Securing Banking and Payment Systems: A View from the Federal Reserve

Jason Ritchie
Assistant Vice President

Houston Branch of the Federal Reserve Bank
September 8, 2016

The thoughts and ideas expressed in this presentation are those of presenter and do not necessarily reflect the official positions of the Federal Reserve Bank or the Federal Open Market Committee.

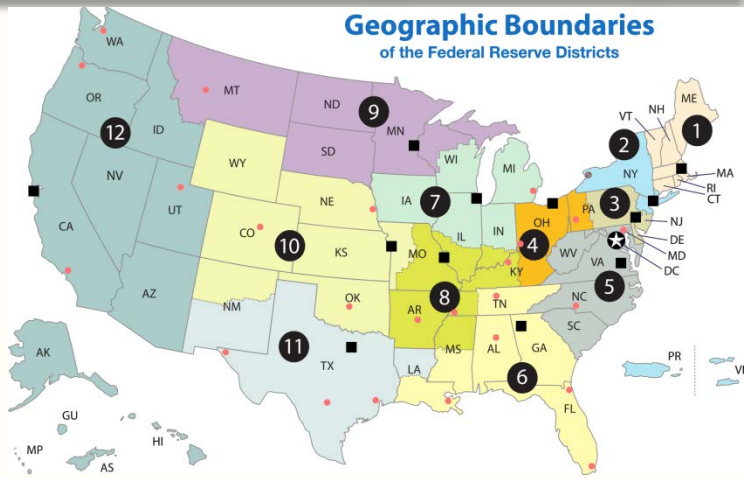
Passwords

Thirteen patterns represent 50% of passwords

- Uaaaaa00
- Uaaaaaa00
- Uaaa0000
- aaaaaaa0
- Uaaaaaaa00
- Uaaaaaa0
- Uaaaaa0000
- Uaaaa0000
- aaaaaa00
- Uaaaaaaa0
- Uaaaa000
- Uaa0000$
- aaaaaaaa

Federal Reserve Bank

- Created in 1913 by Congress
  - Conducts Monetary Policy to maximize employment and stabilize prices
  - Supervises state member banks and bank holding companies
  - Comprises 12 Reserve Bank Districts and Board of Governors
- Not-for-profit organization; not funded by taxpayers
  - Charges fees for services to FIs
  - Makes profit on buying/selling securities as part of monetary policy actions
  - Net payment back to taxpayers of $600 Billion since 2008



Disclaimer

The contents of this presentation—written and spoken—reflect my views only and not the opinions of the Board of Governors of the Federal Reserve System, the Federal Open Market Committee, or the Federal Reserve Bank of Dallas.

Cybersecurity

- FRB Repels 1.5 billion attacks on information infrastructure annually
- Numerous motivators to hack the FRB
  - Financial
  - Reputational
  - Informational
  - Political
- Recommending improvements to the payments system as a collaborative effort to improve security

500+ Task Force Members

"We have seen many of the strategies and tactics included in the plan come to life through broad, unprecedented stakeholder support. When implemented, the strategies will contribute to public confidence and the global competitiveness of the U.S. payment system."

Esther George, President and CEO of the Federal Reserve Bank of Kansas City and executive sponsor of the payments improvement initiative

Ransomware

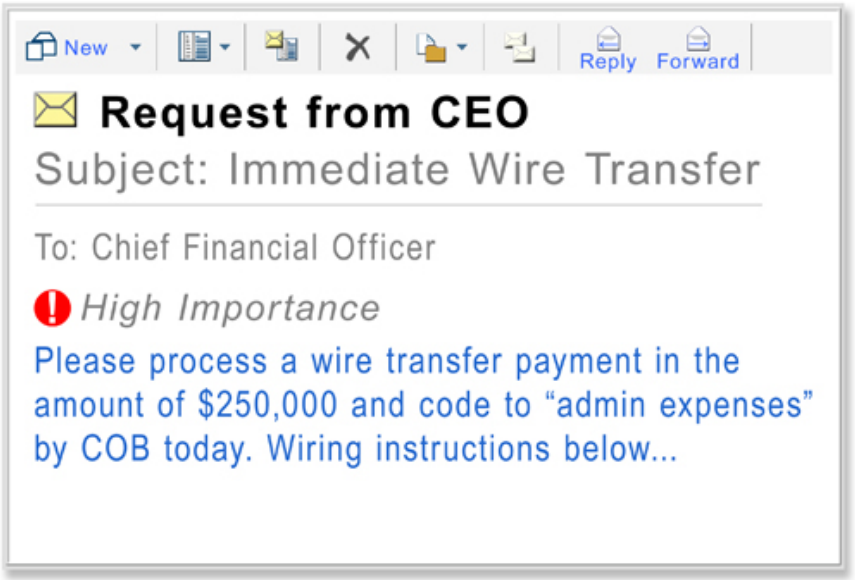
- Ransomware is a form of malware that targets your critical data and systems for the purpose of extortion.
- Ransomware is frequently delivered through spear phishing emails and vulnerability attacks.
- After the user has been locked out of the data or system, the cyber actor demands a ransom payment.

