Strength in Security

Securing our Digital Future

Jenny Menna

January 10, 2018

usbank

Session goal and focus areas

- Session goal:
  - To gain an understanding of cybersecurity risk and how we can address it in the healthcare sector and in your personal lives.
- Focus areas:
  1. How has the cyber landscape changed?
  2. As threats grow, how can we mitigate risk?
  3. How do business leaders engage in what was historically a technical conversation?

What happened in an internet minute in 2018?

174K scrolling Instagram

973K Facebook logins

18M text messages

4.3M YouTube videos viewed

375K Apps downloaded

481K Tweets

187M emails sent

67 voice-first devices shipped

2.4M snaps created

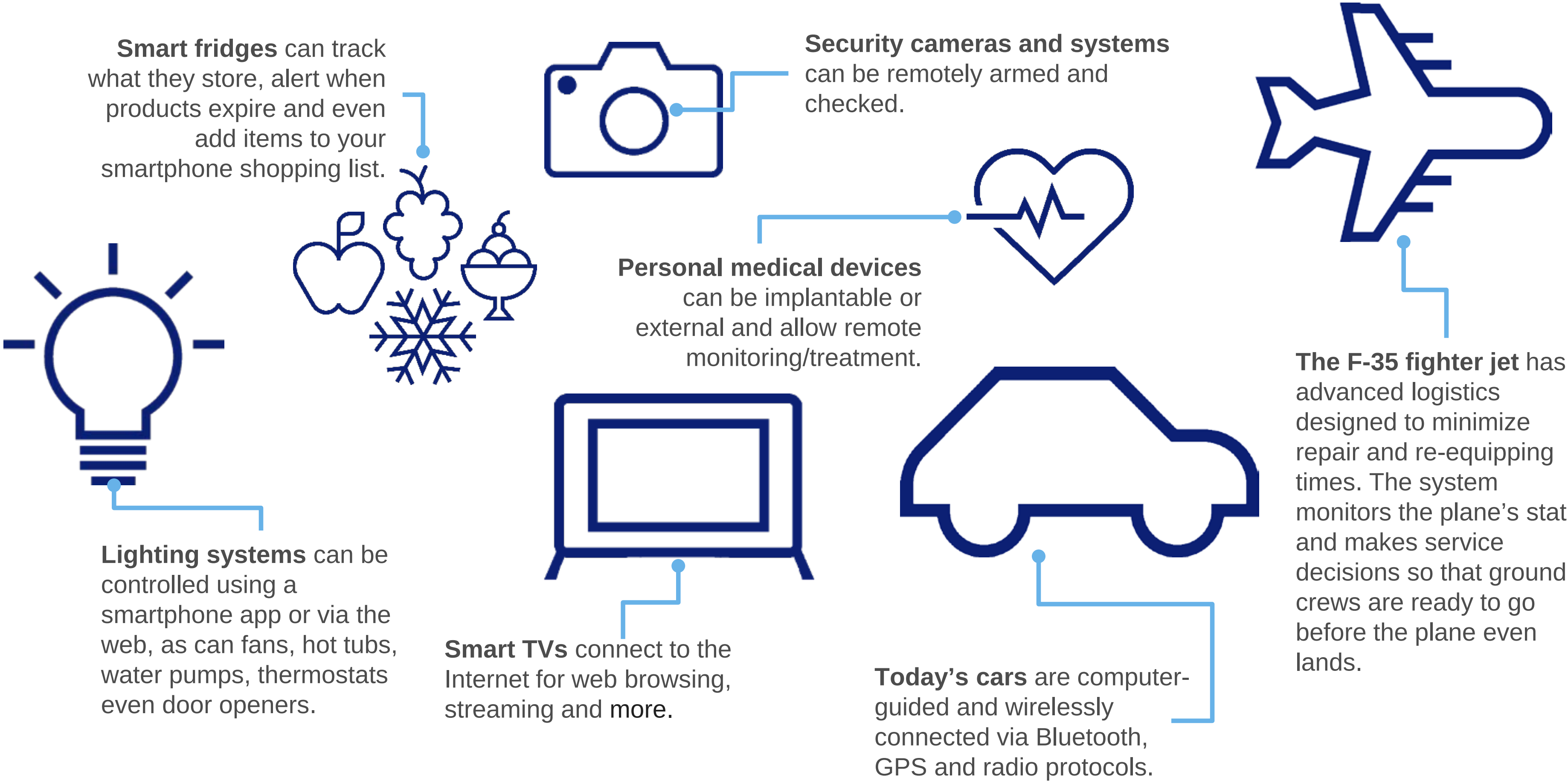
$863,000 spent online

266K Netflix hours streamed

3.7M Google search queries

Source: Data compiled by Lori Lewis and Chad Callahan of Cumulus Media
www.allaccess.com/merge/archive/28030/2018-update-what-happens-in-an-internet-minute

Cyber-physical "Internet of Things"



Smart fridges can track what they store, alert when products expire and even add items to your smartphone shopping list.

Security cameras and systems can be remotely armed and checked.

Personal medical devices can be implantable or external and allow remote monitoring/treatment.

The F-35 fighter jet has advanced logistics designed to minimize repair and re-equipping times. The system monitors the plane's status and makes service decisions so that ground crews are ready to go before the plane even lands.

Lighting systems can be controlled using a smartphone app or via the web, as can fans, hot tubs, water pumps, thermostats even door openers.

