PACB One-Day Cybersecurity Workshop

INCIDENT RESPONSE AND CYBERSECURITY!

PRESENTED BY:
JON WALDMAN, SBS – CISA, CRISC
Agenda

• What is cybersecurity?
• What do I need to know about cybersecurity?
• What are some of today’s cybersecurity threats?
• How do I build a useful Information Security Program?
• How do I build a Risk Assessment that helps me make decisions?
• People are the weakest link; how do I prepare and train my people to mitigate risk?
• Bad things are going to happen; it’s inevitable. How do I plan for and prepare to respond to incidents?
Incident Response
HOW DO YOU PLAN TO FAIL WELL?
Incident Response Components

Fraud Detection
- DDOS
- SANS Automation
- Automated Fraud Detection

Incident Response
- Policy / Framework
- Response Procedures
- Investigations
- Forensics
Distributed DoS

• Denial of Service – (DoS) is an attempt to make a machine or network resource unavailable to its intended user.

• Distributed - attack is one in which a multitude of compromised systems attack a single target, thereby causing a denial of service.
Distributed DoS Targets

- Hacktivist group Izz ad-Din al-Qassam Cyber Fighters Group
- Dec. 11, named five targets: Bank of America, JPMorgan Chase, PNC Financial Services, U.S. Bancorp and SunTrust Banks.
Value of Hacked PC

- Phishing Site
- Malware Download Site
- Warez/Piracy Server
- Child Pornography Server
- Spam Site
- Web Server

- Bot Activity
  - DDoS Extortion Zombie
  - Click Fraud Zombie
  - Anonymization Proxy
  - CAPTCHA Solving Zombie

- Spam Zombie
- E-Mail Attacks

- Financial Credentials
  - Credit Card Data
  - Stock Trading Account
  - Mutual Fund/401k Account

- Online Gaming Characters
- Online Gaming Goods/Currency
- PC Game License Keys
- Operating System License Key
- Virtual Goods

- Account Credentials
  - Web Site FTP Credentials
  - Skype/VoIP Credentials
  - Client Side Encryption Certificates

- Financial Statements
  - eBay/Paypal False Auctions

- Webmail Spam
  - Stranded Abroad Advance Scams
  - Harvesting E-mail Contacts
  - Harvesting Associated Accounts
  - Access to Corporate E-mail

- Hostage Attacks
- Fake Antivirus
  - Ransomware
  - Email Account Ransom
  - Webcam Image Extortion

- Facebook
  - Twitter
  - LinkedIn
  - Google+ 

- Reputation Hijacking
Denial of Service Attack

Attacker

Attacker sends command for his bots to attack bank.

Compromised PC

Compromised PC

Compromised PC

Compromised PC

Compromised PC

Internet

Thousands of requests are sent to the bank website simultaneously.

Bank

Bank is flooded with requests and cannot operate effectively.
Wells Fargo

• Wells Fargo – December 18th, 2012

• "We're seeing an unusually high volume of traffic, which is creating slow or intermittent access to our website for some online customers,"

• "The vast majority of customers are not impacted, but for those who are, we encourage them to access their accounts through our stores, ATMs or by phone as we work to resolve the issue." - Wells Fargo spokeswoman Sara Hawkins

• Arbor Networks, a networking security company, said some of the DDOS attacks peaked at 60Gbps, up from an average attack rate of just 1.67 Gbps in September.
New Norm

• In NTP attacks, similar to DNS amplification attacks, the attacker sends a small forged packet that requests a large amount of data be sent to the target IP Address. (Krebs)

• **200-400 Gbps**
Cyber criminals have found yet another way to steal your hard-earned money: a recent phishing scheme involves spam e-mails—purportedly from the National Automated Clearing House Association (NACHA), the Federal Reserve Bank, or the Federal Deposit Insurance Corporation (FDIC)—that can infect recipients' computers with malware and allow access to their bank accounts.

The malware is appropriately called "Gameover" because once it's on your computer, it can steal usernames and passwords and defeat common methods of user authentication employed by financial institutions. And once the crooks get into your bank account, it's definitely "game over".

Gameover is a newer variant of the Zeus malware, which was created several years ago and specifically targeted banking information.

**How the scheme works:** Typically, you receive an unsolicited e-mail from NACHA, the Federal Reserve, or the FDIC telling you that there's a problem with your bank account or a recent ACH transaction. (ACH stands for Automated Clearing House, a network for a wide variety of financial transactions in the United States.) The sender includes a link in the e-mail that will supposedly help you resolve whatever the issue is. Unfortunately, the link goes to a phony website, and once you're there, you inadvertently download the Gameover malware, which promptly infects your computer and steals your banking information.

