BKD LLP

CPAs & Advisors

BKD THOUGHTWARE®

THE EVOLUTION OF CYBERSECURITY: IDENTIFICATION OF BEST PRACTICES

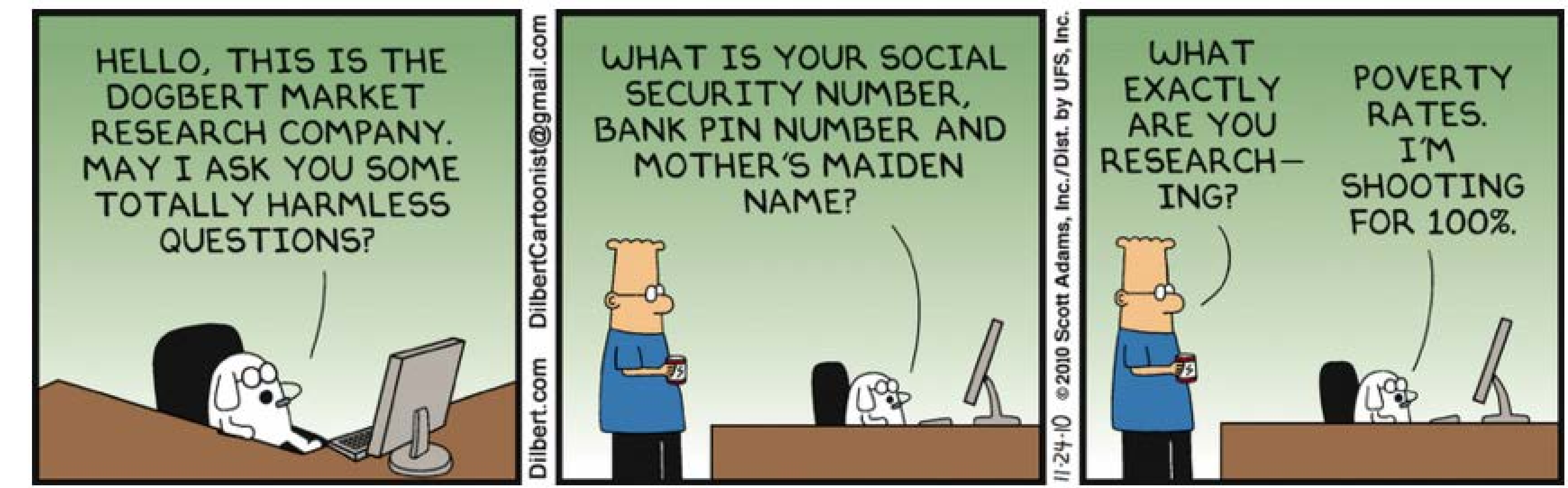
Ron Hulshizer

Managing Director

IT Risk Services

State IA Advisory Board – October 26, 2016

Technology – The Dark Side


HELLO, THIS IS THE DOGBERT MARKET RESEARCH COMPANY. MAY I ASK YOU SOME TOTALLY HARMLESS QUESTIONS?
Dilbert.com DilbertCartoonist@gmail.com
WHAT IS YOUR SOCIAL SECURITY NUMBER, BANK PIN NUMBER AND MOTHER'S MAIDEN NAME?
11-24-10 © 2010 Scott Adams, Inc./Dist. by UFS, Inc.
WHAT EXACTLY ARE YOU RESEARCH–ING?
POVERTY RATES. I'M SHOOTING FOR 100%.