Smart TVs connect to the Internet for web browsing, streaming and more.

Today's cars are computer-guided and wirelessly connected via Bluetooth, GPS and radio protocols.

Source: Forbes, Vice, Cisco IBSG, University of Michigan, ABC News, Qmed, Network World

Money movement and technology innovation

Indications of our digital dependence in finance

U.S. GDP

19 trillion

~24% of global economic activity

U.S. debt

22 trillion

~115% of GDP

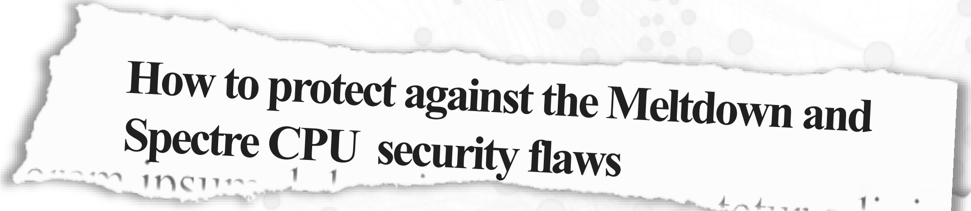
Daily payments via U.S. banking system*

15 trillion

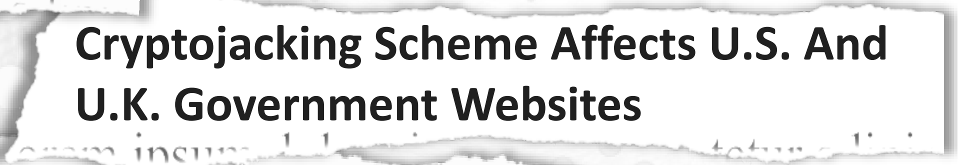
*intraday liquidity flows

Sources: Visual Capitalist, 2018: https://www.visualcapitalist.com/80-trillion-world-economy-one-chart/; Wikipedia, 2018: https://en.wikipedia.org/wiki/National_debt_of_the_United_States, Daily payments via US banking system: Federal Reserve Bank of New York, 2014

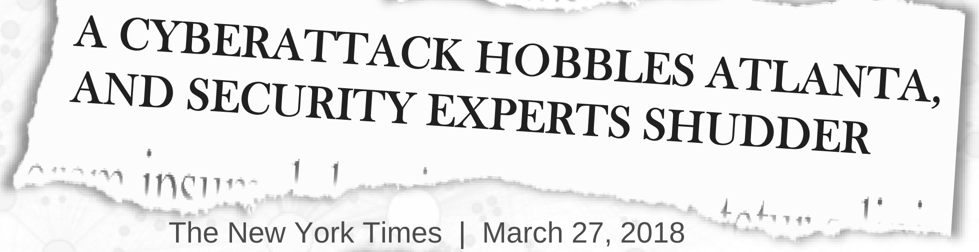
Top Headlines of 2018


How to protect against the Meltdown and Spectre CPU security flaws

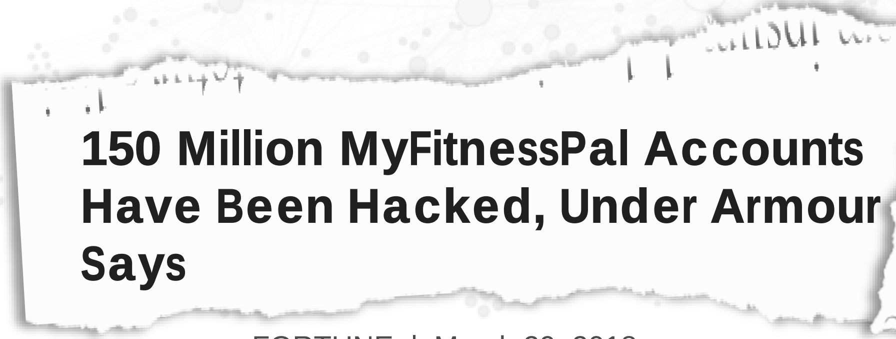
Tech Radar | January 4, 2018


Cryptojacking Scheme Affects U.S. And U.K. Government Websites

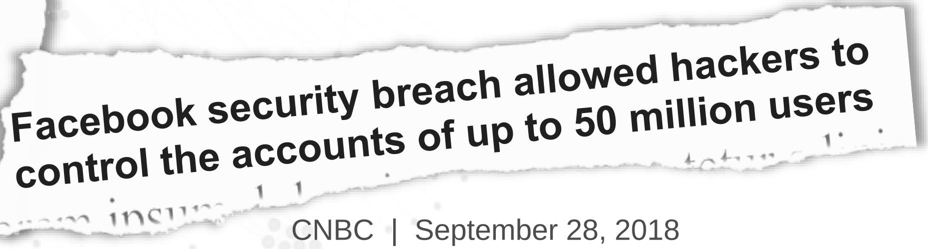
Nextgov | February 12, 2018


A CYBERATTACK HOBBLES ATLANTA, AND SECURITY EXPERTS SHUDDER

The New York Times | March 27, 2018


150 Million MyFitnessPal Accounts Have Been Hacked, Under Armour Says

FORTUNE | March 29, 2018


Facebook security breach allowed hackers to control the accounts of up to 50 million users

