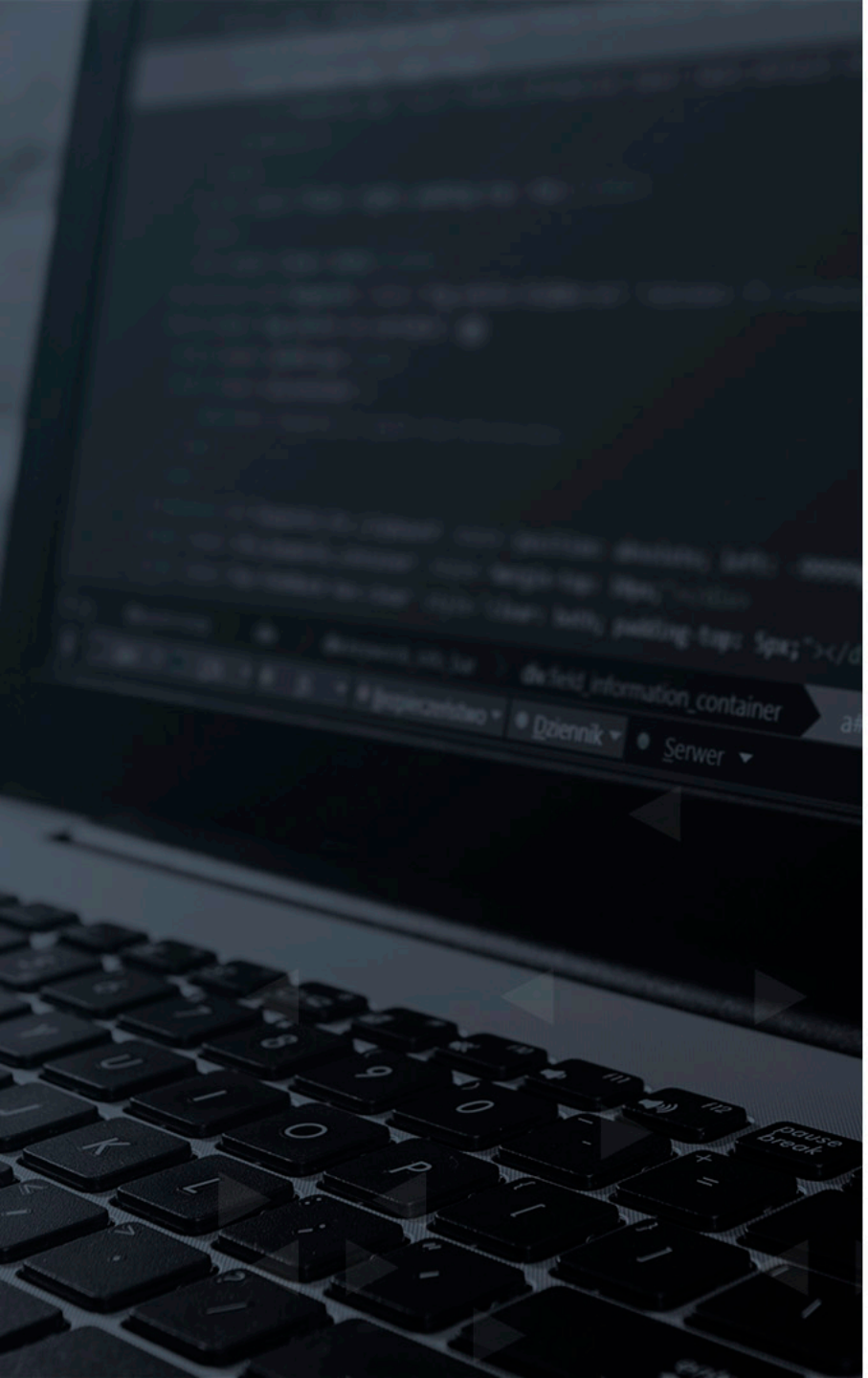
Everyone needs a trusted advisor. Who's yours?



Cybersecurity Update
Threats & Risks

Association of Credit Unions Internal Auditors

Denver, Colorado – June 20, 2019

Ron Hulshizer

Managing Director, BKD Cyber

BKD CYBER

Technology – The Dark Side

BKD CYBER

Objectives

Discuss the ever-evolving landscape of cyberthreats & risks

Identify steps individuals & credit unions can take to help minimize effects of cyberthreats through employee accountability, responsibility & governance

Talk about the top ten BKD cybersecurity areas – discuss how credit unions & credit union members can work together for the common good

Recount the trench stories of cybersecurity cases

Recognize the resources a credit union can leverage

BKD CYBER

Credit Unions in the News

According to NCUA 2018 Annual Report, there are 5,375 credit unions with assets of $1.45 trillion serving 116.2 million members

