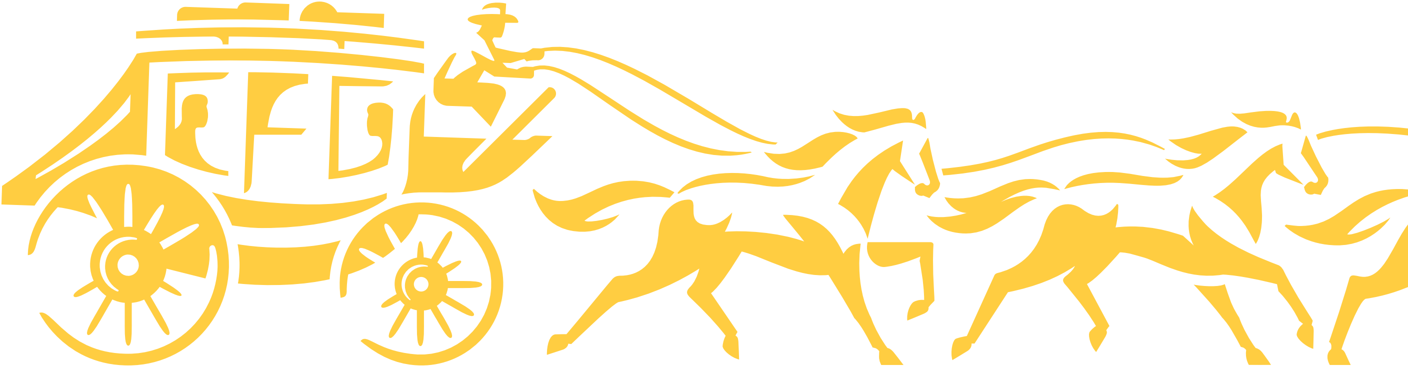
Cybersecurity Overview

March 2019
Elon Ginzburg
Operational Risk Manager and Business Information Security Leader
for Wholesale Banking and Wealth and Investment Management



Agenda

- Cybersecurity threat landscape
- Deep dive into emerging cyber/ fraud attacks
- Looking ahead
- Cybersecurity and you
- Questions

The Vision, Values & Goals of Wells Fargo

Our Vision

We want to satisfy our customers’ financial needs and help them succeed financially.

Our Values

- What’s right for customers
- People as a competitive advantage
- Ethics
- Diversity and inclusion
- Leadership