- Many variants
  - Cerber
  - CryptXXX
  - Locky
  - CryptoWall

- Cost of attacks
  - Bitcoin payments of $ 679 on average
  - Downtime
  - Incident response
  - Data loss
  - Operational loss/safety
  - Reputational

Latest Trends in Fraud

- Incidents of fraud are about the same for large corporations (revenue over $1 billion) and smaller organizations
  - 16% point gap in 2013
  - 9% point gap in 2014
  - 2% point gap in 2015
- Wire transfer fraud is dramatically increasing
  - 14% in 2013
  - 27% in 2014
  - 48% in 2015
- Business Email Compromise (BEC) contributing factor



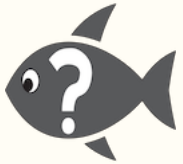
AFGlobal BEC Attack

- AFGlobal's Director of Accounting received an email from the CEO's email account on May 21, 2014 regarding an urgent and confidential financial operation
- The Director was contacted by an alleged lawyer requiring the company to wire $480K to the Agricultural Bank of China for good faith money for an acquisition
- Several days later, the receipt was confirmed with another request of $18M to finalize the acquisition
- According to the FBI, thieves stole nearly $2.3b from 17,642 businesses, Oct. 2013-Feb. 2016, globally

Best Practices

- Implement detection to flag e-mails with extensions similar to the company e-mail
  - e.g., if your company e-mail is @company.com, the e-mail @c0mpany.com would be flagged
  - Flag all emails that are external to the organization
  - Perform email monitoring; don't rely solely on spam filters to catch these emails
- Perform phishing training and simulations

  http://krebsonsecurity.com/2012/01/phishing-your-employees-101/



- Register all company domains similar to the actual company domain
- Block social media and personal email
- Call backs on all wire transfers

Card Swipe Terminals

Skimmers

Skimmer Increases

- Debit-card compromises at ATMs located on bank property jumped 174% from January 1 to April 9, 2015, compared with the same period in 2014
- Attacks at nonbank machines increased by 317%
- 3-D Printers, Bluetooth technology, cellular connections, micro cameras, and key loggers are making skimmers very high-tech and automated

EMV & October 1, 2015

- Liability Shift: Visa instituted a U.S. liability shift for domestic and cross-border counterfeit card-present POS transactions, eff. Oct. 1, 2015.
  - Fuel-selling merchants have until Oct. 1, 2017
  - Jan. 2016: “More than 1.3m fuel dispensers in the U.S. that need to be updated in the next 21 months.”
- As of June 2016, only 24% of terminals chip-enabled
- Visa expects 50% of locations to be enabled by EOY16

EMV – Where Are We Now?

- At the top 5 chip-enabled merchants, counterfeit card fraud was down by 18.3% from 4Q14 to 4Q15
- Conversely, at the top 5 non-EMV merchants, counterfeit card fraud increased 11.4% during the same period

Liability

- Individual Americans are protected by Reg E & are liable for a maximum $50 if a cyber-thief strikes
  - But companies have no such guarantees
- In the US, corporate customer liability is governed by the Uniform Commercial Code (UCC)
- Companies are responsible for stolen funds if:
  - they have agreed to a security procedure with the bank,
  - the bank followed it, and
  - the procedure was 'commercially reasonable'

Choice Escrow v. BancorpSouth

- 2010: Choice Escrow & Land Title, victim of hackers who obtained its online banking details using malware and wired $440,000 to a bank in Cyprus
  - Choice sued BancorpSouth for failing to provide “commercially reasonable security”
  - Suit was rejected based on the fact that Choice declined to use security measures BSB had encouraged it to use
- When Choice adopted online banking in 2009, BSB usually required that customers use dual control
  - Choice declined dual control in communications with the bank on two different occasions
  - Preferred convenience and indicated the employee who handled wires was often in the office by herself

State Bank of Bellingham v. BancInsure

- State Bank of Bellingham, Minnesota – 5 employees
- Oct. 2011: A computer at the bank, used to conduct wire transfers was infected with malware
  - A bank employee did not remove two physical tokens from the PC after conducting a wire
  - Tokens were left in the PC overnight
  - Two unauthorized wires summing $940,000 had been sent
- Bank's insurance company, BancInsure, argued an exclusion in the bank's policy due to "employee-caused losses"
- Bank ultimately won the court cases, including an appeal

SOURCE: "Analysis: Bank Sues Insurer for Fraud Coverage, Wins…," by Tracy Kitten, bankinfosecurity.com, June 6, 2016

