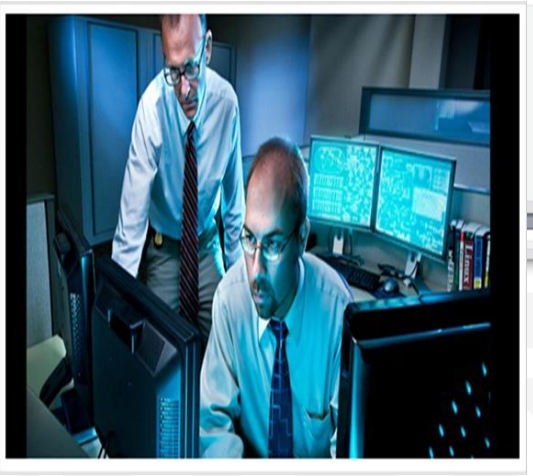


BEST PRACTICES IN COMBATING CYBERCRIME

SOUTHEAST BANKERS OUTREACH FORUM
SEPTEMBER 30, 2014

Tony DaSilva, AAP, CISA
Senior Examiner, Federal Reserve Bank of Atlanta

The opinions expressed are those of the presenter and are not those of the Federal Reserve Bank of Atlanta, the Federal Reserve System, or its Board of Governors.

FEDERAL RESERVE BANK of ATLANTA

TOPICS

- Cybercrime
- DoS & DDoS
- Fraud – The Primary Reason?
- Payments Fraud
- FFIEC Guidance June 28, 2011
- Requirements
- FRS Guidance
- Best Practices
- Cybersecurity Assessments

CYBERCRIME – WHERE & WHY?

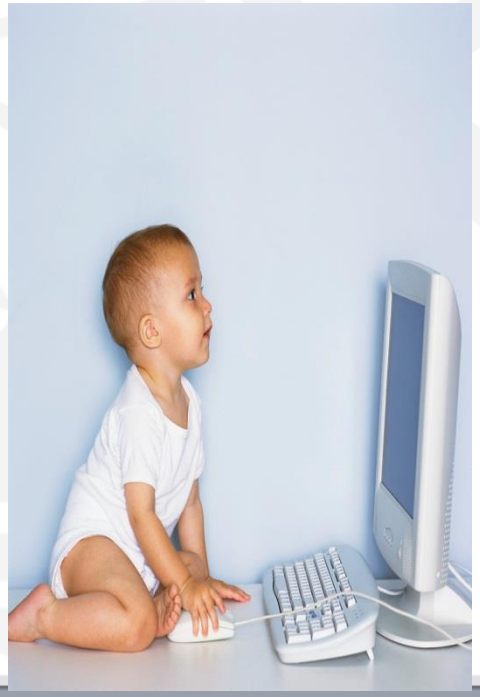
- Where do cyber attacks come from?
- What is the motivation?
  - Ideology – making a political statement
  - Extortion – demand for payment to avoid website attack
  - Competition – disrupt a competitors online services
  - Fraud – used as a tool to aid in unauthorized financial gain

TRENDS

HOW DO CYBER CRIMINALS GAIN ACCESS?

- Deception via DDoS
- Spam
- Phishing attempts
- Spoofed web pages
- Popup ads and warnings
- Malware (Trojans, worms, etc.)
- Theft (laptops, thumb drives, etc.)
- Email attachments
- Downloads
- Social mediums

DENIAL OF SERVICE ATTACK



DoS & DDoS

WHAT IS A DENIAL OF SERVICE ATTACK?

- **Objective(s):**
  - **Render a service unavailable**
  - **Cripple the infrastructure**
- **Typical targets:**
  - **Bank**
  - **Credit card payment servicers**
- **Mode of attack: Saturate the target with external requests for connectivity or communication**

READILY AVAILABLE MAYHEM

- Botnet malware development kits are available for purchase over the internet.
- The most recent versions may cost less than two thousand dollars.
- Older versions can be obtained for a few hundred dollars or for free.
- Botnet administrators also lease their botnets on a per-project basis.
- The DDoS attack application software called Low Orbit Ion Cannon is available for free download from sourceforge.net.

DDOS

- Despite the threat, there's still an effective way to protect your network against these attacks – network design decisions. The only way to protect against this is by having a system to identify the DDoS source and block it.