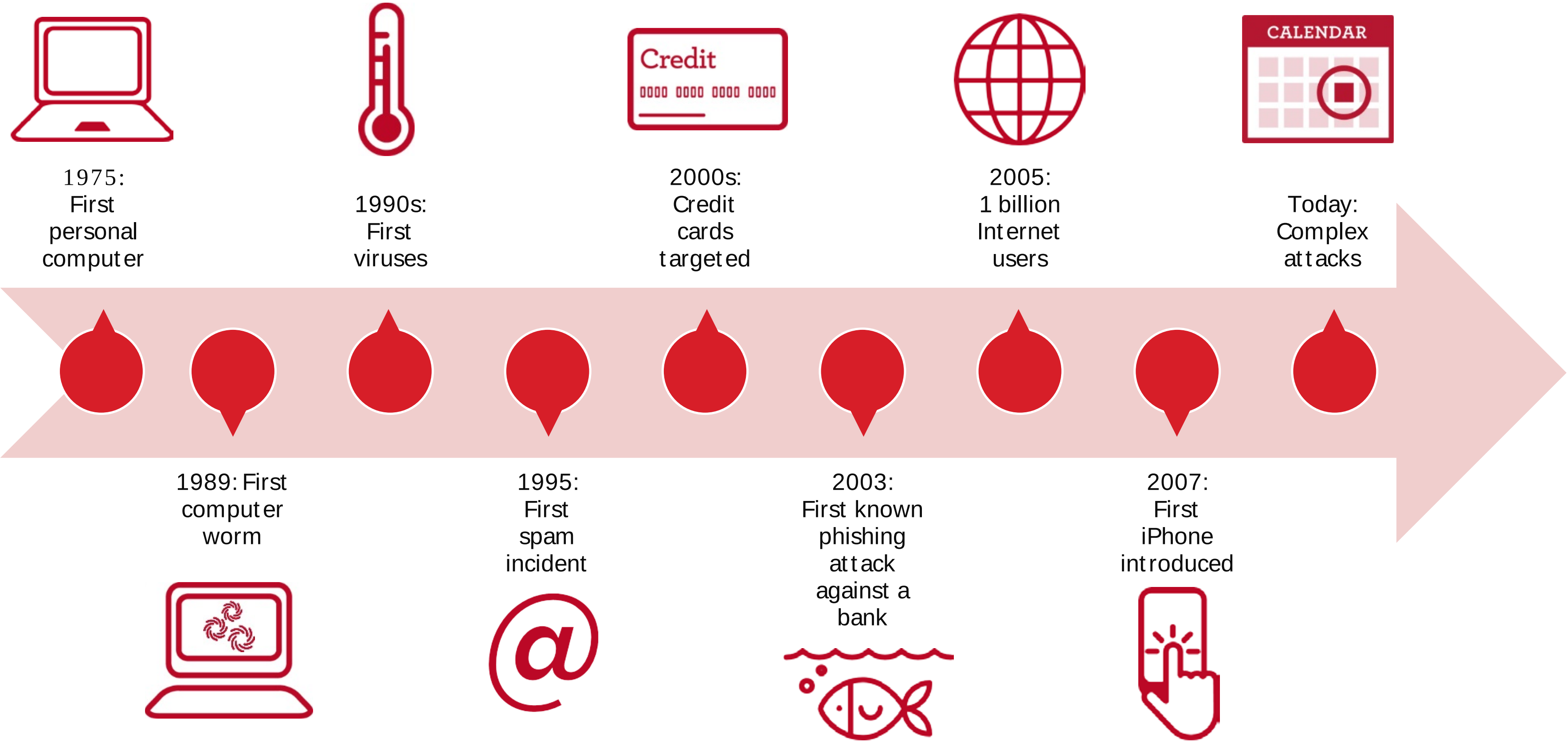
Our Goals

We want to become the financial services leader in these areas:

Customer service and advice	Team member engagement	Innovation
Risk management	Corporate citizenship	Shareholder value

Cybersecurity threat landscape

History of cybersecurity



1975: First personal computer

1989: First computer worm

1990s: First viruses

1995: First spam incident

2000s: Credit cards targeted

2003: First known phishing attack against a bank

2005: 1 billion Internet users

2007: First iPhone introduced

Today: Complex attacks

Sources:

- Ted Julian, Defining moments in the history of cyber-security and the rise of incident response, Infosecurity Magazine, http://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/, accessed November 7, 2018
- Jakob Nielsen, One billion Internet users, Nielsen Norman Group, https://www.nngroup.com/articles/one-billion-internet-users/, accessed November 7, 2018
- Phishing.org, History of phishing, http://www.phishing.org/history-of-phishing, accessed November 7, 2018

What are the top cyber risks, and why are they so dangerous?

- Malware and ransomware
- Cloud services and third party service providers
- Phishing and social engineering
- Insider threat
- Recent leaks of nation-state cyber exploitation tools
- Rapid growth of vulnerabilities in widely used technologies
- Severe shortage of cyber talent