Insider Threats

Source: IBM 2015 Cyber Security Intelligence Index

- Consider Best Practices
  - Separation of duties
  - Dual controls
  - Eliminate privileged access
  - Data Loss Protection

First Commonwealth Bank v. St. Paul Mercury

- SVP credentials were hacked through malicious software, and three wire transfers summing $3.5 million were executed August 31 and September 4, 2012
- Bank refunded losses with their own funds and then filed a claim against its Professional Liability policy
- Claim was denied, but court ruled in the bank's favor
- Lessons Learned
  - Policyholders should focus on insurance obligations at the outset of a cyber event so as not to compromise potential coverage
  - Coverage for cyber risks remains available under multiple types of insurance

Lambrecht & Associations v. State Farm Lloyd's

- Virus destroyed records and server on February 9, 2000
- Records had to be manually recreated, server had to be replaced and rebuilt, and income was lost due to the outage
- Business insurance policy insures against “accidental direct physical loss”
- After appeal, court rules in favor of plaintiff as it was accidental from Lambrecht’s perspective and physical loss included “electronic media and records”

Retail Ventures v. National Union Fire Insurance

- DSW Shoe Warehouse was compromised; credit card and checking account numbers for more than 1.4 million customers at 108 stores
- Losses of $5 million included amounts incurred for
  - communications with customers
  - public relations in reaction to the breach
  - defense costs for responding to various government investigations
  - responding to customer complaints related to compromised credit card information (largest line item)
- A computer fraud rider on the commercial crime policy covered “direct” losses only
- Amounts paid to customers through chargebacks and amounts paid to the credit card companies were “proximately caused” by the data breach; hence, these losses were covered

Sources

- https://fedpaymentsimprovement.org/
- https://www.kansascityfed.org/publicat/econrev/pdf/14q3Sullivan.pdf
- https://securityintelligence.com/media/cyber-security-intelligence-index-2015/
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
- https://commercial.jpmorganchase.com/jpmpdf/1320699130738.pdf
- https://www.pnc.com/content/dam/pnc-com/pdf/corporateandinstitutional/Treasury%20Management/2016_AFP_Payments_Fraud_Report.pdf
- http://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion
- https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams
- https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams
- http://krebsonsecurity.com/2016/01/firm-sues-cyber-insurer-over-480k-loss/#more-33617
- http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes
- http://www.dallasfed.org/assets/documents/banking/firm/fi/fraud_survey.pdf
- http://krebsonsecurity.com/2016/02/the-great-emv-fake-out-no-chip-for-you/
- http://www.digitaltransactions.net/news/story/Nearly-40_-of-U_S_-Visa-Credit-and-Debit-Cards-Now-Have-an-EMV-Chip
- http://www.digitaltransactions.net/news/story/Visa-Tweaks-Chip-Card-Processing-Protocol_-Says-EMV-Debit-Cards-Now-Surpass-Their-Credit-Brethren
- http://www.digitaltransactions.net/news/story/Guarding-the-Online-Channel
- http://www.digitaltransactions.net/news/story/6235
- http://www.bostonfed.org/bankinfo/payment-strategies/publications/2015/tokenization-prime-time.pdf
- http://www.paymentssource.com/news/risk-analytics/more-payment-companies-make-security-a-moving-target-3020595-1.html
- https://www.ffiec.gov/cyberassessmenttool.htm
- http://krebsonsecurity.com/2011/06/court-favors-small-business-in-ebanking-fraud-case/
- http://www.americanbar.org/publications/blt/2014/10/02_desjardins.html
- http://krebsonsecurity.com/2015/03/hospital-sues-bank-of-america-over-million-dollar-cyberheist/
- http://www.americanbanker.com/news/bank-technology/sneaky-dyre-malware-bilks-corporate-bank-accounts-1073613-1.html
- https://www.fsisac.com/sites/default/files/news/Alert%20--%20Securing%20Merchant%20Terminals%20Remote%20Access%20FINAL%207%20July%202015.pdf
- http://www.bostonfed.org/bankinfo/payment-strategies/publications/2015/summary-of-mpiw-meeting-april-2015.pdf
- http://law.justia.com/cases/federal/district-courts/pennsylvania/pawdce/2:2014cv00019/214082/21/
- http://fortune.com/2016/03/29/81-million-stolen-from-bangladeshs-central-bank/
- http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR
- http://www.reuters.com/article/us-cyber-heist-bangladesh-exclusive-idUSKCN0YQ041

Takeaways

- Comply with best practices
  - Multi factor authentication
  - Separation of duties/dual controls/insider threat
  - Complicated passwords/encryption of hard drives and email
  - Adopt Positive Pay/reconcile bank statements
  - Patch and Scan
  - Classify data
  - Adopt EMV
  - Be skeptical
  - Perform assessments
- Gain experience and education

GREATER HOUSTON PARTNERSHIP
Making Houston Greater.

FINANCIAL SERVICES Information Sharing and Analysis Center