CNBC | September 28, 2018

Cost of cybercrime

$1.3 MILLION

Average cost per phishing/social engineering attack

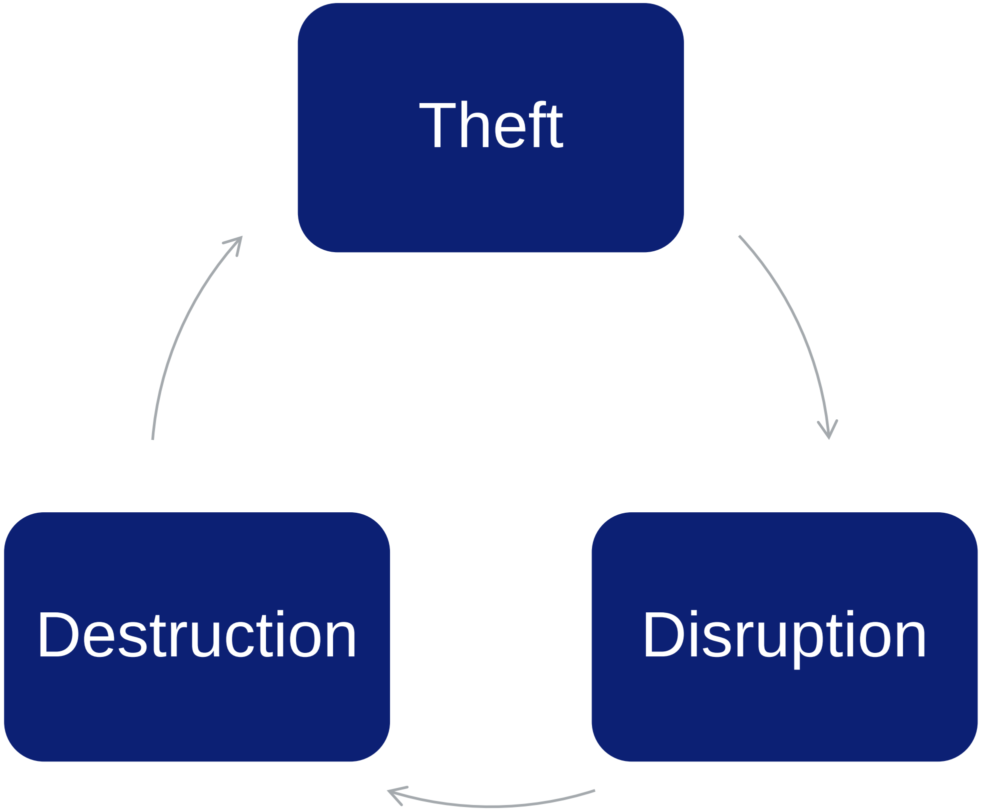
Gartner, Forecast: Information Security, Worldwide, 2014-2020, 1Q16 Update, May 10, 2016

Rapidly evolving threats—motivational shifts

Fraudsters

Hacktivists

Nation-States



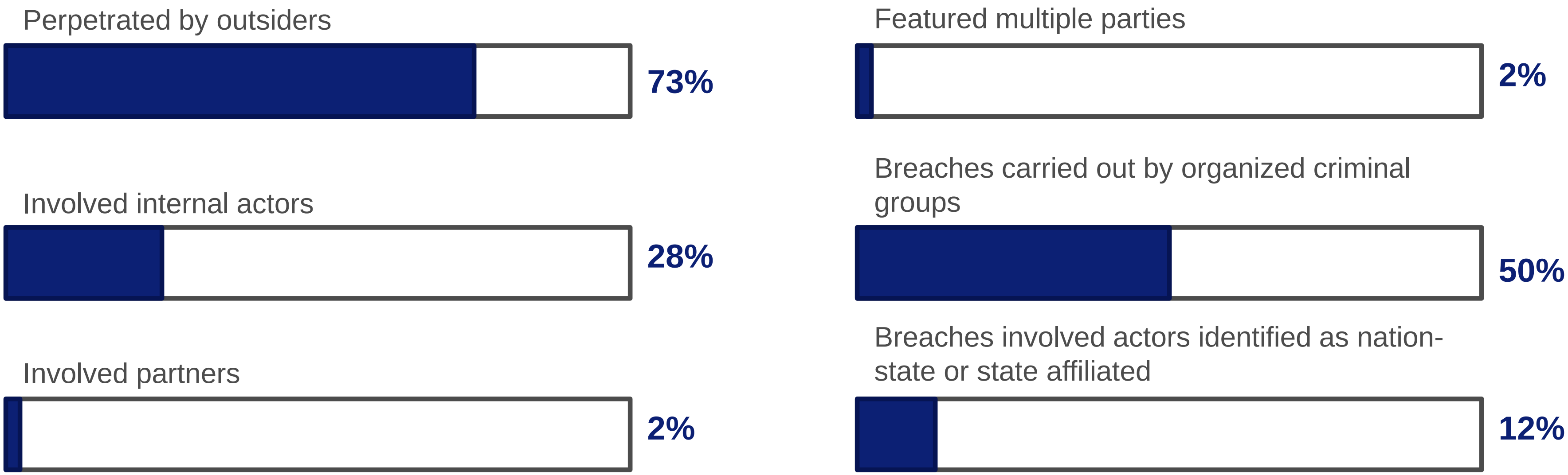
Theft

Disruption

Destruction

Who’s behind the breaches?