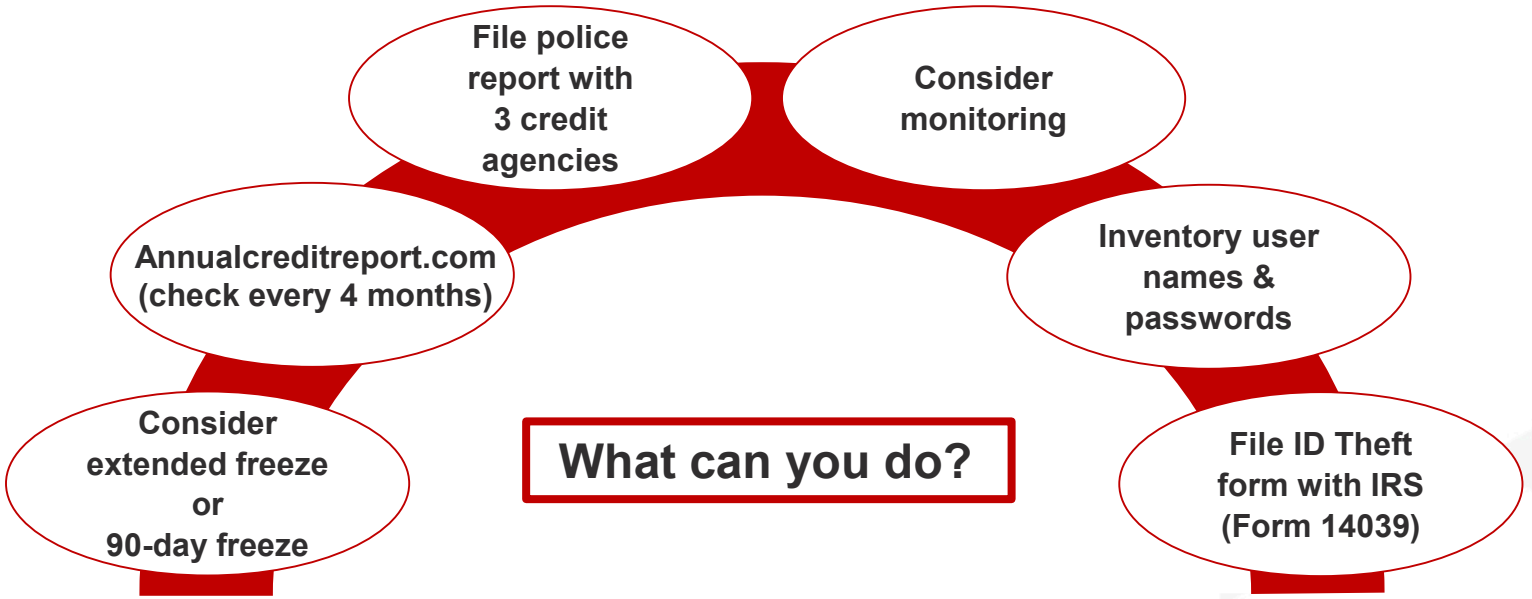
Credit Union #1
$1.6 billion assets – website was compromised with web shell that allowed hackers to intercept data & control website remotely, 60,000+ members

Credit Union #2
$300 million assets – ATM was found with skimmer, debit card fraud, unknown dollar amount

Credit Union #3
$500 million assets – Identity theft of member, bad guys perpetrated wire fraud of $100K

BKD CYBER

Personal Accountability
Identity Theft Case – Equifax Hack



Consider all these steps. Download paper at CFPB. Released Sept 18, 2018.

BKD CYBER

Responsibility – Know Threats & Risks

Threats	Risks
Wireless Cantenna	Lack of visibility
Portable Tablets	Apple vs. Microsoft vs. Google
Key Logger/Physical Information & Cell Phones	Classic Threats
“Security Testing” Devices	Unintended Uses
Drones	Unintended Uses
Employees	Weakest Link
Change	Enemy of Security