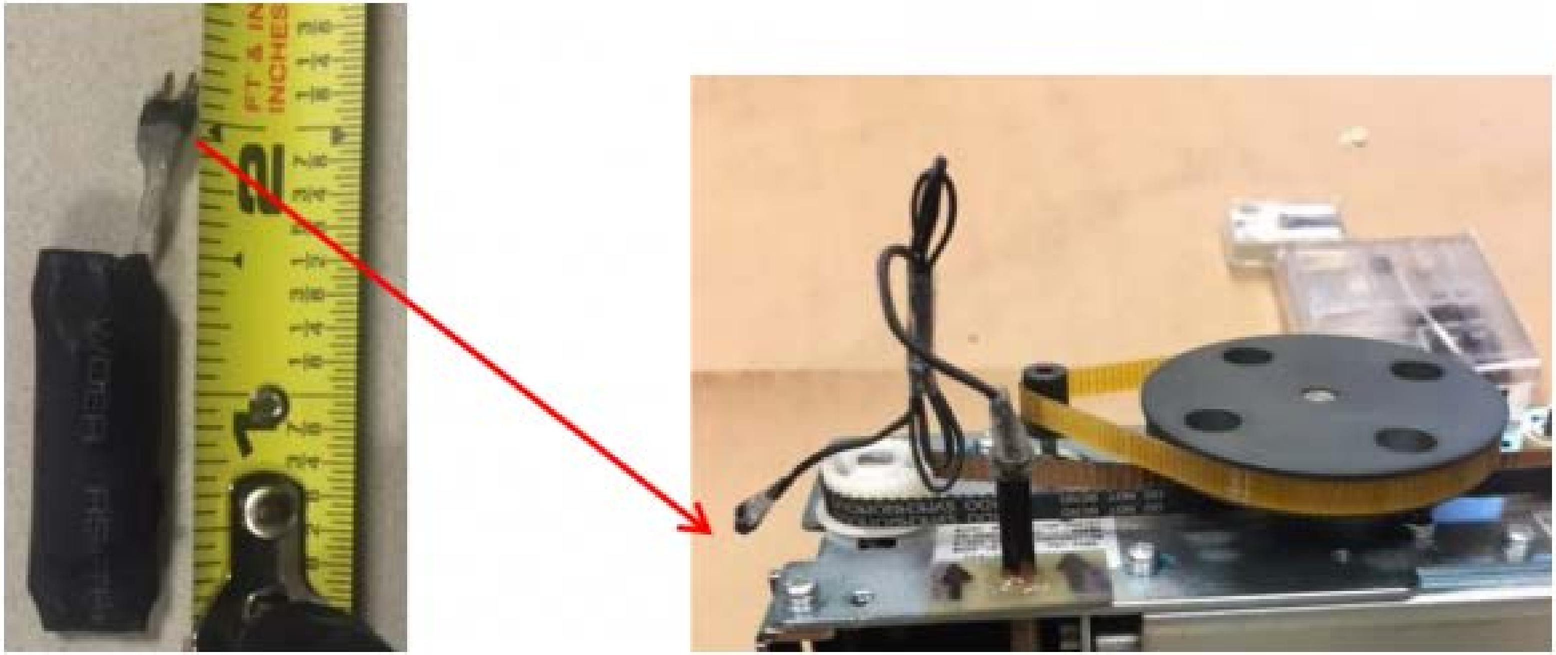
Cybersecurity

- Objectives
  - Review the dark side of security
  - Cover the weakest link to security
  - Cybersecurity Top Ten List

IT Security – Starts with Threats and Risk

- Wireless cantenna
  - What you may or may not see
- Portable tablets
  - Apple vs. Microsoft vs. Google
- Key logger/Physical Information/Cell Phones
  - Classic threats
- "Security testing" devices
  - Unintended uses
- Drones
  - Unintended uses

ATM Periscope Skimmer



At left, the skimming control device. Pictured right is the skimming control device with wires protruding from the periscope. These were recovered from a cash machine in Connecticut.

Source: Krebs On Security – September 2016

IT Security – Starts with Risk

- Employees
  - Weakest link
- Change
  - Enemy of security

Social Engineering

- CEO Scam
  - Education and Awareness
  - Verbal Approval
- Elderly Abuse
  - Education and Awareness
- Wire Fraud
  - “Know who you are dealing with”

Good guys versus the Bad Guys

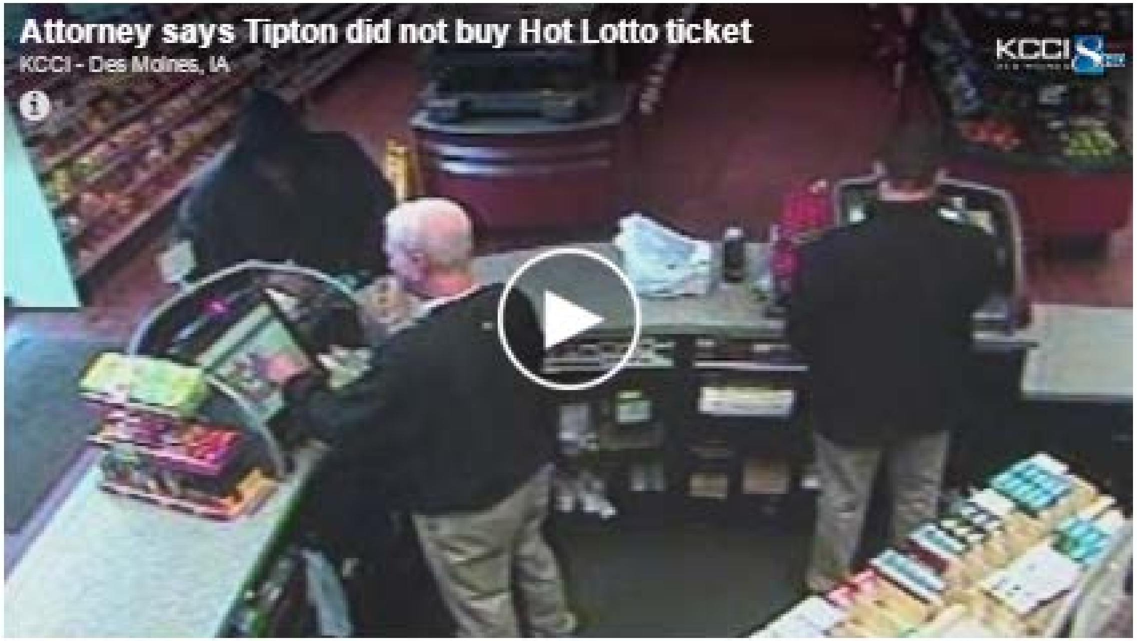
- White Hat
  - A security consultant during the day
- Black Hat
  - A hacker after midnight
- Grey Hat
  - A Security Consultant during the day, a hacker after midnight