Threat landscape: By the numbers

146 days

median number of days an attacker resides within a network before detection

16.7 million

Number of victims of identity fraud in 2017, a record high over 2016

$6 trillion

projected yearly global cybersecurity damages, 2021

76% of breaches

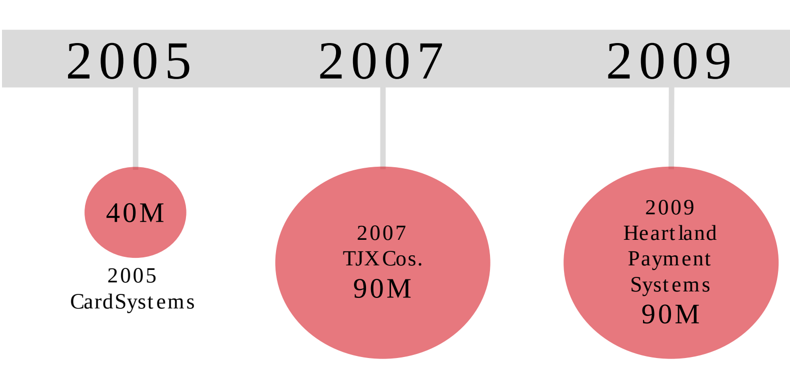
were financially motivated

$3.8 million

the average cost of a data breach to a business

Sources: http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html Verizon 2017 Data Breach Investigations Report
http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html
2016 Cost of Cyber Crime Study & the Risk of Business Innovation, Ponemon Institute LLC