- This is easier said than done. Identifying the source of a DDoS attack can be tricky and, in most cases, involves tweaking an intrusion detection system (IDS) to differentiate between legitimate requests and attacks. Testing its effectiveness is not easy either. In any case, this will cause quite a few false positives.

FINANCIAL INSTITUTION MITIGATING ACTIONS

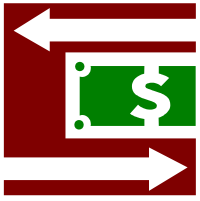
- Targeted banks have been very successful in employing numerous means of thwarting the DDoS attacks.
- There has been unprecedented sharing of information amongst the targeted banks as well as with their regulators and other government agencies.
- Banks are working with service providers to address the problems and to scrub/reduce the attack volumes.
- Leading DDoS protection providers (Prolexic, VeriSign, Akamai, etc.)
- Internet Service Providers - AT&T, Verizon, etc.

ADHERE TO THESE BEST PRACTICES

- Don’t assign all resources to DDoS mitigation.
- Dedicate at least some staff to watching entry systems during attacks.
- Make sure everything is patched.
- Keep your security up to date.
- Have dedicated DDoS protection.
- Scrambling to find a solution in the midst of an emergency only adds to the chaos - and any intended diversion.

PAYMENTS CYBERCRIME

ACH and Wire Transfers



TECHNOLOGY ENABLING FRAUD

As payments have evolved significantly, largely due to technological advancements, so has the sophistication of EFT fraud. Expertly crafted emails, malicious links on legitimate websites (such as social networking sites), and other methods are used to place malware within the networks of corporate customers. The malware then harvests security information, including login credentials, subsequently allowing the criminals to initiate electronic payments through hijacked accounts.

WHO

- **Law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses.**

- **Eastern European organized crimes groups are believed to be predominantly responsible for the activities that are also employing witting and unwitting accomplices in the United States (money mules) to receive, cash and forward payments from thousands to millions of dollars to overseas locations via popular money and wire transfer services.**

PROOF

- Eastern Europe is proudly refining its reputation as the world's top cyber thief place of business, as a group of Russian thieves was accused Tuesday (Aug. 5, 2014) of what is possibly the largest high-tech swindle to date. The take? About 1.2 billion usernames and passwords in addition to more than 500 million E-mail addresses, according to a report in The New York Times.

- The haul included "confidential material gathered from 420,000 websites, including household names, and small Internet sites."

