Threat Landscape and Globalization of Cybercrime

Dr. Kevin Streff, kevin.Streff@protectmybank.com
Founder, Secure Banking Solutions, www.protectmybank.com
Professor – Dakota State University, www.dsu.edu
Hot Technologies

Banking Technologies
- Branch of the Future
- Interactive Teller Machines (ITM)
- Advanced Payment Systems
- Mobile Delivery Systems
- Remote Deposit Products
- Customer Relationship Management (CRM)

Infrastructure Technologies
- Cloud
- Virtualization
- Cybersecurity Products
  - DLP
  - MSS
  - ERM Tools
- Continuous Monitoring
Online vs. Mobile

• Online banking is commodity
• Mobile banking revolution is over
• On to the Internet of Things
• On to self service
Mobile Banking – Adoption Rates

Percent Adoption – Community Banks

- 2011
- 2013
- 2015
CYBERSECURITY
Which Represents the Most Risk to the Financial Institution?

or
Threats are growing

- “…around 85% of cyber attacks are now targeting small businesses.”
  - Howard Schmidt (White House Cybersecurity Coordinator)

- “32% of businesses in this study lost more than $25,000 as a result of the ACH fraud and 7% were unable to determine their loss”
  - Ponemon Institute, 2015

Source: FDIC, Ponemon, White House
Threats are growing

- “The Department has increased our cybersecurity workforce by 500 percent over the past two years.”
  - Department of Homeland Security
- “Millions of Americans have been victimized, their privacy violated, their identities stolen, their lives upended, and their wallets emptied”
  - President Obama, 2016

Source: DHS, Obama
Threats are growing

- 74% of small and medium businesses reported attacks over the past two years.
  - Department of Homeland Security

- Only 52% of businesses have a cybersecurity plan, and 40% of businesses do not have a response plan.
  - Department of Homeland Security

Source: DHS, Obama
Layered Security Approach
Gramm-Leach-Bliley Act

• Management must develop a written information security program meeting the security standards of Part 364, Appendix B

• What is the “M” in the CAMEL rating?

The Information Security Program is the way management demonstrates to regulators that information security is being managed at the bank.
Top Security Threats

1. Hacking
2. Data Leakage
3. Social Engineering
4. Corporate Account Takeover
5. Vendor Risk
6. ATM
7. Ransomware
Hacking

Threat #1
Hacking

• Small and medium-sized businesses are the new target
  – Won’t get caught, won’t get prosecuted, fewer security controls, etc.

• Hackers are Organized
  – Used to be for fun, now it is for profit

• How it works
  – Find a computer/network vulnerability and exploit it
Hacker Tools Examples

• Tools to hack your bank are downloadable

• Default passwords are all available

• Economy is available to sell stolen data ("underground markets")
Threat: Downtime

• How much time would it take to recover if all of your computers got a virus tomorrow?
  – Data Loss
  – Down Time
  – Cost to replace vs. fix

  “Of those businesses that experience a disaster and have no emergency plan, 43% never reopen; of those that do reopen, only 29% are still operating two years later.”
Critical Infrastructure Protection

- White House is concerned that our nation’s critical electronic infrastructure will be impaired by the hackers
- PDD63
Data Leakage

Threat #2
Data Leakage

- Data Leakage is about insiders leaking customer information out of your bank
- Most attention is paid to outsiders breaking into your network (aka hackers)
- Malicious Behavior
- Accidental
Three Data Leakage Examples

• WikiLeaks
  – Army Private accessed and downloaded classified information that he later sent to WikiLeaks.

• Two Nebraska Tellers
  – Print-screen consumer records over the course of two years

• FDIC Employee
  – Divulged personal information of failed bank's customer
Misuse of Bank Computers

- At least once a day: 63%
- At least once a week: 7%
- Several times a week: 8%
- At least once a month: 2%
- Several times a month: 2%
- Never: 17%
Social Engineering

Threat #3
Social Engineering

• What is Social Engineering?
  – Exploitation of human nature for the gathering of sensitive information.
  – Tool attackers use to gain knowledge about employees, networks, vendors or other business associates.
Sample Social Engineering Methods

• Phishing/Pharming
• Telephone (Remote Impersonation)
• Dumpster Diving
• Impersonation
• E-mail Scams
• USB Sticks
Corporate Account Takeover

Threat #4
Commercial Banking Fraud

- January 22, 2009
- Experi-Metal Inc. - Sterling Heights, MI
- Sues Comerica Bank ($60M) - Dallas, TX
- An EMI employee opened and clicked on links within a phishing email
- $1.9M stolen, $560,000 was not recoverable
- 47 wires in one day to foreign and domestic accounts which EMI never wire to before
- Ruling: Bank failed to detect the fraud and must pay Experi-Metal $560,000 in losses.
Small Business Security

- 70% lack basic security controls
- Conduct a risk assessment looking for these basic security controls
  - Firewall,
  - Strong passwords,
  - Malware Protection
  - Etc.
Finger Pointing?