Growth in breaches



2005

40M

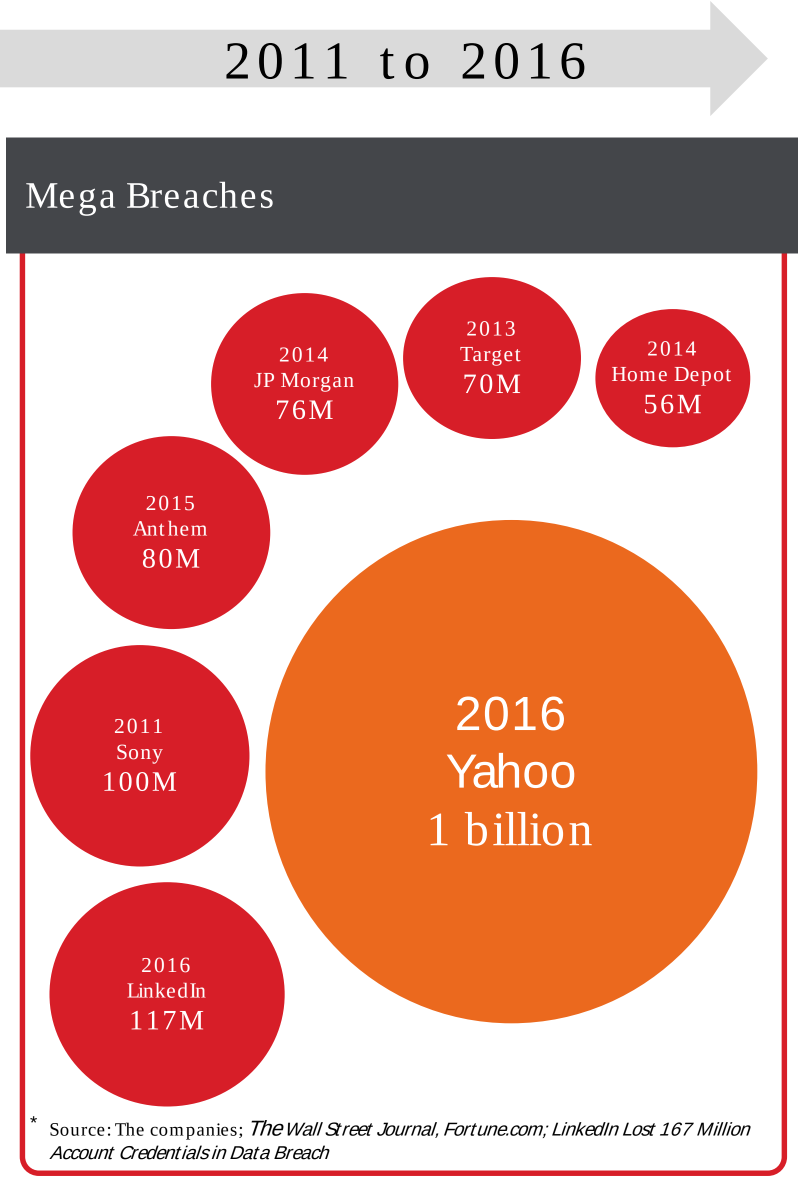
2005
CardSystems

2007

2007
TJX Cos.
90M

2009

2009
Heartland
Payment
Systems
90M



2011 to 2016

Mega Breaches

2014
JP Morgan
76M

2013
Target
70M

2014
Home Depot
56M

2015
Anthem
80M

2011
Sony
100M

2016
Yahoo
1 billion

2016
LinkedIn
117M

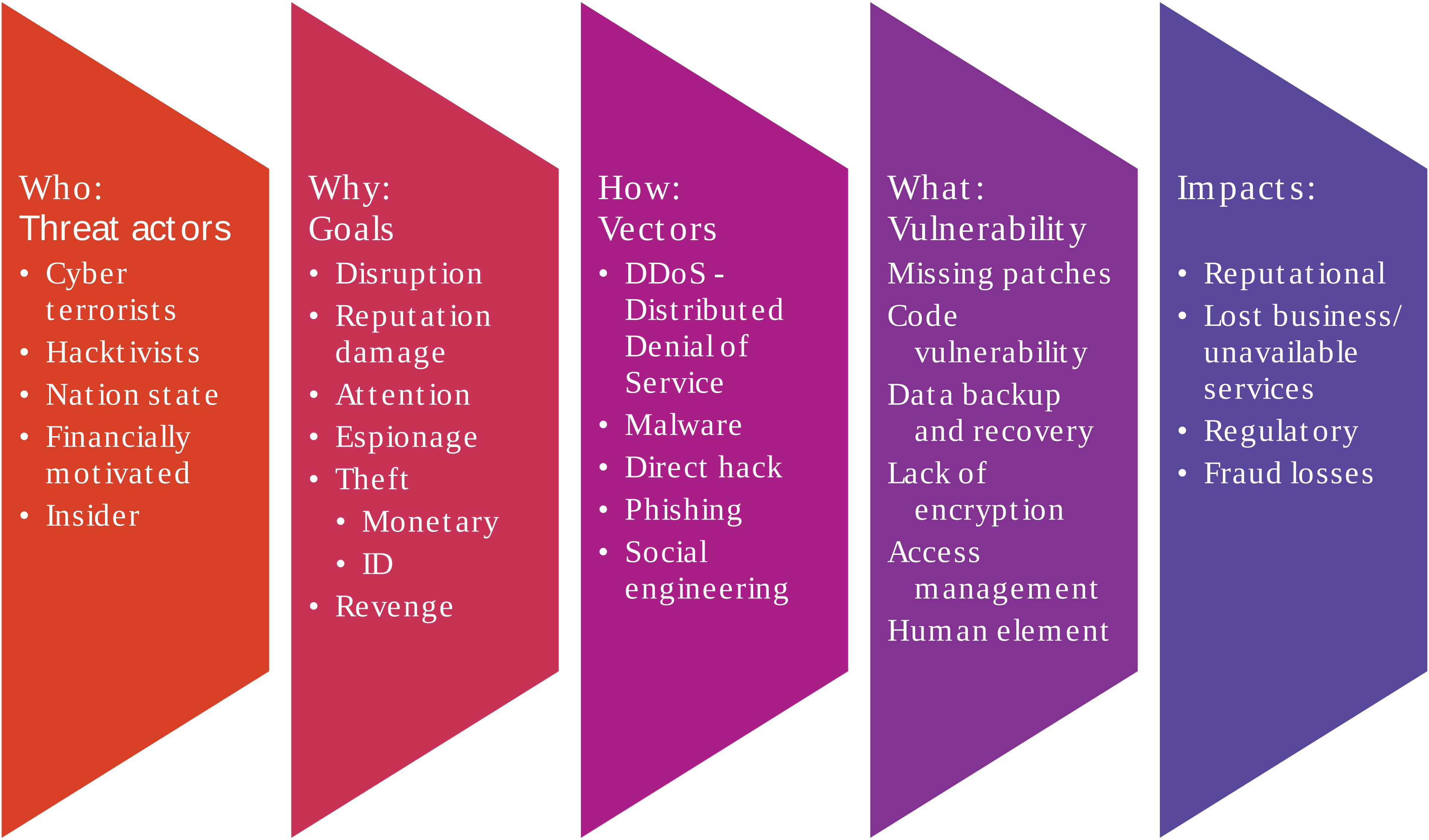
* Source: The companies; *The Wall Street Journal, Fortune.com; LinkedIn Lost 167 Million Account Credentials in Data Breach*