BKD CYBER

Emerging Social Engineering

CEO Scam

- Education & Awareness
- Verbal Approval

Elderly Abuse

- Education & Awareness

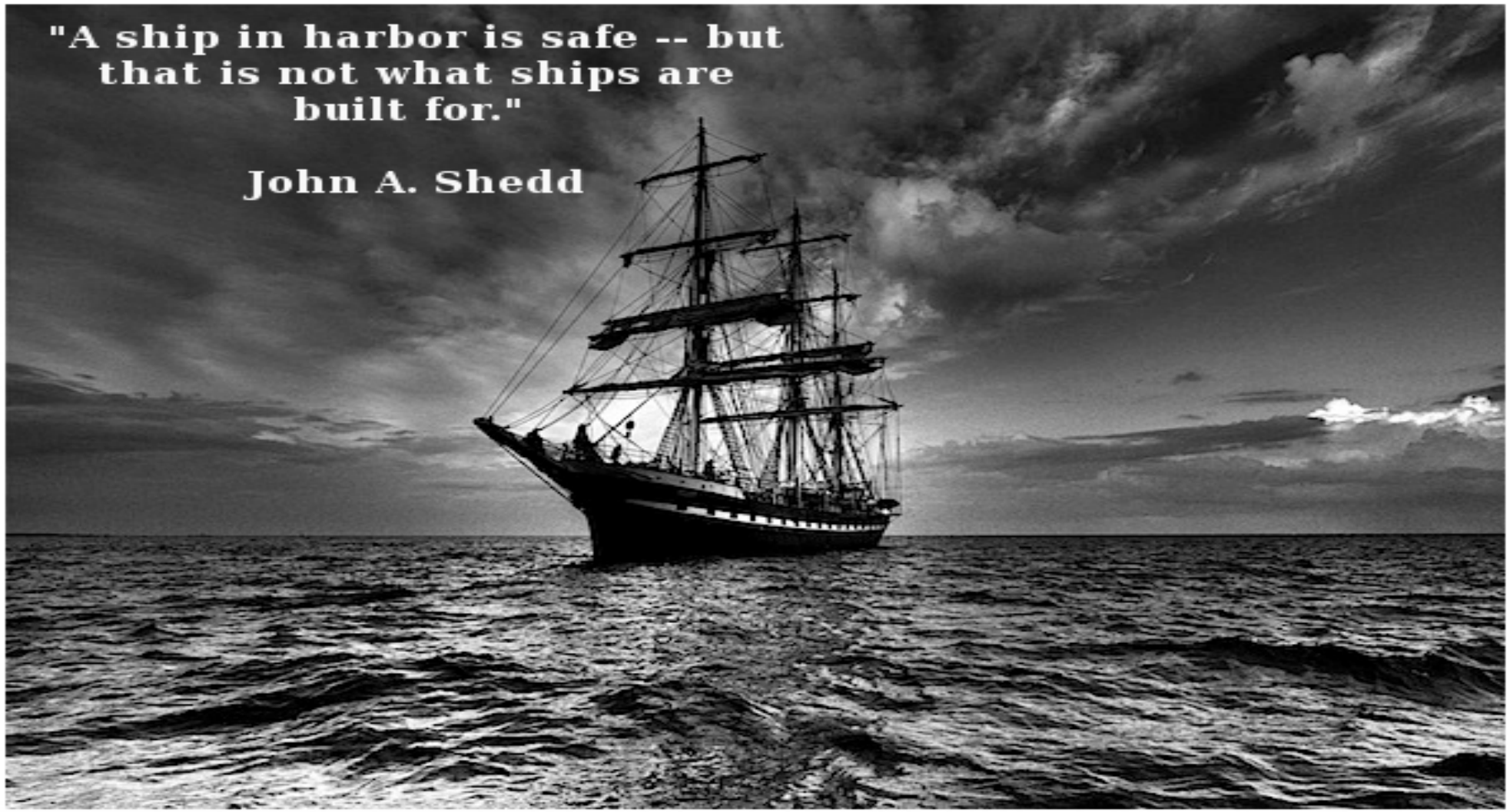
Wire Fraud

- “Know who you are dealing with”

Sometimes the simplest answer is best!
Utilize thought exercises that are simple & obvious.

BKD CYBER

Balancing RISK vs. Cost – BKD'S Cybersecurity Top 10 – Opportunity for Governance



BKDCYBER

#1 – Know Who Can Access Your Data

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

- Screen employees prior to employment
- Document additions & modifications with standard change management
- Timely removal of terminated employees
- Limit Vendor Remote Access
- **Administrator Access**
- **Segregation of Duties**

BKD CYBER

The Good Guys vs. the Bad Guys

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

Eddie Tipton

IOWA Lottery – IT Security Director

BKD CYBER

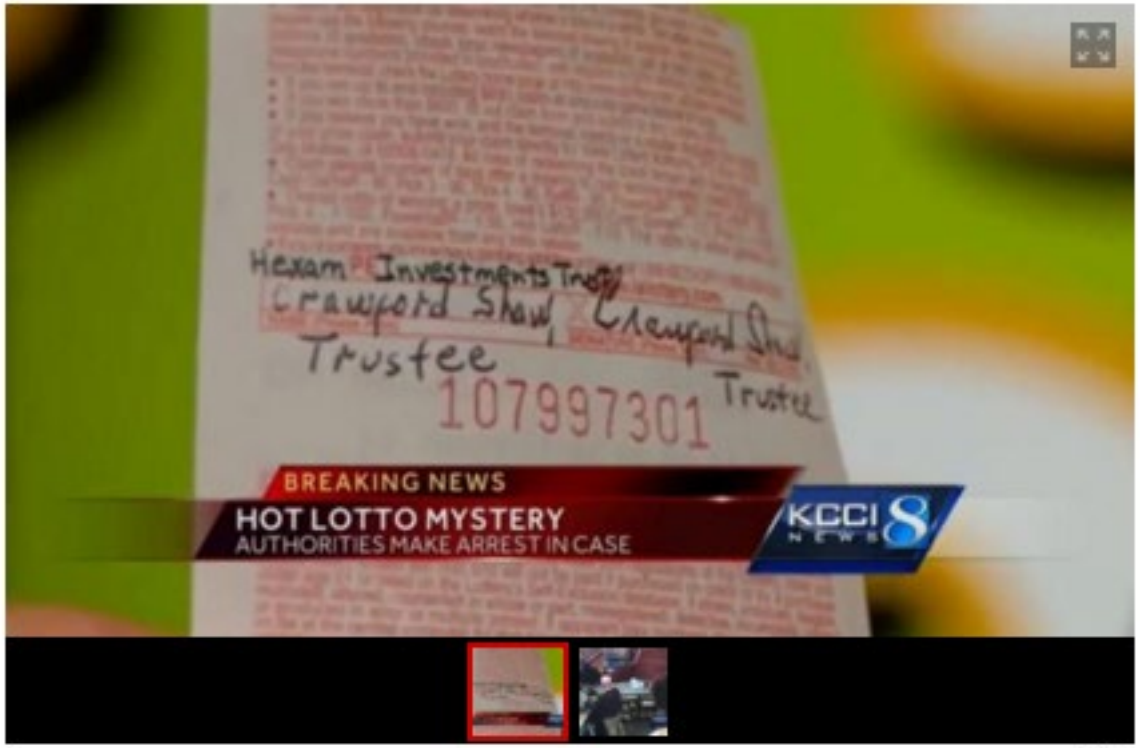
Eddie Tipton

Purchases lottery ticket at Des Moines convenience store

BKD CYBER

Lottery Ticket

Ticket sent to NY attorney Crawford Shaw



BKD CYBER

Eddie Tipton Now?