Breach: an incident that results in the confirmed disclosure —not just potential exposure — of data to an unauthorized party


Perpetrated by outsiders
73%
Involved internal actors
28%
Involved partners
2%
Featured multiple parties
2%
Breaches carried out by organized criminal groups
50%
Breaches involved actors identified as nation-state or state affiliated
12%

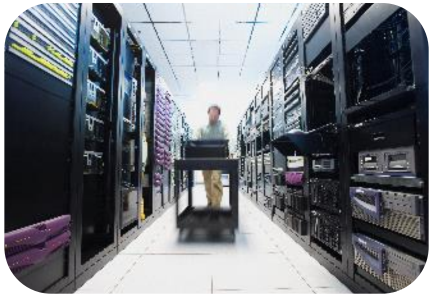
Source: Verizon 2018 Data Breach Investigations Report, 11th edition

Extremely organized crime

What does this operational model remind you of?

Criminal Organization									
Sales, Marketing and Licensing	HR Recruiting and Staff Mgmt	Technology Operations				Finance	Quality Assurance		
Affiliate programs	Fraudster University	Online Web Portals	Big Data Analytics	Hosting	Develop-ment teams	Money mules	Multiple language and regional support	24/7 Call Centers	Offshore QA teams

2019 industry predictions



Crypto-mining takes over as ransomware declines

Stricter **data protection policies** within companies

Increased **nation-state attacks** and surveillance on individuals

Multi-factor authentication will be norm for online transactions

More targeted **spear phishing**

Talks of global **cyberwarfare rules of engagement**

Sources: *CSO: https://www.csoonline.com/article/3322221/security/9-cyber-security-predictions-for-2019.html*

Cybersecurity alert: cryptomining/jacking

Malware that can harness your computer's power to mine cryptocurrency for profit

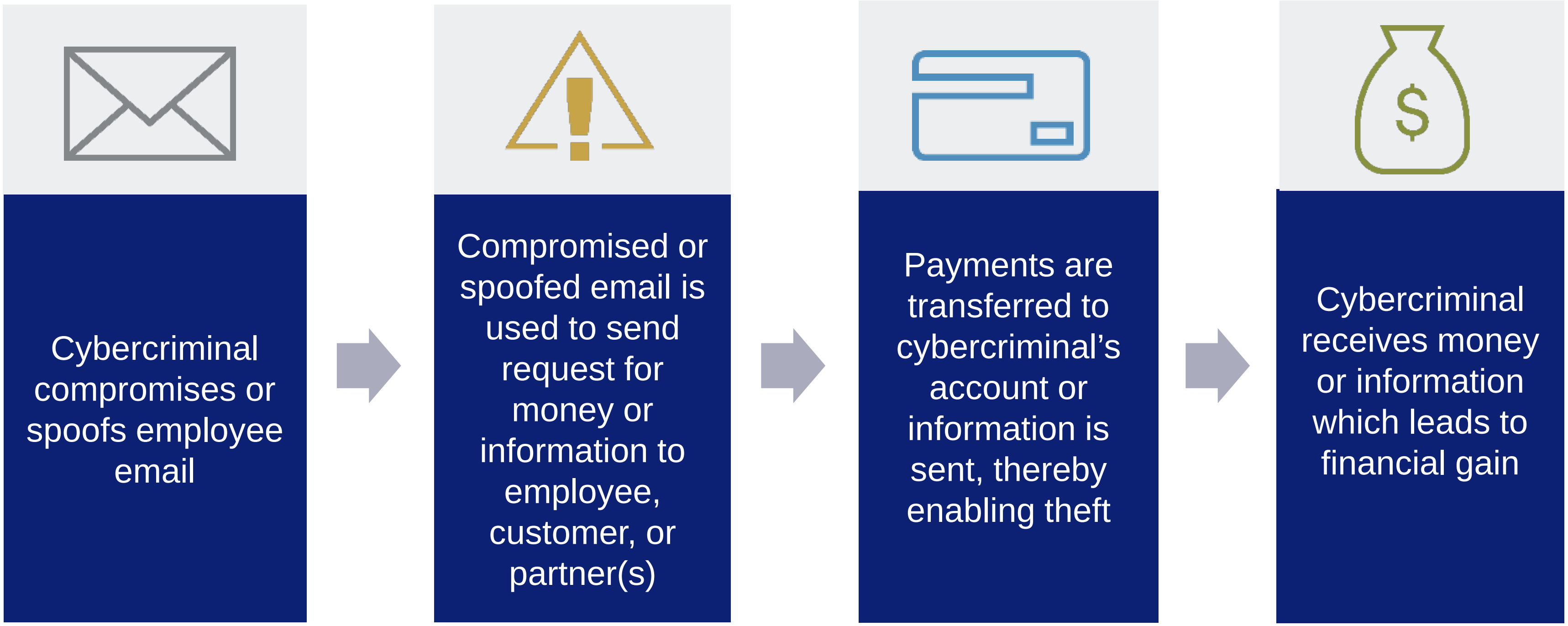
- Can target computers, smart TVs, cell phones, and any internet-connected device
- 629% increase at beginning of 2018
- Recognize by overheated or strange behaving electronics

New threat, but old rules still apply:

Strong passwords Security updates Anti-virus

Sources: Forbes: *https://www.forbes.com/sites/rachelwolfson/2018/11/13/cryptojacking-on-the-rise-webcobra-malware-uses-victims-computers-to-mine-cryptocurrency/#379d4567c336*

Cybersecurity alert: business email compromise



Cybercriminal compromises or spoofs employee email

Compromised or spoofed email is used to send request for money or information to employee, customer, or partner(s)