After the perpetrators access your account, they conduct what's called a distributed denial of service, or DDoS, attack using a botnet, which involves multiple computers flooding the financial institution's server with traffic in an effort to deny legitimate users access to the site—probably in an attempt to deflect attention from what the bad guys are doing.

**But that's not the end of the scheme:** Recent investigations have shown that some of the funds stolen from bank accounts go towards the purchase of precious stones and expensive watches from high-end jewelry stores. The criminals contact these jewelry stores, tell them what they'd like to buy, and

**How Can You Protect Yourself?**

- Obviously, make sure your computer's anti-virus software is up to date.
- Don't click on e-mail attachments from unsolicited senders. NACHA, FDIC, and the Federal Reserve all say they don't send out unsolicited e-mails to bank account holders. If you want to confirm there's a problem with your account or one of your recent transactions, contact your financial institution directly.
- Don't accept unsolicited jobs online that require you to receive funds from third parties.
- Keep pornography sites off your system. This is a telltale sign of a botnet.
Resources


- DDOS protection services - http://ddos-protection-services-review.toptenreviews.com
Network Segmentation
Host Based Intrusion Prevention (HIPS)

• Signature based HIP’s
  ◦ Protects against known attacks using IPS signatures.

• Behavioral based HIP’s
  ◦ Detect anomalies or behavioral characteristics of applications, network traffic or other actions that are consistent with attacks.

• Products
  ◦ Most Endpoint Software Providers have this capability with a central alerting system
SIEM

• Security Information and Event Management
• Gathering, analyzing and presenting information from many network and security devices.
• Advanced Log Correlation
• Solution Ideas:
  • https://www3.trustwave.com/siem/
  • http://www.manageengine.com/products/eventlog/
Application Whitelisting

“Antivirus is dead, says maker of Norton Antivirus – WSJ”
Transaction Monitoring

http://www.protectmybank.com/
Critical Control 1: Inventory of Authorized and Unauthorized Devices
Critical Control 2: Inventory of Authorized and Unauthorized Software
Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Critical Control 4: Continuous Vulnerability Assessment and Remediation
Critical Control 5: Malware Defenses
Critical Control 6: Application Software Security
Critical Control 7: Wireless Device Control
Critical Control 8: Data Recovery Capability
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
SANS Top 20

• Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
• Critical Control 12: Controlled Use of Administrative Privileges
• Critical Control 13: Boundary Defense
• Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
• Critical Control 15: Controlled Access Based on the Need to Know
• Critical Control 16: Account Monitoring and Control
• Critical Control 17: Data Loss Prevention
• Critical Control 18: Incident Response and Management
• Critical Control 19: Secure Network Engineering
• Critical Control 20: Penetration Tests and Red Team Exercises
Security Process


Incident Response Planning

At a minimum, an institution’s response program should contain procedures for:

- **Assessing the nature and scope** of an incident and identifying what customer information systems and types of customer information have been accessed or misused;
- **Notifying its primary federal regulator** as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
- Consistent with the agencies’ Suspicious Activity Report (SAR) regulations, filing a timely SAR, and in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notifying appropriate law enforcement authorities;
- **Taking appropriate steps** to contain and control the incident to prevent further unauthorized access to or use of customer information; and
- **Notifying customers** when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it. (FDIC FIL-27-2005)
Common Issues

- Does not address specific threats
- Does not have procedures for evaluating if customer information was exposed
- Does not have procedures for SAR
- No standard incident response form
- Missing Forensics Support
- Not tested
Creating an Incident Response Policy

- Incident Response Policy should contain at a minimum:
  - Overview
  - Purpose
  - Responsibilities
  - Incident Response Plan Requirements
  - Testing Requirements
Incident Response Plan
Requirements

• Incident Response Policy should set Plan requirements that include:
  ◦ Assess the nature and scope of the incident
  ◦ Escalate response procedures accordingly
  ◦ Take appropriate steps to contain and control the incident
  ◦ Notify primary regulator as soon as possible
  ◦ File a Suspicious Activity Report (SAR)
  ◦ Notify customers when warranted, the notice shall contain:
    ▪ Description of the incident
    ▪ Type of information subject to unauthorized access
    ▪ Containment measures taken
    ▪ Telephone number for information and assistance
    ▪ Remind customers to vigilantly monitor credit / debit activities for the next 12 to 24 months.
**Types of Incidents**

- **Incident Types Include:**
  - **General Information Technology Incidents**
    - Internal breach or incident: malware, DDOS, internal misuse, network/system compromise
  - **Service Provider Incidents**
    - Outsourced Core Banking System provider (compromised)
    - Credit Card / Debit Card breach
    - Online Banking System
  - **Physical Theft or Loss**
    - Laptop or Mobile device
    - Backup tapes
    - USB storage device
    - Paper Documents
Procedures for Handling General Incidents