NBC News

“Massive Equifax Data Breach Could Affect Half of the US Population”

September 7, 2017

Motivations and methods



Who: Threat actors

- Cyber terrorists
- Hacktivists
- Nation state
- Financially motivated
- Insider

Why: Goals

- Disruption
- Reputation damage
- Attention
- Espionage
- Theft
  - Monetary
  - ID
- Revenge

How: Vectors

- DDoS - Distributed Denial of Service
- Malware
- Direct hack
- Phishing
- Social engineering

What: Vulnerability

Missing patches

Code vulnerability

Data backup and recovery

Lack of encryption

Access management

Human element

Impacts:

- Reputational
- Lost business/ unavailable services
- Regulatory
- Fraud losses

Deep dive into emerging cyber/fraud attacks

- Spear-phishing
- Ransomware
- Imposter fraud
- Denial of service
- Wire service attacks

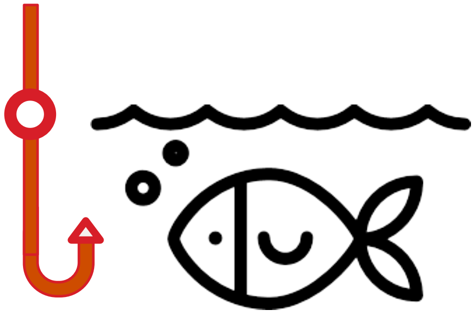
Spear-phishing, a form of social engineering, is one of the most effective techniques to breach security

What is it?

- A targeted, custom form of phishing
  - Spear-phish is an email that appears to be from an individual or business that you know
  - Intention — Getting information, such as account login, or installing a malware
- Spear-phishing is often based on research using social media
  - Who do you work with?
  - What do you do?
  - Who are your friends?

What can you do about it?

- Remove corporate email from LinkedIn and social networks
- Be vague about what you do
- Watch for spoofed email — look at the email address not only the displayed name



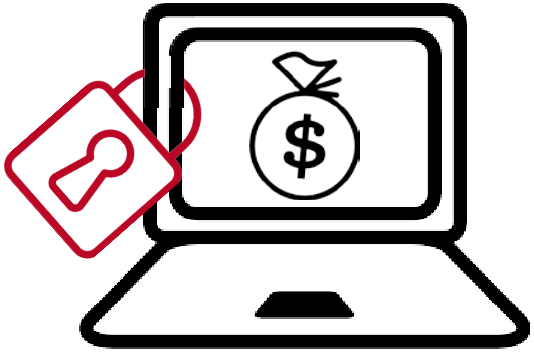
Ransomware is a proven effective attack tactic, impacting everyone and everything

What is it?

- A malicious software that scrambles all files on an infected computer with strong encryption, and then requires payment from the victim to recover them.
  - Distribution through multiple ways (websites, phish, spear-phishing)
  - Impacts both individuals and institutions
- Attacks tend to focus on:
  - End-user computers
  - Servers
  - Internet of Things (IOT) devices

What can you do about it?

- Don’t click
- Backup data regularly
- To pay or not to pay



Business Email Compromise—another form of social engineering—is one of the fastest growing schemes

What is it?