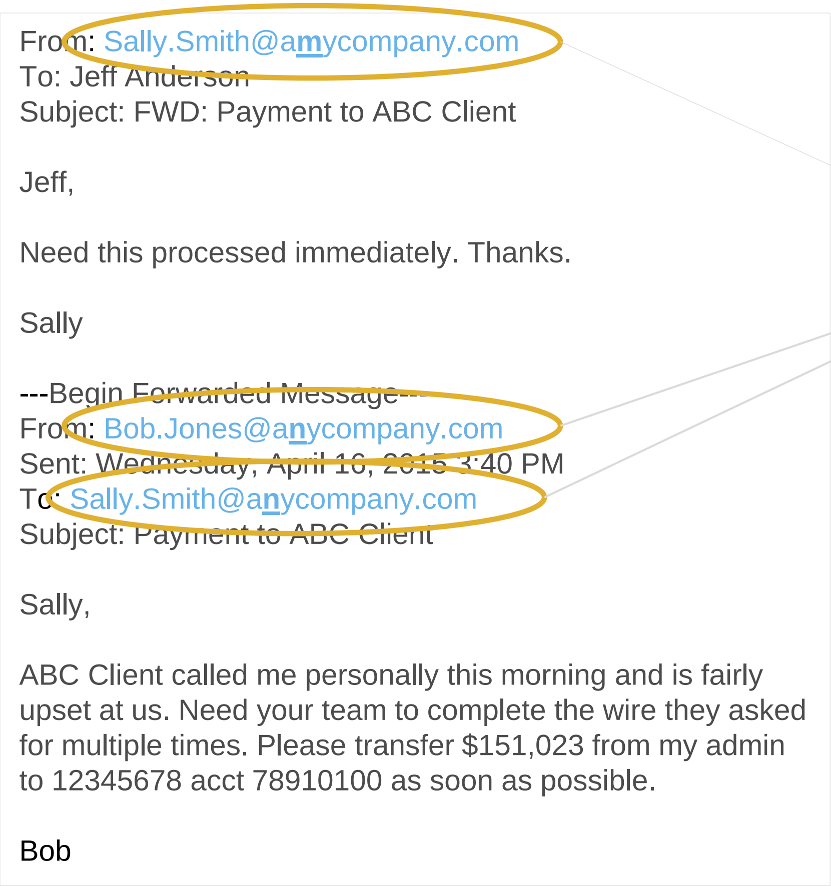
Payments are transferred to cybercriminal’s account or information is sent, thereby enabling theft

Cybercriminal receives money or information which leads to financial gain

“To sound legitimate, the attackers manipulate the tone of their email copy. They take on different personalities, including ‘the authoritarian’ who uses a direct and urgent approach, or ‘the conversationalist’ who builds a dialogue before asking for the request…” (Proofpoint 2017 Email Fraud Report)

Cybersecurity alert: business email compromise

Example of spoofed email



From: Sally.Smith@a**m**ycompany.com
To: Jeff Anderson
Subject: FWD: Payment to ABC Client

Jeff,

Need this processed immediately. Thanks.

Sally

---Begin Forwarded Message---
From: Bob.Jones@a**n**ycompany.com
Sent: Wednesday, April 16, 2015 3:40 PM
To: Sally.Smith@a**n**ycompany.com
Subject: Payment to ABC Client

Sally,

ABC Client called me personally this morning and is fairly upset at us. Need your team to complete the wire they asked for multiple times. Please transfer $151,023 from my admin to 12345678 acct 78910100 as soon as possible.

Bob

Pay attention to email domain names.
Here the attacker sent the email from “a**m**ycompany.com” and spoofed a previous internal email from “a**n**ycompany.com”

Business Email Compromise (BEC) is on the rise

$12B Total and potential losses globally from 2013 – 2018

17% Increase in BEC attacks last year

13 Average number of people targeted in an organization

1/3rd Of BEC messages contain the word “payment” in the subject line; Most attacks are designed with wire transfer fraud in mind)

11% Of all email fraud attacks use ‘fake email chain’ messages, to give a realistic experience and appear more credible

Source: InfoSec Magazine - https://www.infosecurity-magazine.com/news/bec-attacks-jumped-17-last-year/

Cybersecurity alert: ransomware

From: DD4BC Team” <dd4bc@safe-mail.net>
Sent: Sunday, Feb 16, 2015 5:42 PM

Btw. Attack temporarily stopped. If payment not received within 6 hours, attack restarts and price will double up.

---Original Message---
From: “DD4BC Team” <dd4bc@safe-mail.net>
Sent: Sunday, Feb 16, 2015 12:34 PM
Subject: DDOS ATTACK!

Hello,

Your site is extremely vulnerable to DDoS attacks. I want to offer you info how to properly setup your protection, so that you can’t be ddosed. If you want infor on fixing it, pay me 1.5 BTC to
1E8R3cgnr2UcusyZ9k5KUvkj3fXYd9oWW6ABC

Recognizing phishing

Look at overall email message

- Is it from an **external email** address? Is it **unsolicited**? Does the email address look legit, but is slightly “off” (ex: linkedin.com)? Does it require urgent or immediate action?

Look at links

- Look out **for spoofed links** to seemingly legit sites. Hover over links to see the actual destination – does it match the link? Check the **country code** in the domain – does it match the sender’s info?

Look at attachments/files

- Beware of attachments which can contain embedded malware or launch malware. Don’t open or download!