Eddie Tipton

- IOWA Lottery – IT Security Director

Eddie Tipton

- Purchasing lottery ticket at Des Moines convenience store

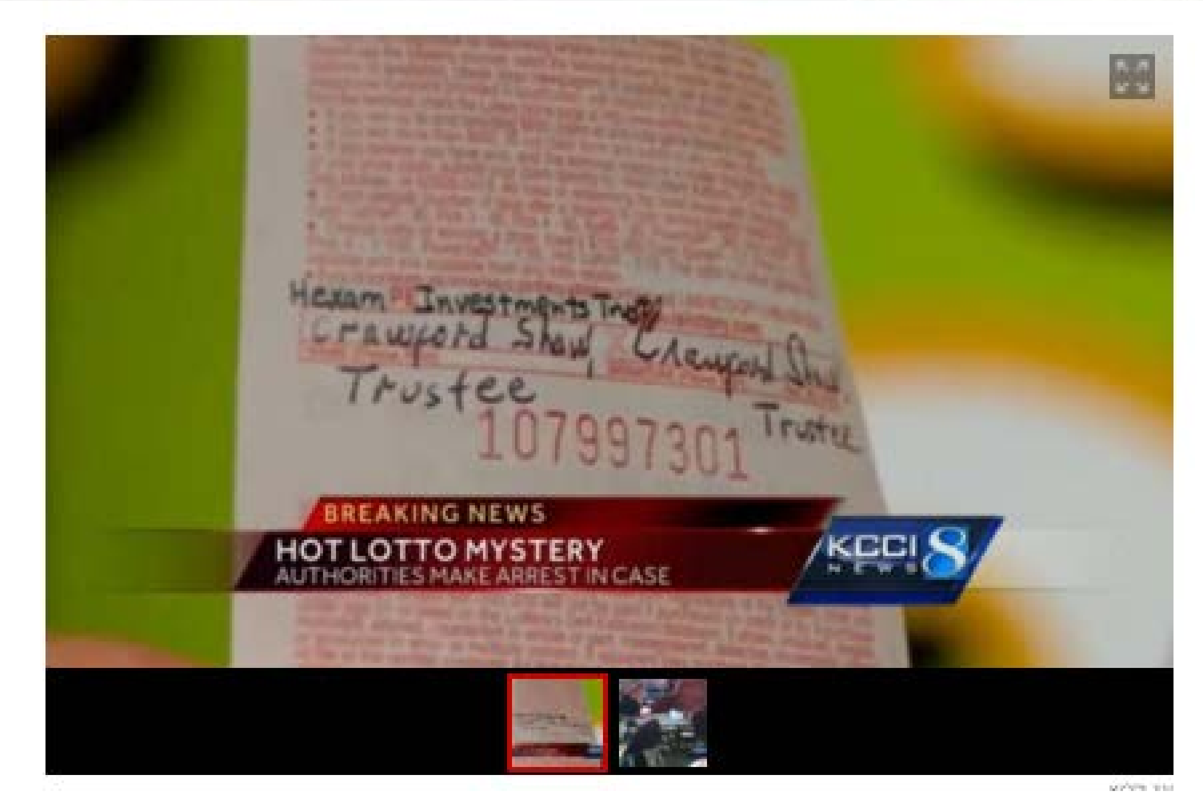


Attorney says Tipton did not buy Hot Lotto ticket

KCCI - Des Moines, IA

Lottery Ticket

- Sent to NY Attorney Crawford Shaw



Eddie Tipton

- OOPS – Sentenced to 10 Years in September

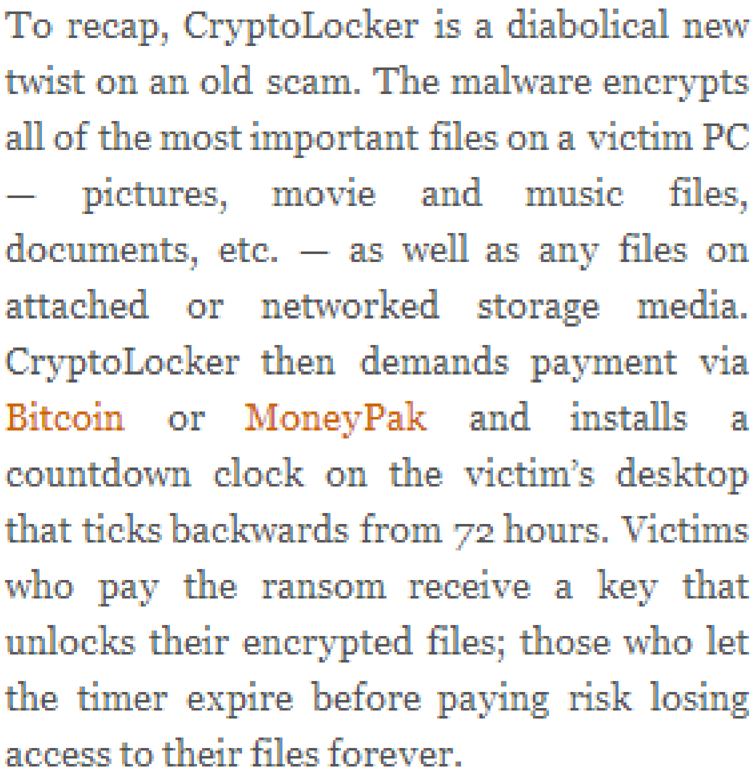
Update July 2016

- Tipton's attorney, Dean Stowers, argued before the court last month that there was no direct evidence to show that Tipton had changed the computer number-picking program or had any connection with the people who tried to cash in the $16.5 million Iowa Hot Lotto lottery ticket. Iowa lottery officials never paid the jackpot because they couldn't confirm whether the ticket was legally purchased or possessed.
- The appeals court justices found in addition to filing charge too late, there was no firm evidence that Tipton was involved in the scheme to cash in the winning ticket and said that charge must be dismissed.
- The court found there was enough evidence to substantiate the computer tampering conviction.
- "Based on this circumstantial evidence, the jury reasonably could have found that Tipton tampered with the random number generator computers with the intent to influence the lottery winnings," the court found.
- Tipton faces a second trial in Iowa in February on ongoing criminal conduct and money laundering charges alleging that he manipulated computers to fix lottery games in Colorado, Kansas, Oklahoma and Wisconsin, and then worked with others to cash the tickets.

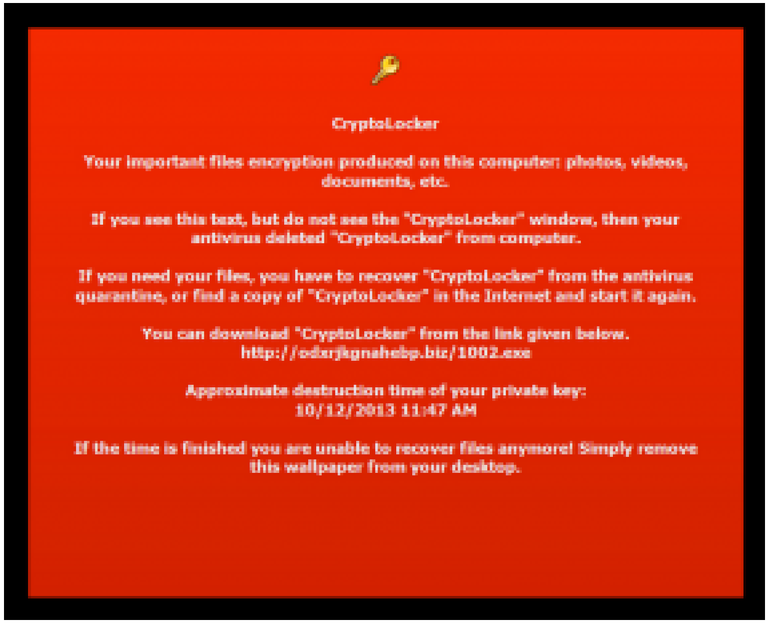
Malware

- Email – FedEx package is on its way
- Employee clicks on link
- Crypto Locker - Payload is downloaded
- Spreads to other computers on network
- Extortion message received - Bitcoin