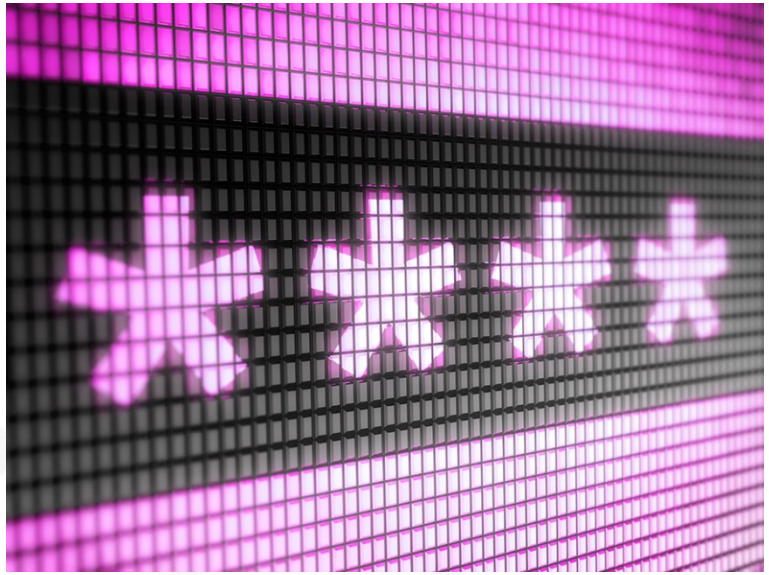
Sentenced to 25 years in prison on August 22, 2017, for rigging the system in several states so he could collect the jackpots. The largest jackpot, a $16.5 million Hot Lotto prize in Iowa in 2010, was never paid. And ultimately, it would be the one that would do Tipton in.

BKD CYBER

#2 – Take Advantage of Security Controls

Establish, implement & actively manage security configuration settings for all hardware & 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



BKD CYBER

Athena

Dedicated Password Cracker

We utilize Hashcat, power of the Nvidia video cards

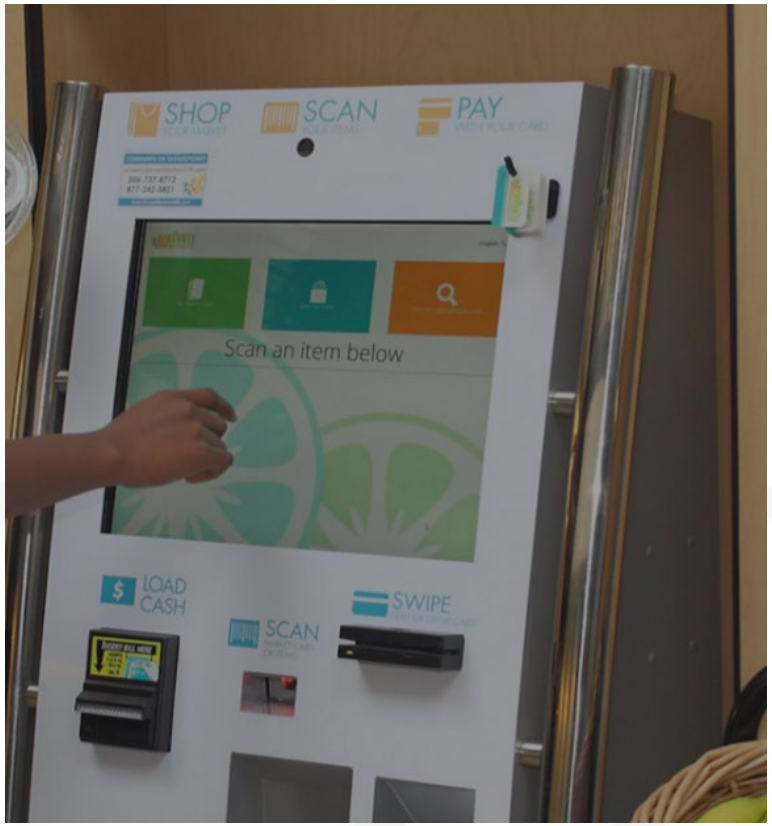
We increased speed from previous device by close to 100 times

We have cracked passwords up to 16 characters, complex

Dictionary words easiest to crack

BKD CYBER

How Good Is Multifactor Authentication?



The bad guys on July 4 hacked into the Avanti Market Kiosk system & got not only credit/debit card data, but the fingerprint Biometric data tied to the credit/debit card.