Know how to report suspicious emails within the company.

Don’t delete suspicious emails before reporting them. It’s important to investigate potential threats.

Tips to help avoid being a victim

Avoid password reuse	Update anti-virus (AV)	Email and browse smart	Keep software current
Remember to: • Use strong/multi-factor authentication for high risk transactions • Make sure all passwords are complex	AV has its limitations: • Most AV is reactive and struggles to find new or hidden malware strains • Only catches a fraction of malware	Be careful of: • Email links • Downloading files • Plug ins for your browser • Be cautious on social media	Remember: • Computers and phone do not “stay secure” over time • Regular updates or patches fix security issues

Staying safe online

Beware of unsolicited offers.

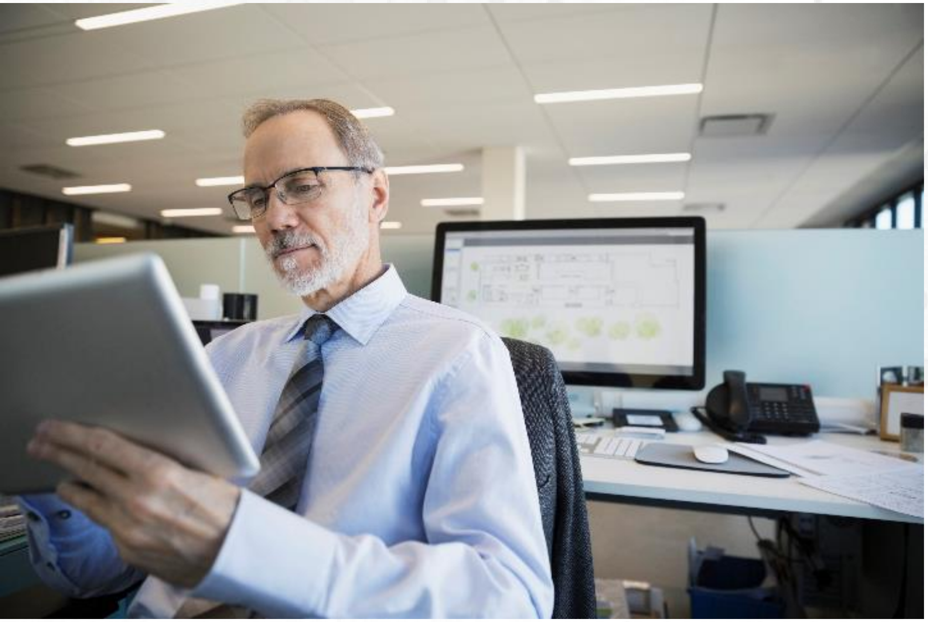
- Phishers can easily conduct reconnaissance on you beginning with social media sites like **LinkedIn, Facebook, and Instagram.**
- **On social media, phishers can learn:**
  - **1)** your employer
  - **2)** your position
  - **3)** your current location (geo-location)
  - **4)** products and subjects that you “like” or find interesting
  - **5)** your connections like friends, family and even co-workers

Your interests inform phishers on how to target you.

- A phisher can even guess your work email address using standard naming conventions **(e.g., jane.doe@municipalityname.gov).**