CryptoLocker



To recap, CryptoLocker is a diabolical new twist on an old scam. The malware encrypts all of the most important files on a victim PC — pictures, movie and music files, documents, etc. — as well as any files on attached or networked storage media. CryptoLocker then demands payment via Bitcoin or MoneyPak and installs a countdown clock on the victim's desktop that ticks backwards from 72 hours. Victims who pay the ransom receive a key that unlocks their encrypted files; those who let the timer expire before paying risk losing access to their files forever.



CryptoLocker

Your important files encryption produced on this computer: photos, videos, documents, etc.

If you see this text, but do not see the "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer.

If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, or find a copy of "CryptoLocker" in the Internet and start it again.

You can download "CryptoLocker" from the link given below.
http://odxrjkgnahebp.biz/1002.exe

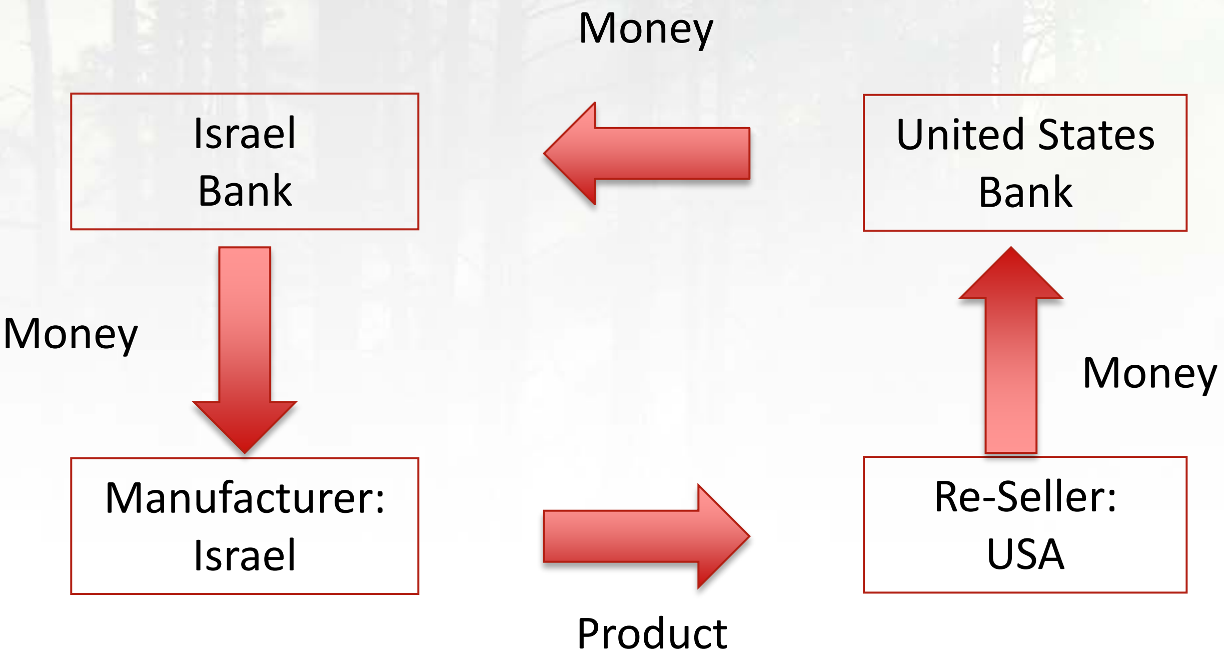
Approximate destruction time of your private key:
10/12/2013 11:47 AM

If the time is finished you are unable to recover files anymore! Simply remove this wallpaper from your desktop.

This message is left by CryptoLocker for victims whose antivirus software removes the file needed to pay the ransom.