BKD CYBER

Passwords

Standard Network Password

- 8 characters, complex, 90 days
  - Summer2018$
- Galatians 5:22-23 But the fruit of the Spirit is love, joy, peace, patience, kindness, goodness, faithfulness, gentleness and self-control. Against such things there is no law.
  - G5:22sljppkgfgs

BKD CYBER

Accountability – Avoid These Common Password Pitfalls

Current month or season	A holiday	City or street where you are located
Child's name with a number (especially a birth year)	Name of a popular song/nursery rhyme/religious passage	"Password" or "I hate passwords"
Vulgarity or racial slurs	Name of Windows service	Name of common network protocols

CRACKED PASSWORDS

$central1
$$Zack$$
tommyh14!
pay$1596
Twins123%
qwert123Q!
gnik.Tk75
tyui-789
zxcv-5987

Cracking 28% of bank & CU passwords recently!

BKD CYBER

#3 – Know Where Your Data Is Stored

Document & 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 minimizing effort of monitoring & tracking access to that data

BKD CYBER

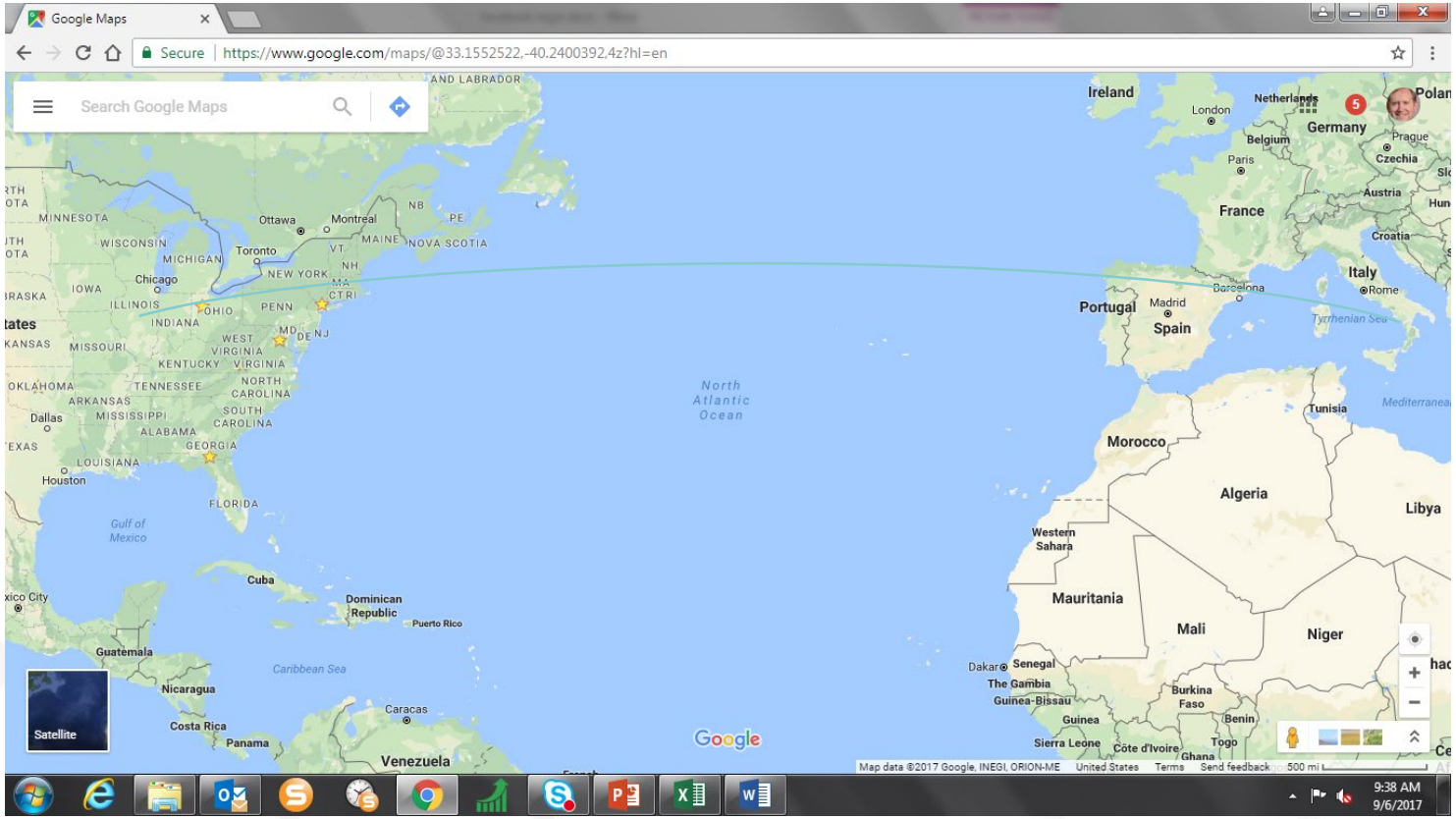
#4 – Implement Data Loss Prevention Controls

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., **Layered Security**
- 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