- Fraudster poses as a trusted person — a company executive or a critical partner/vendor — and is looking for quick responses in order to steal funds
  - Email is spoofed or compromised
- Emerges in 2013 (~$170MM)
- Between October 2013 and May 2018, global losses totaled more than $2.9 billion.
  - FBI public service announcement, June 11, 2018

What can you do about it?

- Establish and follow operational procedures when conducting high risk transactions such as approving payments, such as:
  - Out-of-band
  - Dual-factor authentication

Denial of service can take multiple forms

What is it?

- Attempts to render an online service unavailable by overwhelming it with unwanted traffic from multiple sources
  - Types: DOS (denial of service), DDOS (distributed denial of service)
  - Intention — Disrupt services and operations by:
    - Creating traffic jams
    - Crashing systems
    - Locking accounts
    - Many others…

What can you do about it?

- Defensive controls aim to block illegitimate traffic through:
  - Attack detection
  - Traffic classification
  - Response tools
  - Several vendors offer end-to-end solution geared to deflect traditional DDOS activities

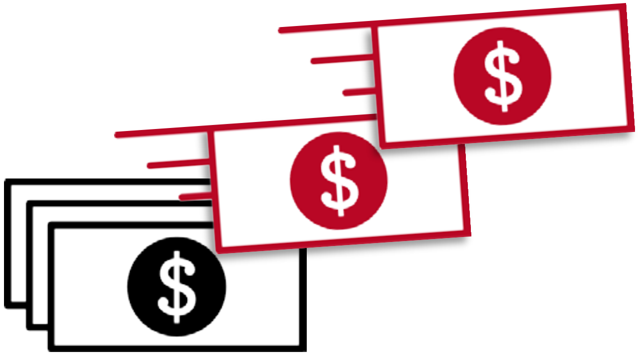
Attacks on payment ecosystems

What is it?

- Several highly-publicized cyber-attacks originated wire transactions from member banks through the SWIFT network:
  - Central Bank of Bangladesh, $81MM loss
  - Tien Phong Commercial bank, Vietnam, loss unknown
  - Banco del Austro, Ecuador, $9MM loss
- Hackers appeared to:
  - Compromise the bank's environment by **deploying sophisticated malware**
  - Obtain valid operator credentials, gaining **unauthorized access** to create, approve and submit SWIFT messages from within the institution
  - Submit **fraudulent messages** by impersonating operators using stolen credentials
  - **Hide evidence** by removing traces of the fraudulent messages

What can you do about it?

- **SWIFT** created Customer Security Program that members need to adhere to.
- Wells Fargo Bank introduced a bank-wide, multiyear, and well-funded initiative to increase security of payment eco systems.



Looking forward: threats and predictions

- Artificial intelligence
- Crypto mining
- Internet of Things botnets
- State-sponsored cyber activity
- Cloud security
- Direct payment system fraud
- Supply chain attacks
- CPU vulnerabilities

Cybersecurity and you —
Information security is everyone's business

10 tips to protect yourself online

1. Check your computer for personally identifiable information
   - Look for social security information, driver's license numbers, and bank account numbers.
2. Re-think how you connect
   - Avoid unsecured Wi-Fi when possible. If you must connect, do not go on sensitive sites.
3. Get professional help
   - Find an IT professional to help if you're over your head.
4. Avoid suspicious links
   - Be careful when you click a link or open a program.
5. Protect your passwords
   - Aim for complex, hard to guess, and changed them often.

10 tips to protect yourself online

6. Be aware of common scams
   - Exercise extreme caution if someone asks you for money, usernames, passwords, or account details.
7. Update your software
   - Patch your operating system, software, browser, and plug-ins.
8. Plan for the unexpected
   - Back up your important data in multiple ways.
9. Keep up-to-date
   - Follow news, trends, and developments to stay in the know.
10. Consider automatic alerts
    - Many services will inform you of suspicious activity automatically.

WELLS FARGO

Thank you.

Questions?