- General Incidents Include:
  - Malicious Code
  - Inappropriate Usage
  - Unauthorized Access
  - Zero-Day Threat (Heartbleed bug, IE bug,...)
  - Denial of Service (DoS)
  - Distributed Denial of Service (DDoS)
  - Power Disruptions or loss of Internet Connectivity.
Example - Malicious Code

1. Report the incident to the Information Security Officer (ISO)
2. Contain the incident
   • Identify infected systems
   • Disconnect infected systems from the network
   • Mitigate vulnerabilities that were exploited by the malicious code
   • If necessary, block the transmission mechanisms for the malicious code
3. Eradicate the incident
   • Disinfect, quarantine, delete, and replace infected files
   • Mitigate the exploited vulnerabilities for other hosts within the Bank
4. Document Incident Response Form
5. Recover from the incident
   • Return the systems to the network
   • Confirm that the affected systems are functioning normally
6. Create a follow-up report
7. Hold a lessons learned meeting
Procedures for Handling Specific Incidents

• Specific Incidents Include:
  ◦ FedLine Advantage
    ▪ ACH
    ▪ Wire Transfer
  ◦ Corporate Account Takeover (CATO)
  ◦ ACH Originator/Third Party Senders
Example - FedLine Advantage

Unauthorized Access Incident

1. Report the incident to the Information Security Officer (ISO)
2. Perform an initial containment of the incident
   • Power down and disconnect the FedLine Advantage VPN device.
3. Acquire, preserve, secure, and document evidence
4. Document Incident Response Form
5. Certificate Revocation
   • Request to revoke all certificates suspected of being compromised from the Registration Authority.
6. Secure Sensitive Customer Information
   • Ensure the security of customer information
7. Confirm the containment of the incident
   • Further analyze the incident and determine if containment was sufficient (including checking other systems for signs of intrusion)
   • Implement additional containment measures if necessary
8. Eradicate the incident
   • Identify and mitigate all vulnerabilities that were exploited
   • Remove components of the incident from systems
   • Delete and destroy all copies of the revoked certificates and/or tokens.
9. Recover from the incident
   • Reconnect and power on the FedLine Advantage VPN device.
   • Confirm that the systems are functioning normally
   • If necessary, implement additional monitoring to look for future related activity
10. Customer Notification
11. Suspicious Activity Report
12. Create a follow-up report
13. Hold a lessons learned meeting
Procedures for Handling Service Provider Incidents

- Service Provider Incidents Include:
  - Debit Cards/ Credit Cards
  - Internet Banking provider
  - Outsourced Core Banking System
Example - Online Banking

Unauthorized Access Incident

1. Report the incident to the Information Security Officer (ISO)
2. Complete Incident Response Form
3. Notify Incident Response Team
4. Notify Internet Banking personnel
5. Contact the FDIC. They will most likely have additional requirements of the Bank; complete those requirements before proceeding with any procedure.
6. Reset Passwords
   • All accounts suspected of unauthorized access must have passwords reset on the Management Console Admin Platform Website.
7. Notify customers; see Customer Notification procedures
   • Use Generic Customer Notification Letter or contact customer via electronic mail with details of the incident and their new password.
8. Suspicious Activity Report
9. Create a follow-up report
10. Hold a lessons learned meeting
Customer Information Evaluation

1. Evaluate the incident to determine if unauthorized access to or use of sensitive customer information has occurred.
   - NO – The security of customer information has not been breached, resume previous incident response procedure. However, if the Bank becomes aware a breach in customer information security at a later time, it must resume this procedure.
   - YES – Continue with this procedure.

2. Notify Incident Response Team and Board of Directors.

3. Complete Incident Response Form.

4. Contact the FDIC. They will most likely have additional requirements of the Bank; complete those requirements before proceeding with any procedure. For assistance in contacting the regulators by email, please reference the Communication to Regulators Letter. This letter can also be used as a guide when calling incidents into the regulators.

5. Return to previous incident response procedure and complete the remaining steps. After completing those procedures resume this procedure.


7. Complete the Suspicious Activities Report (SAR)
Cyber Incident Investigation

• Insure your Incident Response Plan addresses
  ◦ The Bank
  ◦ Customers
  ◦ Third Parties

• Timely investigation is key to success

• Ensure containment, do more than you think is necessary to ensure your problems do not increase

• Seek professional assistance
Computer Forensics

- Forensics is the process of using **scientific knowledge** for collecting, analyzing, and presenting evidence to the courts.
- A component of your defense-in-depth strategy.
- You **may not know** the **extent of a breach** without it.
- **Don’t touch** the PC until you consult an expert, often times shutting it down, moving files, or cleaning up malware can destroy evidence and the change of custody.
- Addresses fraud, intrusion, insider threat, phishing and other cyber-crimes
Computer Forensics

Best Practices

- Only **quarantine** the incident, **preserve** the evidence
- **Contact an expert** forensics resource or have one on staff
- If not, at least create **forensic image** or keep the hard drive for a period of time, for future investigations
- When contained and imaged, **rebuild** the system for scratch.
4 Main Principles

The four main principles from this guide (with references to law enforcement removed) are as follows:

1. **No action should change data** held on a computer or storage media which may be subsequently relied upon in court.