JUST A FEW EXAMPLES

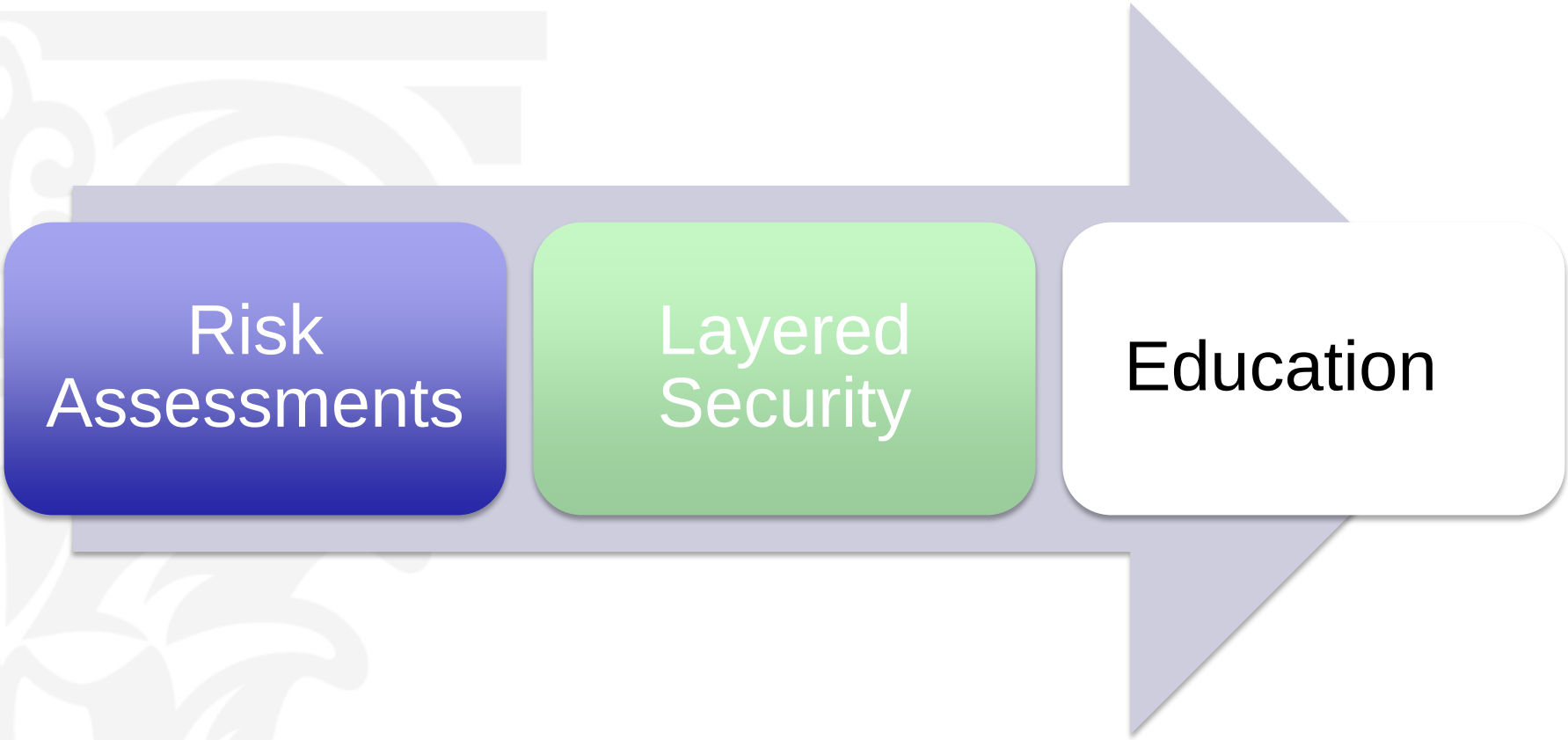
- SpyEye– A Zeus variant that "wakes-up" and steals credentials in real time.
- OddJob–Keeps online sessions open after logout by the user
- Tatanga– Caused a screen freeze or displays a "please wait" message as it conducts transactions in the background.
- Zeus Mitmo– Steals SMS one-time passwords via social engineering. Can utilize smishing to get user to download malware that forwards SMS messages
- Ramnit Worm – It was paired with source code from the Zeus botnet, and began targeting financial institution and has the ability to "bypass two-factor authentication and transaction signing systems."

THE FFIEC GUIDANCE SUPPLEMENT

Effective 1/1/2012:

On June 28, 2011, the Federal Financial Institutions Examination Council (FFIEC) released a supplement to the 2005 "Authentication in an Internet Banking Environment" guidance that describes the measures financial institutions should take to protect Internet banking customers from online fraud.

THREE PRIMARY REQUIREMENTS



FRS GUIDANCE

- **In recognition of the constant evolution in online threats, institutions should review and update risk assessments prior to implementing new electronic financial services or at least every twelve months.**

- **Institutions should implement a layered approach to security for high risk Internet-based transactions (i.e. access to sensitive customer information and/or movement of funds to other parties), including at a minimum processes to detect and respond to anomalous or suspicious behavior relating to initial login and to transactions that transfer funds to other parties.**

FRS GUIDANCE

- For business/commercial online accounts, layered security at a minimum should include enhanced controls for users granted access or change permissions to administrative and configuration functions.

- Institutions' customer awareness and education programs should clearly explain the applicability of Regulation E protections to each account type accessible over the Internet. Further, institutions should take steps to see that customers are informed of security control options and alternatives.

NOTE

- **Similar to the 2005 guidance, the June 2011 supplement applies to all electronic banking delivery channels, including the mobile banking channel.**

- **Whether financial institutions provide all or part of their electronic banking activities to customers through in-house systems or outsourced, service-provider arrangements, the institutions are responsible and accountable for conformance with the 2005 guidance and the 2011 supplement. VENDOR MANAGEMENT**