Cybersecurity is a key to risk management

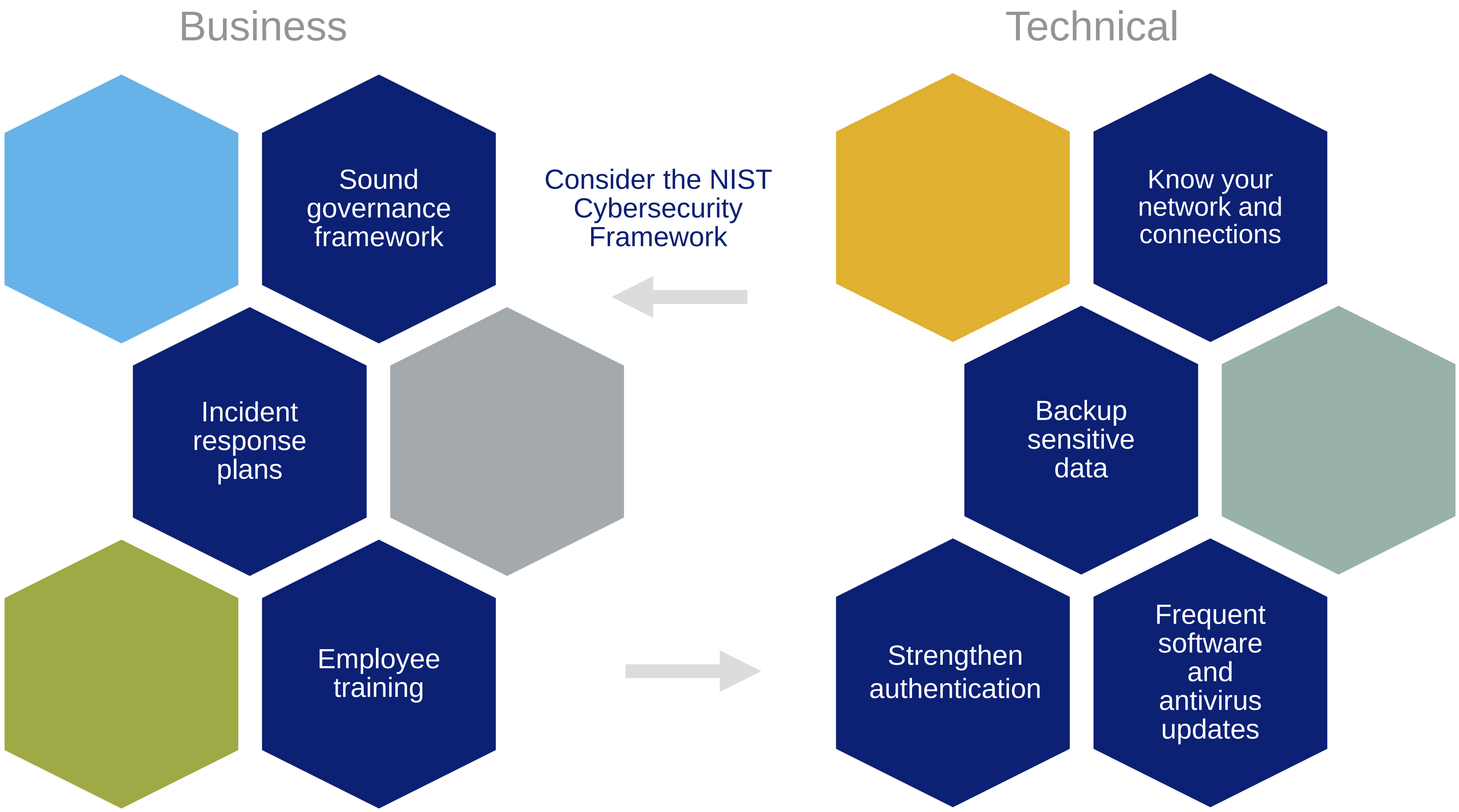
We must keep in mind…



- Size of the "opportunity"
- Frequency of attacks
- Successes to date embolden the "bad guys"
- Number of exposed points is exploding
- Cyber risk is not about a couple of guys in their basement

Sources: *https://www.ic3.gov/media/2016/160614.aspx ; https://www.wsj.com/articles/in-the-bitcoin-era-ransomware-attacks-surge-1471616632 http://blogs.microsoft.com/microsoftsecure/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/*

Industry cybersecurity best practices



Business

Sound governance framework

Incident response plans

Employee training

Consider the NIST Cybersecurity Framework

Technical

Know your network and connections

Backup sensitive data

Strengthen authentication

Frequent software and antivirus updates

Report on Cybersecurity Practices, FINRA, February 2015
https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

By the Numbers

Cybersecurity awareness is critical to the entire organization.

$6 Trillion Dollars

The total global projected cost of cybercrime damage by the year 2021.

78 Percent

People who say they are aware of the risks of unknown links in emails, but click anyway.

31 Percent

Of organizations say employee negligence is the root cause of data breaches.

4,000

The amount of ransomware attacks daily.