2. In circumstances where a person finds it necessary to access original data held on a computer or storage media, that **person must be competent to do so** and be able to give evidence explaining the relevance and the implications of their actions.

3. An **audit trail or other record** of all processes applied to computer-based electronic evidence should be created and preserved. An independent third-party should be able to examine those processes and achieve the same result.

4. The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

https://forensiccontrol.com/resources/beginners-guide-computer-forensics/
Forensic Assistance

- Hard Drive Digital Preservation and Imaging
- Data Preservation and Imaging Training
- Computer Forensic Investigation and Data Recovery
- Disk Forensics
- Network and Internet Forensics
- Email Forensics
- Malware Impact Analysis

- Digital Forensic Retainers
- [https://www.protectmybank.com/services/cyber-security-retainer/](https://www.protectmybank.com/services/cyber-security-retainer/)
Comprehensive Incident Response

• Don’t just address:
  ◦ Bank Incidents
  ◦ Third Party Incidents
  ◦ Customer Incidents

• From the perspective of the Bank.

• Build or ensure each layer has their own procedures:
  ◦ Customer’s IRP
  ◦ Third Party’s IRP
Customers

FFIEC Supplement to Authentication in an Internet Banking Environment requires:

• A listing of institutional contacts for customers’ discretionary use in the event they notice suspicious account activity or experience customer information security-related events.
Dear Customer,

In an interest to protect your funds we would like to encourage you to contact us immediately whenever you notice specious activity.

Monitor high risk systems, such as those which transfer funds. Review account activity often.

Call 555-555-5555 and ask for the security officer or inform the caller that you suspect fraud.

Timely response to fraudulent activity is critical in reducing the impact of fraud.

- Banker
Third Party Management

• Contractual Statements
  ◦ Require notification in the event of a breach
  ◦ Establish a timeframe
  ◦ Establish a procedure for who is to be notified and how
  ◦ Establish penalties for a breach or recourse abilities by the bank.

• Risk Assessment
  ◦ Verify the existence and adequacy of their plan
  ◦ Request regular testing reports
  ◦ Request independent audit reports covering the plan
Response Toolbox

• What tools will you need at your institution to respond adequately?

• Build these items into a toolbox:
  ◦ Bootable device for scanning computers
  ◦ Forensic imaging equipment
  ◦ Extra hard drives
  ◦ System images for reloading computers quickly
  ◦ Network backup of local documents
  ◦ Network monitoring tools
  ◦ Log analysis software
  ◦ Log analysis cheat sheet/error ID definitions
  ◦ Common port cheat sheet
  ◦ Malware documentation library
Security Incidents

“We will bankrupt ourselves in the vain search for absolute security.” – Dwight D. Eisenhower

A cyber security incident at some point is almost certain.

Incident Response Procedures are a required item that makes good security sense.

Treat it just like a criminal investigation.
- Involve law enforcement and forensic experts
- Identify, Collect, and Preserve evidence
- Document, Document, Document
- Interview, photograph, video record as needed
Information Sharing and Analysis

Purpose: “share risk and threat information“

https://www.fsisac.com/

https://www.us-cert.gov/

Brian Krebs
http://krebsonsecurity.com

www.protectmybank.com
Summary

• What is cybersecurity?
• What do I need to know about cybersecurity?
• What are some of today’s cybersecurity threats?
• How do I build a useful Information Security Program?
• How do I build a Risk Assessment that helps me make decisions?
• People are the weakest link; how do I prepare and train my people to mitigate risk?
• Bad things are going to happen; it’s inevitable. How do I plan for and prepare to respond to incidents?
That’s all she wrote…

• Any questions, comments, or concerns?

• Also, for a much deeper dive on Information Security specifically for Community Banks, check out our new Community Bank Certification Programs!
  ◦ CCB Vendor Manager (CCBVM)
  ◦ CCB Security Professional (CCBSP)
  ◦ CCB Technical Professional (CCBTP)
  ◦ CCB Ethical Hacker (CCBEH)
  ◦ CCB Incident Responder (CCBIH)
  ◦ Ask us about it!

• Contact info:
  ◦ Jon Waldman, Partner
    ▪ jon@protectmybank.com
    ▪ 605-380-8897