Most responsible for ensuring security of online accounts:

- **Our banking institution**: 67%
- **My company**: 19%
- **Government regulators**: 9%
- **Law enforcement**: 5%
Bottom Line: You Lose Customers

How fraud or attempted fraud changes the business banking relationship

- Would diminished our company’s trust and confidence in the bank’s ability to secure our accounts: 36%
- Would result in our company switching to another bank for primary services: 29%
- No affect on the business relationship: 23%
- Would result in the termination of the banking relationship: 12%
Vendor Attacks

Threat #5
Vendor Attacks

• Criminals understand that vast amounts of data are stored and transacted thru bank vendors
• TJX, Heartland, Target, etc.
• Target – RAM Scraping
• While you are outsourcing the task, your bank remains responsible for the data
• Vendor Management Program
ATM Fraud

Threat #6
The real card reader slot.

The capture device

The side cut out is not visible when on the ATM.
Skimmer Overlay
Skimmer Camera
Question

- How long does it take to install a skimmer?

ATMs

• The ATM environment has changed
• Used to be most banks:
  – Closed network
  – Non Windows
• Today, most ATMs are on your bank’s network and run Windows
• 75%+ of ATMs run Windows XP (is no longer supported after April, 2014)
ONE MAN’S MONEY TRAIL
FEB. 19 | 4:31 P.M. TO 9:59 P.M

1. 4:31 P.M.
   2380 BROADWAY
   5 WITHDRAWALS
   $4,015

2. 5:10 P.M.
   2077 BROADWAY
   3 WITHDRAWALS
   $2,409

3. 5:28 P.M.
   1886 BROADWAY
   3 WITHDRAWALS
   $2,409

4. 6:17 P.M.
   1680 BROADWAY
   3 WITHDRAWALS
   $2,409

5. 6:24 P.M.
   1535 BROADWAY
   3 WITHDRAWALS
   $2,409

6. 6:43 P.M.
   515 Seventh Ave.
   3 WITHDRAWALS
   $2,409

7. 7:31 P.M.
   238 Eighth Ave.
   3 WITHDRAWALS
   $2,409

8. 8:55 P.M.
   919 Third Ave.
   3 WITHDRAWALS
   $2,409

9. 9:24 P.M.
   991 Third Ave.
   7 WITHDRAWALS
   $5,621

10. 9:55 P.M.
    1191 Third Ave.
    4 WITHDRAWALS
    $4,015

Suspect Jose Familia Reyes with pack of cash.
ATM Cyber Heists
ATM Fraud

- Skimmers
- Cyber heists
- Remote Access Issues
- Active Ports Being Compromised
- Target Breach
Ransomware

Threat #7
Overview

• Cybercriminals are using ransomware, DDOS, theft of customer information and more to extort funds or require certain actions from financial institutions.
• Very similar to kidnapping insurance that some executives hold in volatile foreign countries, insurance companies are now writing policies to cover the extortion fees and expert technical costs incurred when a company is held as a cyber-hostage.
Ransomware

• Ransomware is a type of malware specifically designed to block or encrypt data, followed by a ransom demand.

• A warning massage usually pops up explaining that an attempt to uninstall or inhibit the ransomware’s functionality in any way would lead to an immediate deal-breaker.
Ransomware

• Like most malware, ransomware spreads through social engineering techniques and traps sent from mostly unsolicited sources, such as spam, phishing emails with malicious attachments, links to bogus websites, and malvertising.
Bitcoins

• A ransom message is displayed on the victim’s screen that demands a particular sum (usually between $100-1,500 for ordinary users) in exchange for a decryption key (usually claimed to be unique), thus completing a vicious cycle of cyber extortion crime done with the help of malware.
DDoS

• Depending on how huge the target is, rates for downing websites vary from as little as $5 to $100 per hour.

• DDoS dealers circulate everywhere online, in underground forums, and even on the public internet.
DDoS

• DDoS attacks may be time limited in order to achieve a maximum psychological effect.

• Cyber extortionists justify the ransom size with crude calculations of the approximate financial negative impact on the victim’s online business in the event of successful DDoS attack.
• Malware can even take control of a webcam and record its owner. Hundreds of Australian visitors of adult websites were literally caught with their pants down and later blackmailed.
Pornography

• Malware planted child pornography, which cannot be deleted easily, and asked for a fee, otherwise a notification would be forwarded to the authorities.
The SANS Institute assesses that thousands of organizations are paying off cyber extortionists. Seemingly, they prefer to choose the lesser evil, at least from their point of view.
Catching and Punishing

• Identification and arrest of cyber extortionists are low because they usually operate from countries other than those of their victims and use anonymous accounts and fake e-mail addresses.
Top Security Threats

1. Hacking
2. Data Leakage
3. Social Engineering
4. Corporate Account Takeover
5. Vendor Risk
6. ATM
7. Ransomware
Contact Info

• Dr. Kevin Streff

  – Dakota State University
    • kevin.streff@dsu.edu
    • 605.270.0790

  – Secure Banking Solutions, LLC
    • www.protectmybank.com
    • kevin@protectmybank.com
    • 605.270.0790
Threat Landscape and Globalization of Cybercrime

Dr. Kevin Streff, kevin.Streff@protectmybank.com
Founder, Secure Banking Solutions, www.protectmybank.com
Professor – Dakota State University, www.dsu.edu