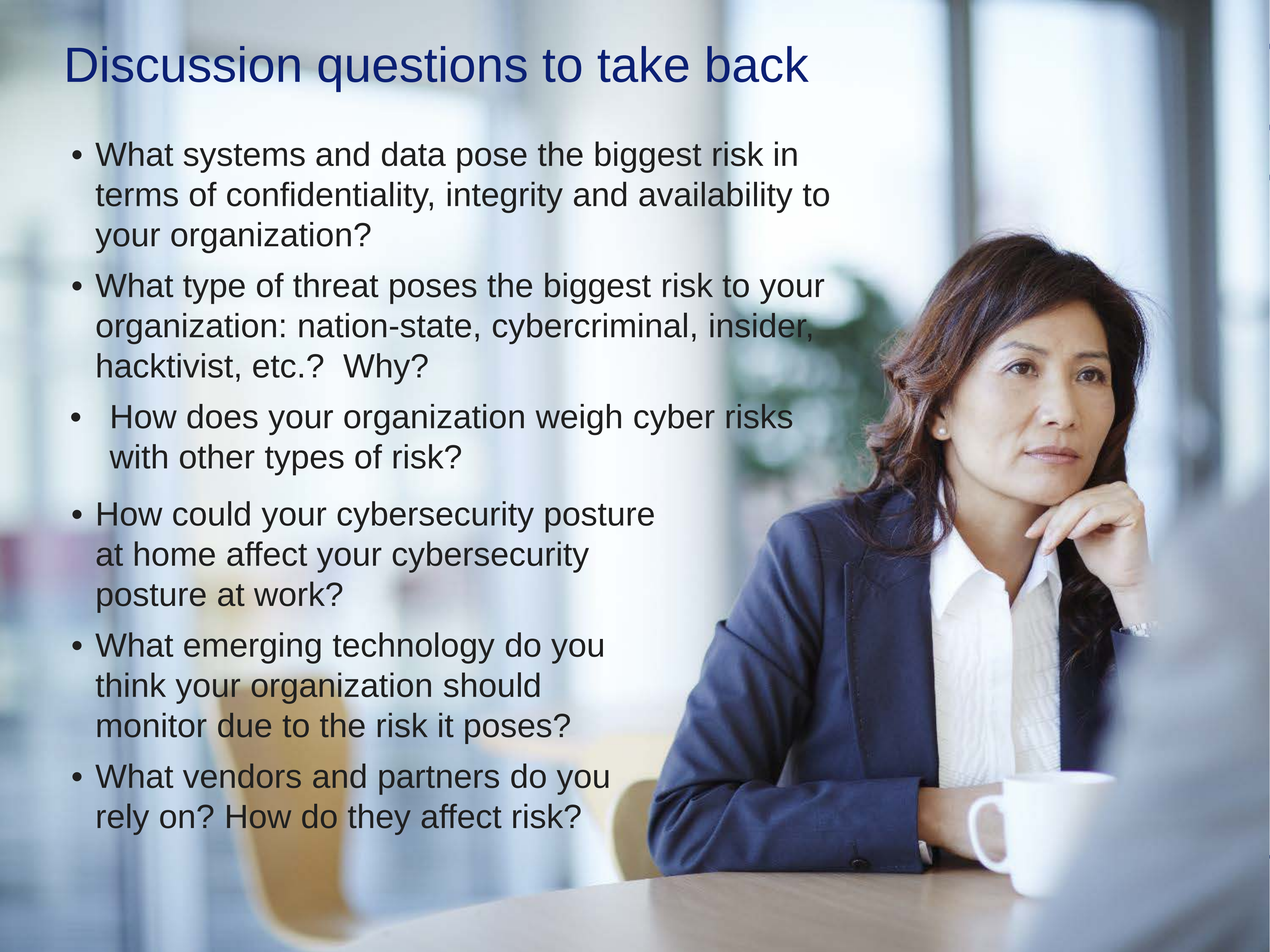
KEEP CALM

AND

CARRY ON

Source: CSO from IDG: https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html
Kroll : http://www.kroll.com/en-us/what-we-do/cyber-security/prepare-and-prevent/cyber-risk-assessments/data-security-statistics
Barkly: https://blog.barkly.com/cyber-security-statistics-2017
Federal Bureau of Investigation: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Discussion questions to take back



- What systems and data pose the biggest risk in terms of confidentiality, integrity and availability to your organization?
- What type of threat poses the biggest risk to your organization: nation-state, cybercriminal, insider, hacktivist, etc.? Why?
- How does your organization weigh cyber risks with other types of risk?
- How could your cybersecurity posture at home affect your cybersecurity posture at work?
- What emerging technology do you think your organization should monitor due to the risk it poses?
- What vendors and partners do you rely on? How do they affect risk?

Free tools

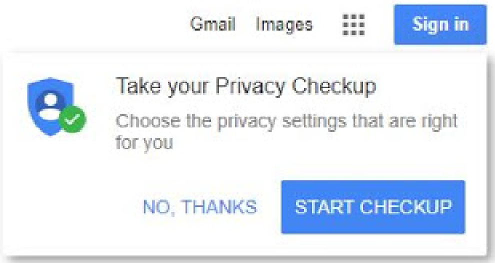
Consumers

NYC SECURE

Get alerts for unsecure Wi-Fi networks, apps, and more.

“Intended for download in New York City only. Zimperium does not accept any responsibility to you if you fail to meet this requirement.”

https://secure.nyc



Take your Privacy Checkup

Choose the privacy settings that are right for you

GOOGLE PRIVACY CHECK-UP

Access and control privacy settings and what data is used.

https://myaccount.google.com/intro/privacycheckup

Developers

NETFLIX STETHOSCOPE

Personalized, user-focused recommendations for employee information security.

https://github.com/Netflix/stethoscope

Free resources

Partnerships & information sharing

- **Infragard -** a partnership between the FBI and members of the private sector providing a vehicle for the timely exchange of information and promotes learning opportunities to protect Critical Infrastructure**:** www.infragard.org
- **Global Cyber Alliance -** working together to eradicate systemic cyber risk: www.globalcyberalliance.org
- **Multi-State Information Sharing and Analysis Center (MS-ISACs)** – https://www.cisecurity.org/ms-isac/

Government

- **NIST Cybersecurity Framework:** https://www.nist.gov/cyberframework
- **Federal Bureau of Investigation Cyber Division:** www.fbi.gov/investigate/cyber
- **Department of Homeland Security Cyber Security Awareness Campaign:** www.stopthinkconnect.org
- **Federal Trade Commission Privacy and Security Site:** https://www.ftc.gov/tips-advice/business-center/privacy-and-security

Free resources

U.S. Bank

- **Strength in Security annual cybersecurity conference** held in October during Cybersecurity Awareness Month. Stay tuned for 2019 details: www.strengthinsecurity.com
- **Online Security microsite** featuring various tips on how to stay safe in your personal and business life: https://www.usbank.com/online-security/
- **Annual Cyber Threat Briefing** document request: jacqueline.sullivan@usbank.com

Publications

- **2018 Verizon Data Breach Investigations Report:** https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
- **Financial Services Information Security & Analysis Center - Destructive Malware Best Practices Paper:** https://www.fsisac.com/sites/default/files/news/Destructive%20Malware%20Paper%20TLP%20White%20VersionFINAL2.pdf
- **Ransomware Best Practices Paper:** https://www.uschamber.com/sites/default/files/documents/files/ransomware_e-version.pdf

Disclaimer

These websites, and the services provided, are under the exclusive control of the respective third-party provider. These links are provided as a courtesy and do not imply, suggest, or constitute any sponsorship, endorsement, or approval of any third party or any affiliation with any such third party. Further, we make no warranties or representations whatsoever with regard to any third party website, merchandise, or service, and we are not responsible or liable to you for any damages, losses, or injuries of any kind arising out of your use of any third party website.

Jenny Menna
Cybersecurity Partnership Executive &
Senior Vice President, U.S. Bank
jenny.menna@usbank.com

Thank You