Source: Krebs On Security, November 6, 2013

Example of Wire fraud



Money

Israel Bank

United States Bank

Money

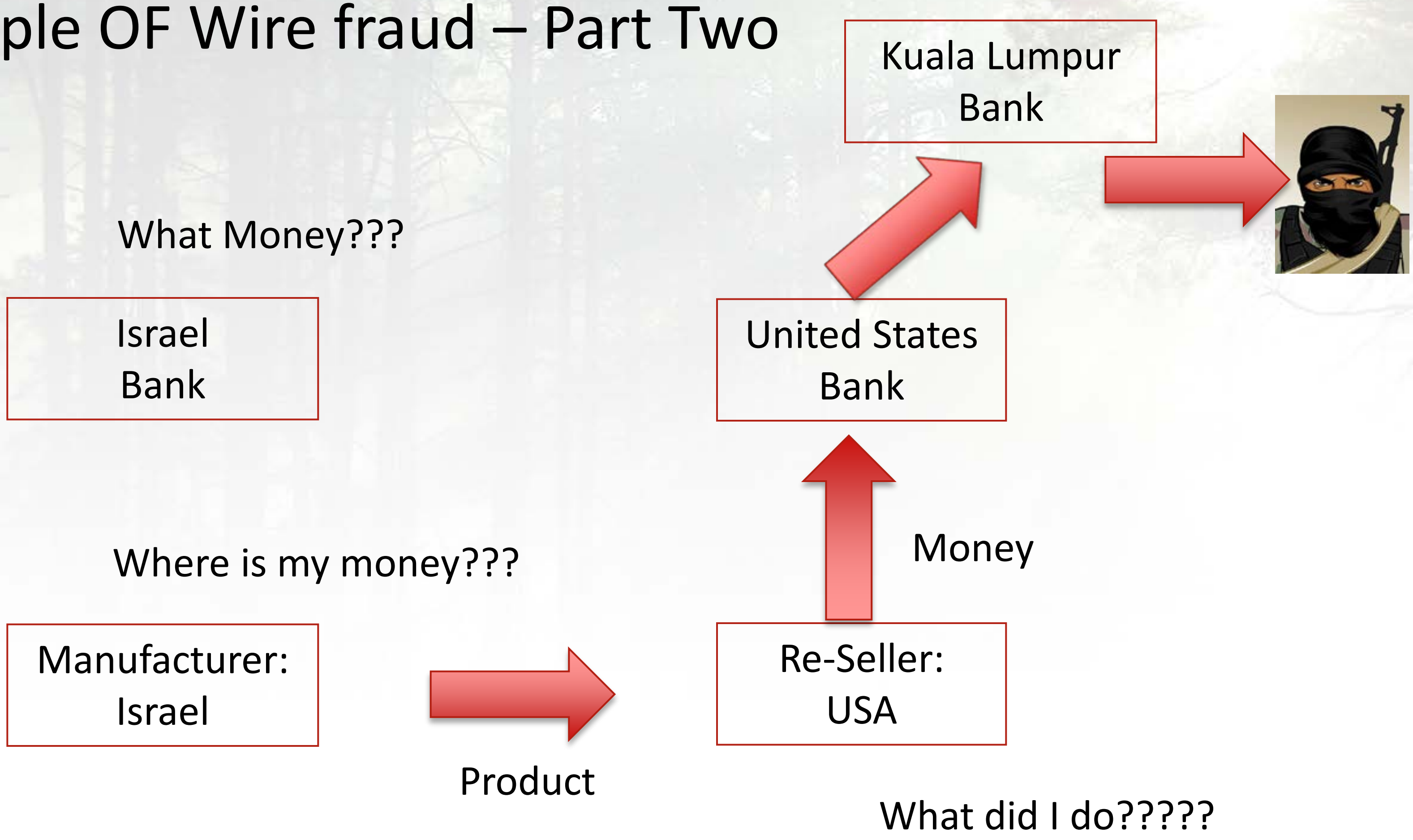
Money

Manufacturer: Israel

Re-Seller: USA

Product

Example OF Wire fraud – Part Two



Kuala Lumpur Bank

What Money???

Israel Bank

United States Bank

Money

Where is my money???

Manufacturer: Israel

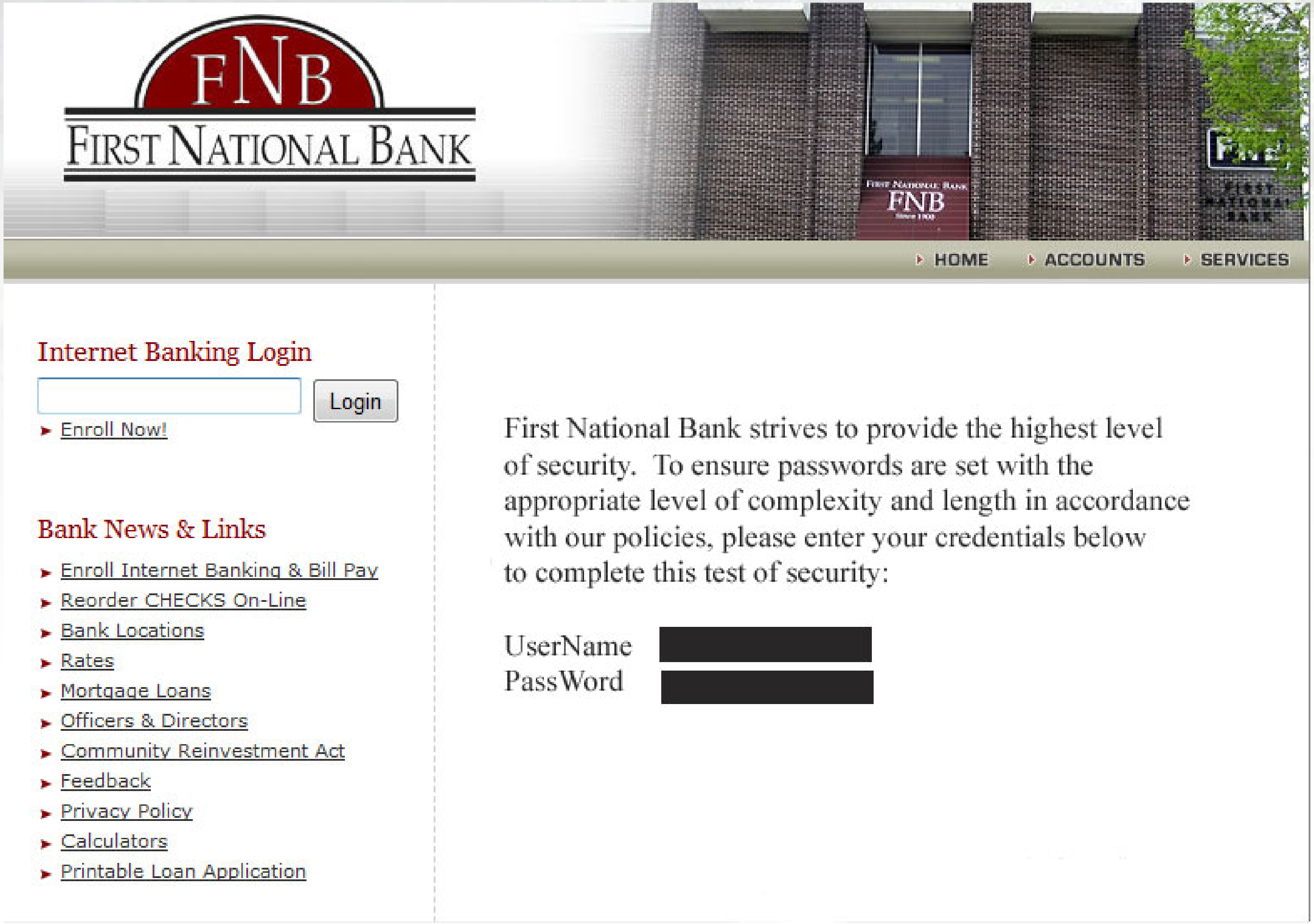
Re-Seller: USA

Product

What did I do?????