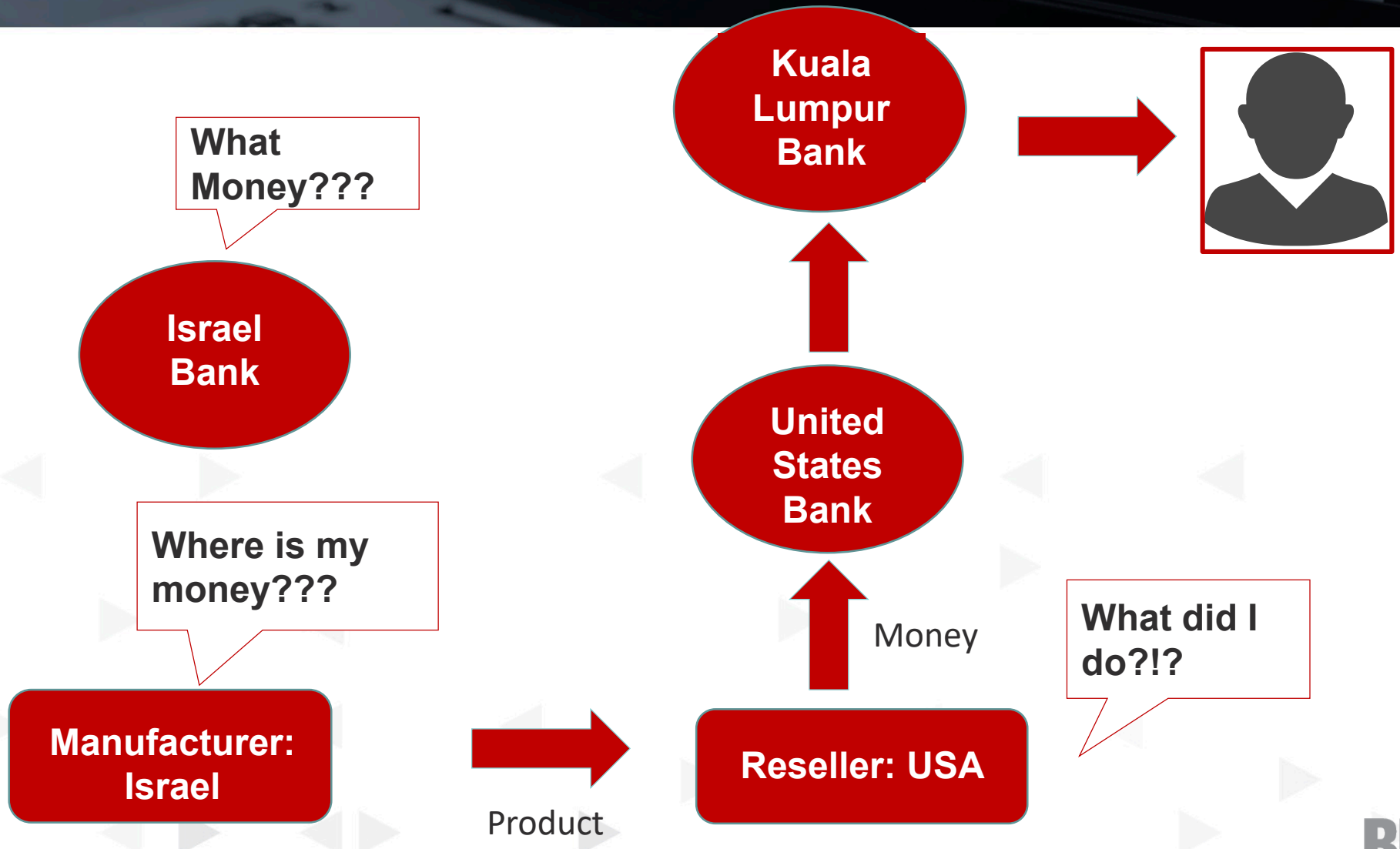
BKD CYBER

Example of Wire Fraud



BKD CYBER

Example of Wire Fraud – Part Two



BKD CYBER

#5 – Ensure All Critical Data Is Encrypted

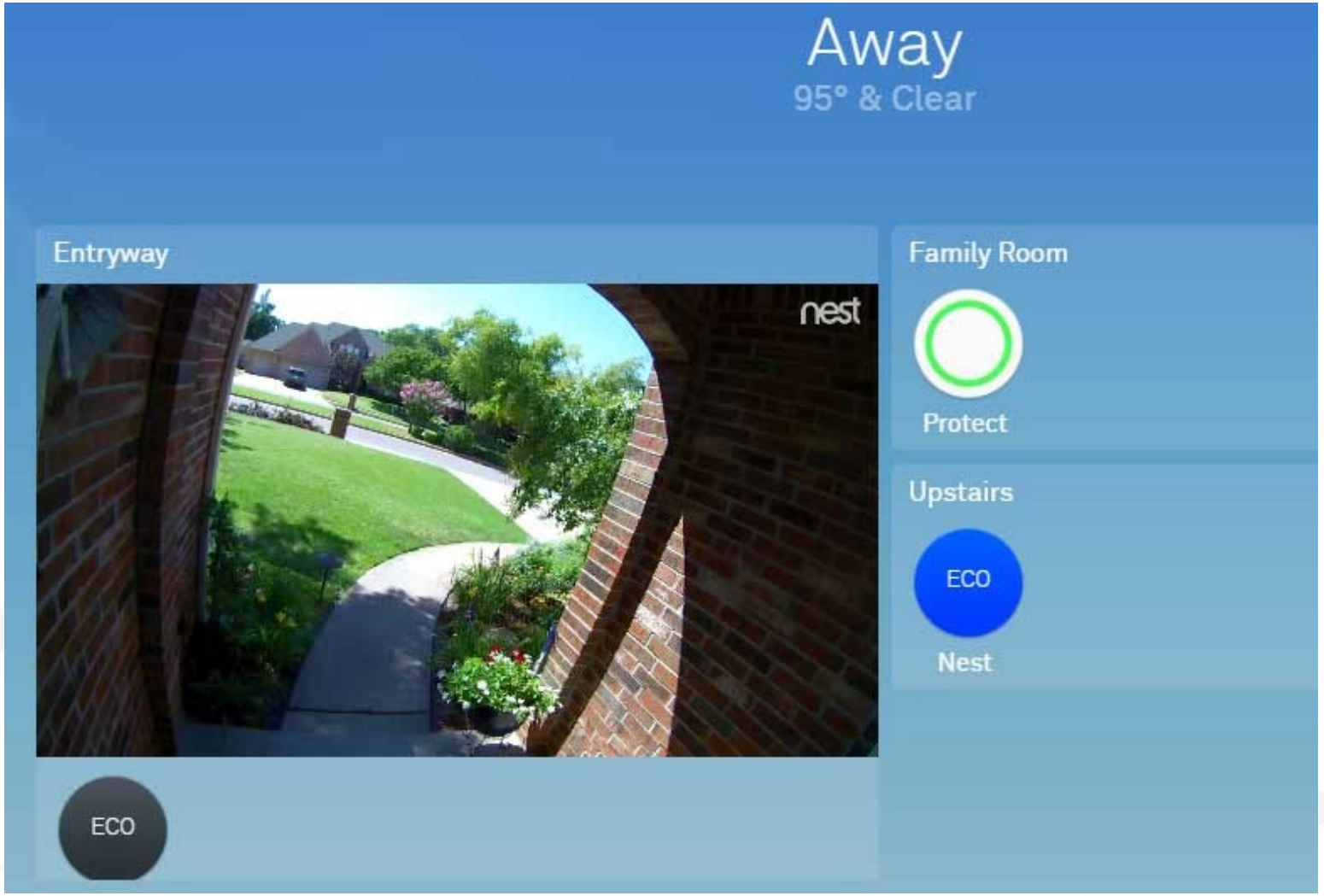
Adoption of data encryption, for data in use, in transit & at rest, provides mitigation against data compromise

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

Note – In event you lose device, compliance mandates may require you to prove the device was encrypted.

BKD CYBER

The Internet of Things



#6 – Effective Patch Management

Ensure all systems, regardless of function or impact, have recent operating systems, application patches applied & 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 7 & Server 2008 expire **January 2020**)

BKD CYBER

#7 – Perform Risk Assessments

Perform an information security risk assessment that is flexible & responds to changes in your environment. Specific focus should be on all protected information & protected GLBA 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

BKD CYBER

Malware – Ransomware

Cryptolocker/WannaCry/Petya all follow the same general strategy

Forced to reply to the extortion message with payment by bitcoin

BKD CYBER

Wana Ransomware Message

Source: Krebs on Security-May 2017

BKD CYBER

County Hospital (~200 Bed) Ransomware

Email came into hospital with Cryptolocker ransomware

- Spread to numerous employee PCs
- Hospital paid $1,000 bitcoin ransom
- Did not completely remove malware
- Two months later, hospital hit with $30,000 bitcoin ransom & paid again
- Hospital put in place after the attack
  - **Layered security – Proofpoint**
  - **Licensed KnowBe4 (knowbe4.com) – employee awareness tool, test for phishing**
  - **Removed administrator rights at user level**
  - **Removed mapped drives – went to SharePoint**