SPECIFIC PRACTICES TO MITIGATE RISKS

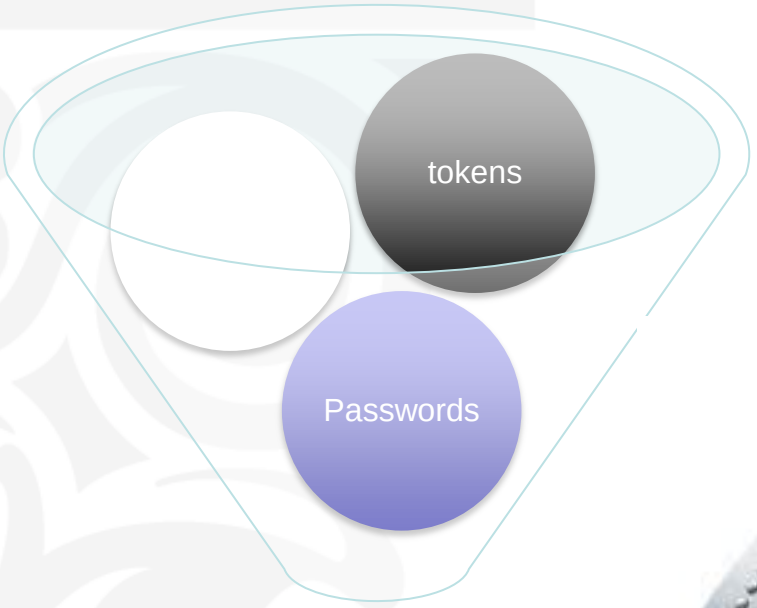
- Ensure centralized fraud detection systems facilitate monitoring across payment channels (i.e., ACH transactions, wire transfers, cards, checks, ATM transactions)
- Review security provisions in customer agreements (agreement alone may not alleviate bank from liability)
- Implement procedures for monitoring new and existing accounts (for new accounts, monitor for ACH credits "money mule activity")

SPECIFIC PRACTICES TO MITIGATE RISKS

Education should include:

- **Use of a single purpose, stand-alone computer for Internet banking (no email/web surfing/downloading)**
- **Monitor accounts daily for unusual activity – notify FI immediately of any errors**
- **Implement dual controls and separation of duties**
- **Maintain up-to-date anti-virus, spyware and firewall protection**
- **Use the strongest form of authentication provided by the bank**
- **Apply security patches quickly, consistently and comprehensively**
- **Contracts/Agreements**

OUT-OF-BAND



Internet

MOBILE

- Rapid adoption of mobile banking
- Increasing adoption of mobile banking by customers
- Majority of banks have adopted/are adopting mobile banking
- Mobile banking functionality is increasing
- Cyber criminals are following the money
- Banks need to assess and manage associated risks

MOBILE MALWARE RISKS TO FINANCIAL INSTITUTIONS

- Account takeovers/fraudulent electronic funds transfers
- Exposure of nonpublic customer information
- Distributed denial-of-service attacks
- Destruction/theft/leakage of internal bank information
- Impersonation of bank communications
- Another expense and operational challenge

RISKS & MITIGATION

Malware and risks

- Account takeovers
- Credit theft and identity spoofing
- Payment fraud
- Mobile wallets
- Mobile e-commerce
- Browser and application spoofing

Security and mitigation

- Content security
- Data loss protection
- Malware detection
- Loss and theft response
- Layered security
- Risk assess accounts
- Anomaly detection

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

February 12, 2014

FRAMEWORK

The Framework Core consists of five concurrent & continuous functions:

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

CYBERSECURITY

The process for managing cyber threats and vulnerabilities and for protecting information and information systems by identifying, defending against, responding to, and recovering from attacks.

CYBERSECURITY PREPAREDNESS

In terms of:

- **Risk exposure,**
- **Risk management, including controls to address the risks, and**
- **Knowledge gaps and proposed strategies to address the gaps.**

ASSESSMENT OF CYBER SECURITY

- Risk Management & Oversight
- Threat Intelligence & Collaboration
- Security Controls
- External Dependency & Vendor Management
- Incident Management