Social Engineering

- Starts with profiling the organization
  - Obtain IT Director’s name
  - Prepare strategy for exploit
  - Mockup Website
  - Originate email campaign
  - Harvest user names and passwords
  - Execute exploitation strategy
  - Experience 5% to 46% of users tested provide info



Internet Banking Login

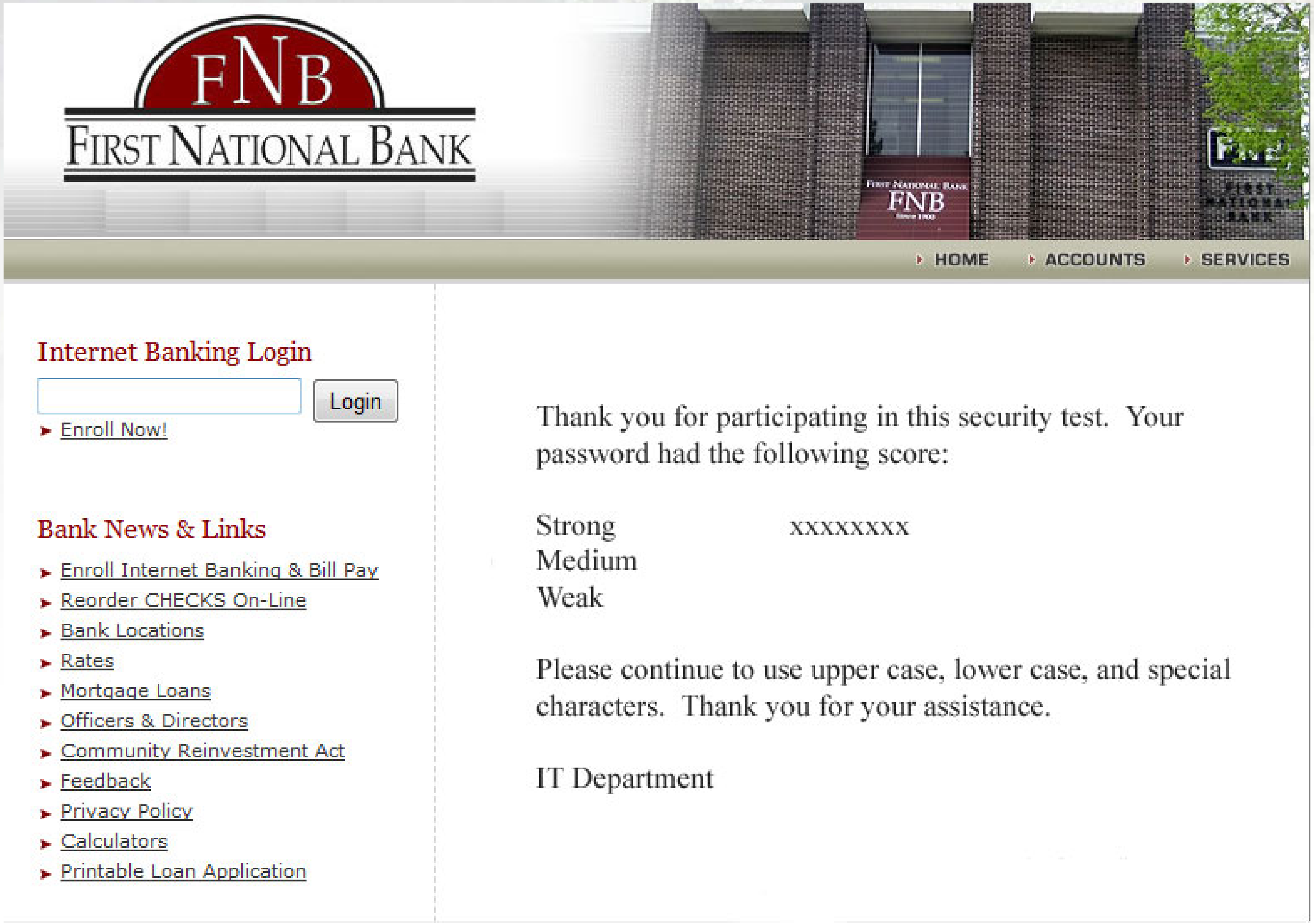
- Enroll Now!

Bank News & Links

- Enroll Internet Banking & Bill Pay
- Reorder CHECKS On-Line
- Bank Locations
- Rates
- Mortgage Loans
- Officers & Directors
- Community Reinvestment Act
- Feedback
- Privacy Policy
- Calculators
- Printable Loan Application

First National Bank strives to provide the highest level of security. To ensure passwords are set with the appropriate level of complexity and length in accordance with our policies, please enter your credentials below to complete this test of security:

UserName [redacted]
PassWord [redacted]



Thank you for participating in this security test. Your password had the following score:

Strong	xxxxxxxx
Medium	
Weak	

Please continue to use upper case, lower case, and special characters. Thank you for your assistance.

