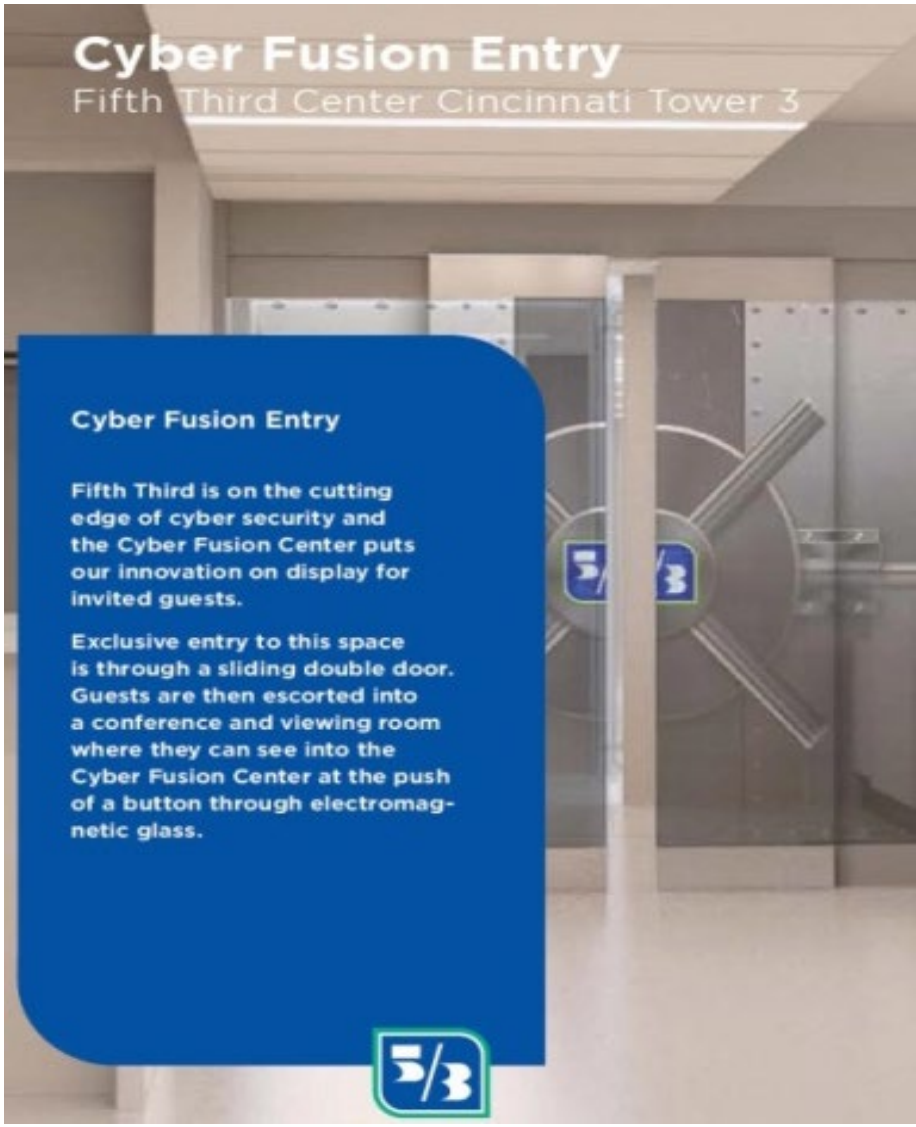
Cyber Defense & Operations



Actionable Intelligence Improves Time to Detect, Analyze, and React

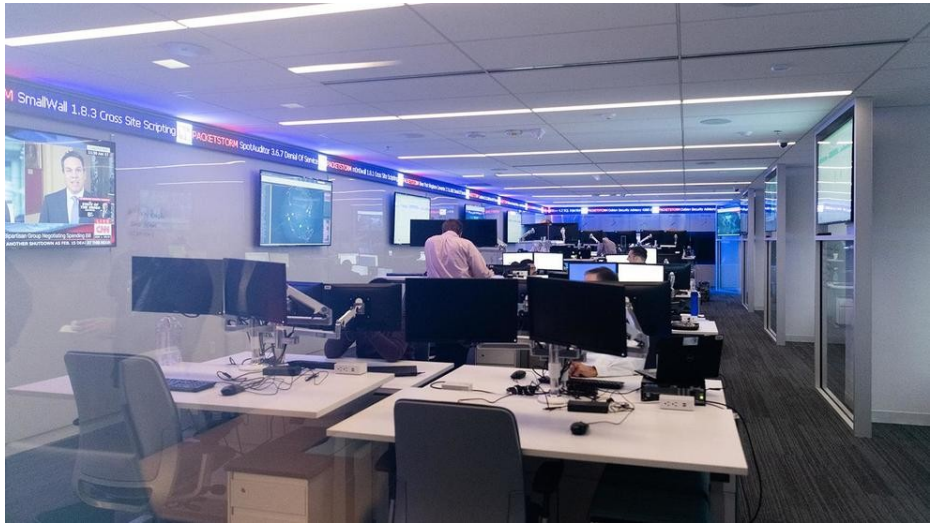
Centralization of cyber security

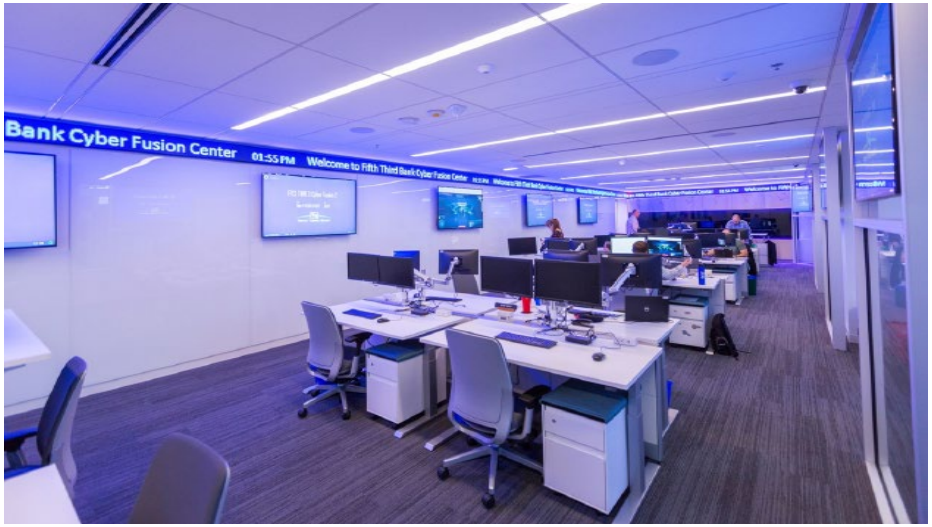
- Reduce risk by integrating all cyber security and fraud prevention functions into a single entity
- Cyber Fusion Center improves strategic, operational, and tactical effectiveness
- Consolidation and streamlining occurs across Bank security teams, including:
  - Fraud strategy
  - Loss prevention
  - Cyber defense
  - Financial crimes
  - Physical security
- Centralization better protects the bank and customers while improving efficiencies



The Fifth Third Cyber Fusion Center

In order to defend against today's ever-evolving cyber threat landscape, organizations must make calibrated investments at all levels of their cyber-security program. Nowhere is this concept exemplified more than in the Bank's New Cyber Fusion Center (CFC) that went operational in 1Q 2019





The CFC will provide a state-of-the-art operations center for teams to collaborate in real-time, co-located, with access to all of the security resources at the Bank's disposal.

Teams Staffing CFC Include:

Attack Detection Analysis and Response | Cyber Intelligence | Fraud Strategy | Fraud Prevention | Financial Crimes| Insider Threat | Vulnerability Management

Thank you for your time and interest!

Questions?