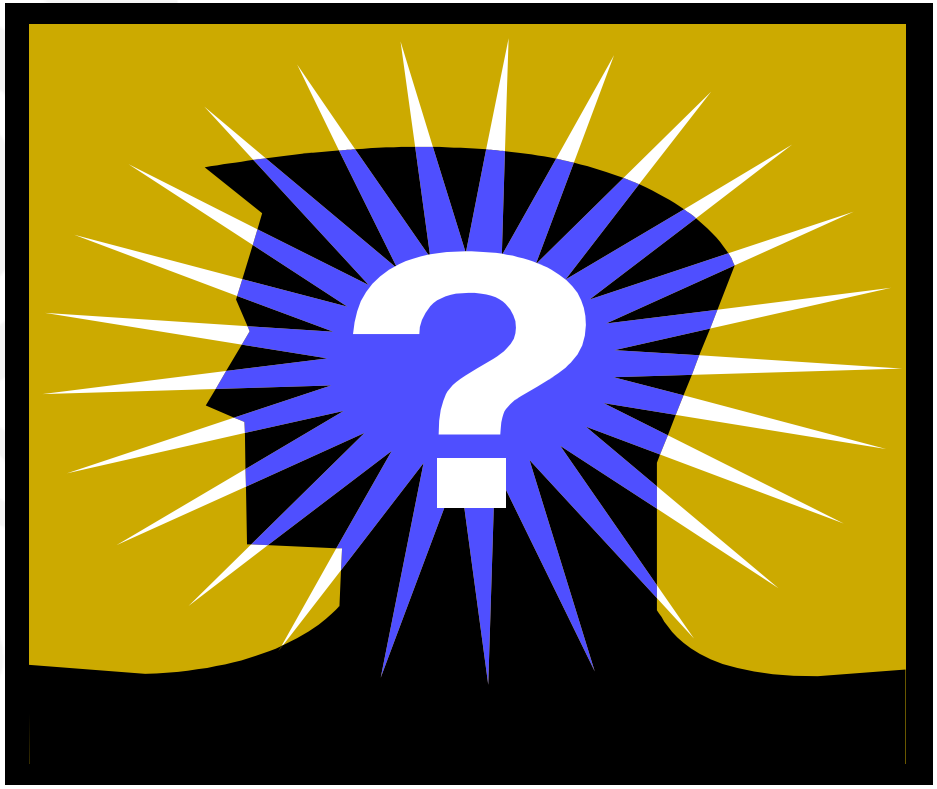
BOARD OF DIRECTORS

- Directors need to understand and approach as an ERM issue, not just an IT issue.
- Directors should understand the legal implications of cyber-risks
- Boards should have adequate access to cybersecurity expertise
- Discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda
- Directors should set the expectation that management will establish an enterprise wide, cyber-risk management framework
- Discussions of cyber-risks between boards and senior managers should include identification of which risks to avoid, accept, mitigate, or transfer.

CONTROLS

- ***Preventative Controls*** **- impede threats from exploiting a weakness**
- ***Detective Controls*** **- identify presence of a vulnerability or threat**
- ***Corrective Controls*** **- recovery from cyber attacks or threat mitigation**

QUESTIONS



FOR MORE INFORMATION

FBI Alert: Fraudulent ACH Transfers

http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm

FDIC Special Alert: Fraudulent Electronic Funds Transfers

http://www.fdic.gov/news/news/SpecialAlert/2009/sa09147.html

FDIC Special Alert SA-185-2009 Fraudulent Funds Transfer Schemes

http://www.fdic.gov/news/news/SpecialAlert/2009/sa09185.html

NACHA Bulletin: Corporate Account Takeovers

http://www.nacha.org/docs/NACHA%20Operations%20Bulletin%20-%20Corporate%20Account%20Takeover%20-%20December%202,%202009.pdf

FOR MORE INFORMATION

FFIEC Guidance Authentication in an Internet Banking Environment

http://www.ffiec.gov/press/pr101205.htm

Identity Theft Red Flags Rule

http://www.federalreserve.gov/BoardDocs/srletters/2008/SR0807.htm

FDIC Guidance on Mitigating Risks from Spyware

http://www.fdic.gov/news/news/financial/2005/fil6605.html

Interagency Guidelines Establishing Information Security Standards (GLBA)

http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm

REGULATORY GUIDANCE

- SR 13-19: Guidance on Managing Outsourcing Risk
- SR 12-14: Revised Guidance on Supervision of Technology Service Providers
- SR 11-9: Interagency Supplement to Authentication in an Internet Banking Environment
- SR 09-2: FFIEC Guidance Addressing Risk Management of Remote Deposit Capture
- SR 06-13: Q&A Related to Interagency Guidance on Authentication in an Internet Banking Environment

REGULATORY GUIDANCE CONTINUED

- SR 05-23: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
- SR 05-19: Interagency Guidance on Authentication in an Internet Banking Environment
- FFIEC Risk Management of Remote Deposit Capture
- FFIEC Information Security Booklet
- SR 01-15: Standards for Safeguarding Customer Information
- SR 01-11: Identity Theft and Pretext Calling—(attachment) Interagency Guidelines Establishing Standards for Safeguarding Customer Information