IT Department

Social Engineering

- Sometimes the simplest answer is best
  - Thought Exercise
  - Simple & Obvious

Group Exercise #1

- Break into small groups of 3 to 4 (ten minutes)
- Discuss a social engineering (phishing scam) either experienced or in the news
- Discuss 1) how you would recognize the phishing email 2) How you would respond to the email and 3) How would you detect and prevent a phishing attack in an organization you are reviewing
- Share with the whole group

Cybersecurity– Best Practices

- Training
  - Employee training
  - Management training
- Layered Security
  - Email – Proofpoint - to organization - to employee
- Education
  - Awareness of security risks – third parties
- Third party review
  - External, independent view of organization
- Self assessment
  - Review organization’s security posture

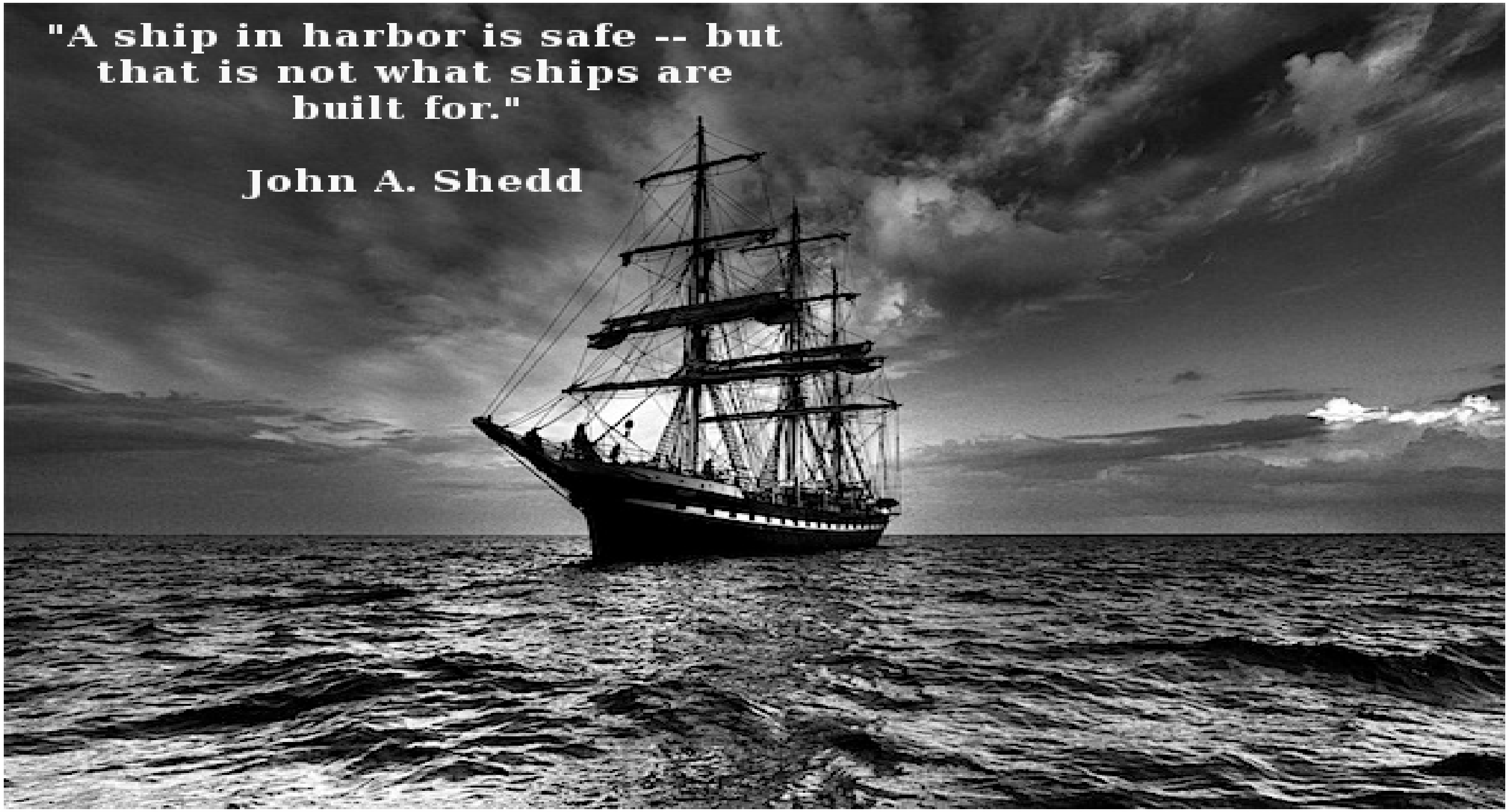
Useful Links

- Krebs On Security www.krebsonsecurity.com
  - Security Newsletter

- Bank Info Security
  - http://www.bankinfosecurity.com/

- Security Tools www.sectools.org
  - Open source security tools, be careful and use at your own risk

Balancing RISK versus Cost – Cybersecurity Top 10



"A ship in harbor is safe -- but that is not what ships are built for."

John A. Shedd

#1 – know where your data is stored

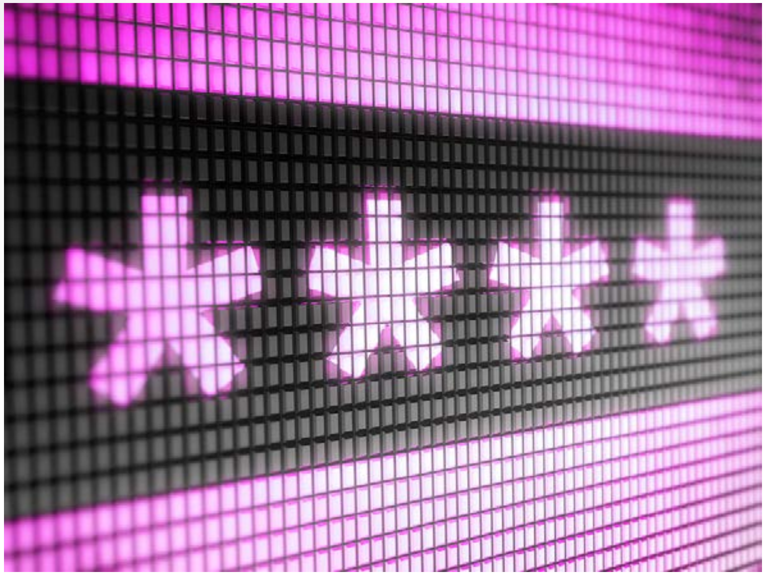
Document and maintain accurate information asset inventories, including all relevant assets that store or transmit sensitive data *(Devices & software – use software like Track-It)*

- Conduct, document & maintain current data flow analysis to understand location of your data, data interchange & interfaces, as well as applications, operating systems, databases & supporting technologies that support & impact your data *(Use white board to create flow charts to document processes, etc.)*
- Locate & consolidate all valuable data into most singular storage possible; by reducing footprint of your data you create fewer potential vulnerabilities, as well as minimize effort of monitoring & tracking access to that data

#2 – take advantage of security controls

Establish, implement and actively manage security configuration settings for all hardware and software for servers, workstations, laptops, mobile devices, firewalls, routers, etc.

- System/device hardening
- Strong password security
- Limit administrative privileges
- Grant only the minimum required access to perform job functions



#3 – know who can access your data

Align logical and physical access authorization, establishment, modification & termination procedures applicable to networks, operating systems, applications and databases

- Screen employees prior to employment
- Document additions and modifications with standard change management
- Timely removal of terminated employees
- Limit Vendor Remote Access

#4 – implement data loss prevention controls

Organizations must limit access to removable media, CD ROMs, email & file transfer websites

- Leverage group policies & existing software such as content filtering, email filters, etc.
- Companies should write clear, well-planned policy that encompasses device use & disposal of information
- When devices are no longer in use, data should be wiped & then physically destroyed

#5 – Ensure all critical Data is Encrypted

Adoption of data encryption, for data in use, in transit and at rest, provides mitigation against data compromise

- Encrypt all hard drives on all portable devices, conducted in conjunction with #1.
- Data backup, retention and archival information should all be under protection of strong encryption to ensure such data that may fall into malicious hands cannot be interpreted and/or otherwise utilized

Note – In event you lose device, compliance mandates may require to *<u>prove</u>* *the device was encrypted.*

#6 – Effective Patch management

Ensure all systems, regardless of function or impact, have recent operating systems, application patches applied and any business-critical applications are maintained at the most current feasible level for your organization

- Evaluate & test critical patches in timely manner
- Apply patches for riskiest vulnerabilities first
- Use WSUS to manage Windows related patches
- Third-Party Applications (Java, Adobe, Flash, etc.) must also be managed

Be strategic & plan for end of life events (for example, Windows XP & Server 2003)

#7 – Perform Risk Assessments

Perform an information security risk assessment that is flexible and responds to changes in your environment. Specific focus should be on all protected information & protected health information (if applicable)

- Asset based format
- Identify foreseeable threats
- Assign inherent risk rating
- Determine likelihood of occurrence
- Determine magnitude of impact
- Input mitigating controls
- Determine residual risk rating
- Update annually to adjust for new threats

#8 – Educate personnel & hold them accountable

Provide staff training on security best practices, internal policies and new threats. Focus on social engineering, phishing and physical security concerns

- Educate all personnel, at least annually, on your company's data security requirements
- Education can be as simple as email reminders, brown bag lunch & learns, etc.
- Make sure new hire onboarding process includes this topic
- Accountability includes ALL personnel– especially senior management – who must lead by example

#9 – Audit & assess controls

Conduct vulnerability scans and penetration tests to identify and evaluate security vulnerabilities in your environment

- Security controls provide most value when they are audited & monitored for compliance &/or maintenance

- Annual audits provide necessary insights into keeping security controls optimized & properly fitted to environments employed to protect

#10 – minimize impact by taking immediate action

Management's ultimate goal should be to minimize damage to the institution and its customers through containment of the incident and proper restoration of information systems

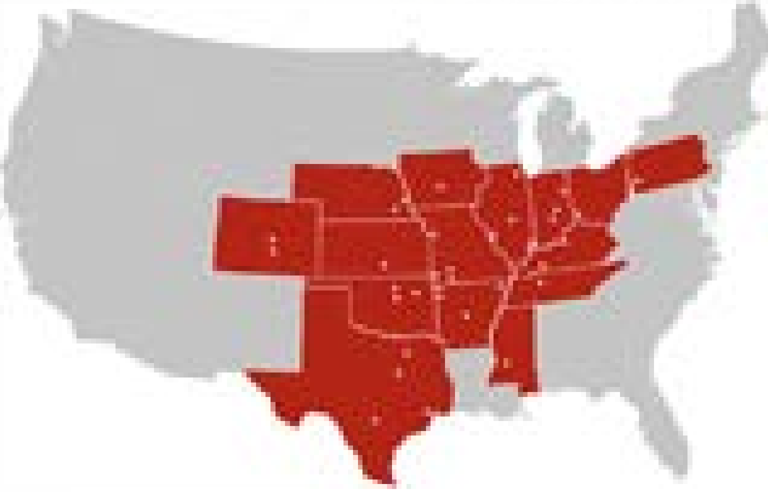
- Conduct analysis of past incidents & applicable responses to determine successful & unsuccessful areas
- Use an incident response team to ensure immediate action is taken following security event to minimize impact on operations & loss of data
- Determine who will be responsible for declaring an incident and restoring affected computer systems once the incident is resolved

Group Exercise #2

- Break into small groups of 3 to 4 (ten minutes)
- Discuss one item in Top 10 list where you think there is room for improvement in organizations that you review
- Share with the whole group

BKD Today

- $500M+ in annual revenue
- 2,400+ employees, including approximately 260+ partners
- Diverse client base spanning health care, manufacturing, distribution, financial services, construction, real estate, not-for-profit, governmental and higher education
- Network of 30+ offices serves clients in all 50 states & internationally
- Largest U.S. member of Praxity, AISBL, a global alliance of independent firms



BKD THOUGHTWARE®

Sign up at **bkd.com/subscribe**

articles // emails // presentations // videos // webinars

QUESTIONS?

THANK YOU!

FOR MORE INFORMATION

Ron Hulshizer
Managing Director – IT Risk Services
rhulshizer@bkd.com
405.842.7977