BKD CYBER

#8 – Educate Personnel & Hold Them Accountable

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

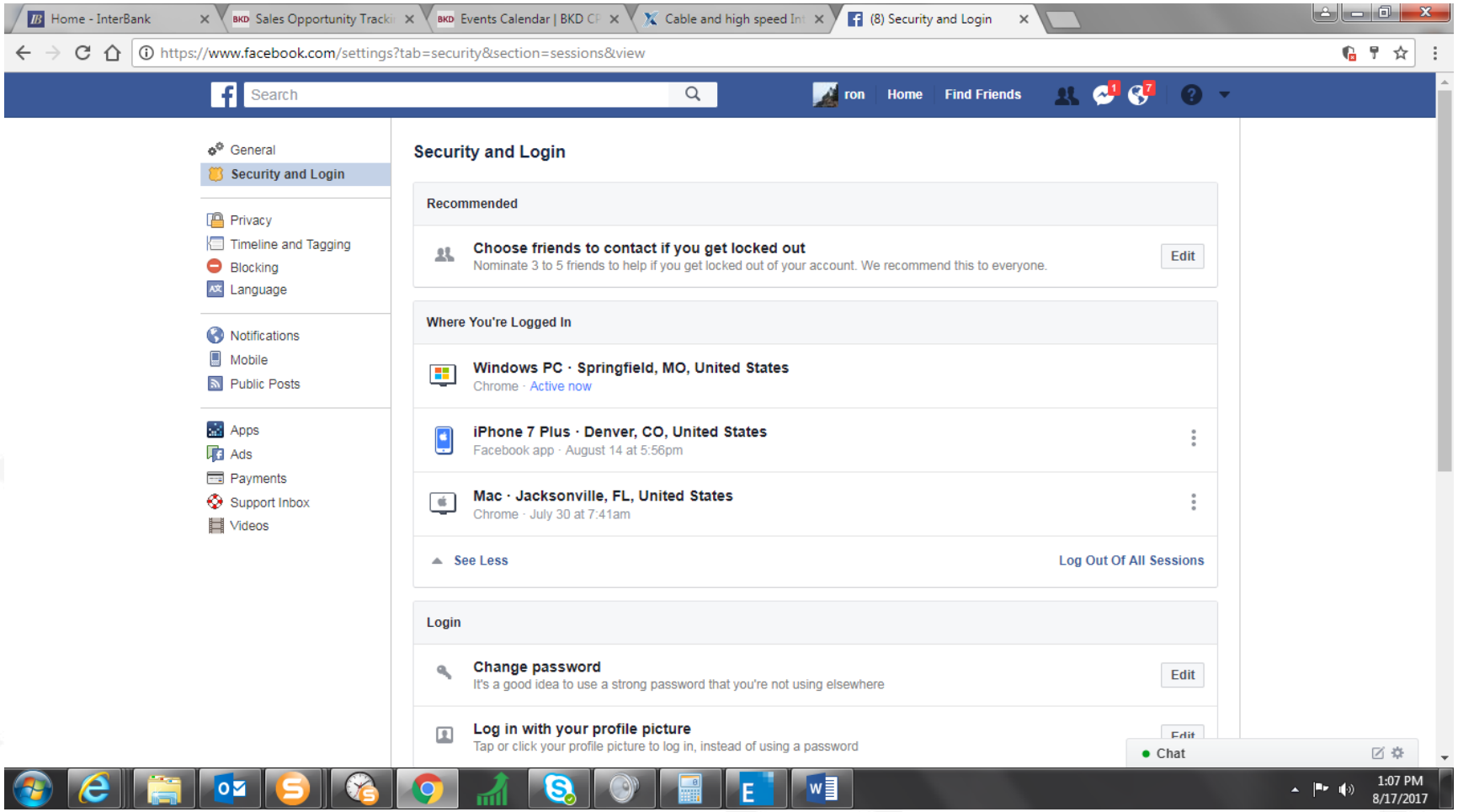
BKD CYBER

Social Engineering

Starts with profiling the organization

- Obtain IT director's name
- Prepare strategy for exploit
- Mock up website
- Originate email campaign
- Harvest user names & passwords
- Execute exploitation strategy
- Experience 5% to 46% of users tested provide info
  - Getting better in last 6 months (1–2% to 7–8%)

Security Settings



BKD CYBER

Group Exercise

- Break into small groups of 3 to 4 (10 minutes)
- Discuss one item of personal accountability & responsibility related to your digital footprint from the threats & risks discussed
- Take it back & apply a solution to your personal situation tomorrow

#9 – Audit & Assess Controls

Conduct vulnerability scans & penetration tests to identify & 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

BKD CYBER

Strengths

- Attempts to dump LSASS were prevented
- Attempts to gain access by running Psexec were prevented
- Attempts to execute executable trojans were prevented

Weakness

- Some PCs are susceptible to LLMNR and NetBios poisoning.
- Many passwords were weak and cracked with minimal effort.
- The network share \\fileserv1.[redacted] does not require authentication and can be accessed by anyone with access to the network regardless of credentials.
- The network share \\fileserv1.[redacted] contains dozens of unprotected files for various users which contain passwords stored in plaintext.

Explanation of Compromise Paths

Broadcast name resolution poisoning began once it was determined systems were likely up-to-date and conventional exploits may not an option. BKD intercepted numerous NTLMv2 hashes over the course of two days and was successful in cracking 12 passwords. Attempts were made to access systems using Psexec via Metasploit to gain shell access to systems. All attempts except one failed. Access to one system succeeded and further attempts were made to obtain in-memory passwords by dumping the system's memory using PowerShell. Those attempts failed. BKD then accessed the system using Microsoft Remote Desktop and attempted to run an executable file containing Meterpreter scripts in an attempt to gain Meterpreter access to the system. The Trojan was detected and prevented from running. Prior to logging off the system, BKD discovered a network share that did not require authentication. A search of the share found dozens of files in various subfolders containing passwords for numerous users to various systems including the Core system.

#10 – Minimize Impact by Taking Immediate Action

Management's ultimate goal should be to minimize damage to the institution & its members through containment of the incident & 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 & restoring affected computer systems once the incident is resolved

IT Governance – Best Practices

- Training
  - Employee Training
  - Management Training – Open Transparent Philosophy
- Layered Security
  - Email – Proofpoint – To Company – To Employee
- Education
  - Awareness of Security Risks – To Outside Parties
- Third-party review
  - External, Independent View of Organization
- Self assessment
  - Review Organization's Security Posture

BKD CYBER

Group Exercise

- Break into small groups of 3 to 4 (10 minutes)
- Discuss one item in Top 10 list where you think there is room for improvement in your organization or your personal digital footprint
- Take it back to your office or apply it your situation tomorrow

BKD CYBER

BKD Top Ten

#1 – Know where your data is stored	#6 – Effective patch management
#2 – Take advantage of security controls	#7 – Perform risk assessments
#3 – Know who can access your data	#8 – Educate personnel & hold them accountable
#4 – Implement data loss prevention controls	#9 – Audit & assess controls
#5 – Ensure all critical data is encrypted	#10 – Minimize impact by taking immediate action

BKDCYBER

Useful Links

- ACUIA www.acuia.com
  - Networking/conferences/webinars
- 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 & use at your own risk

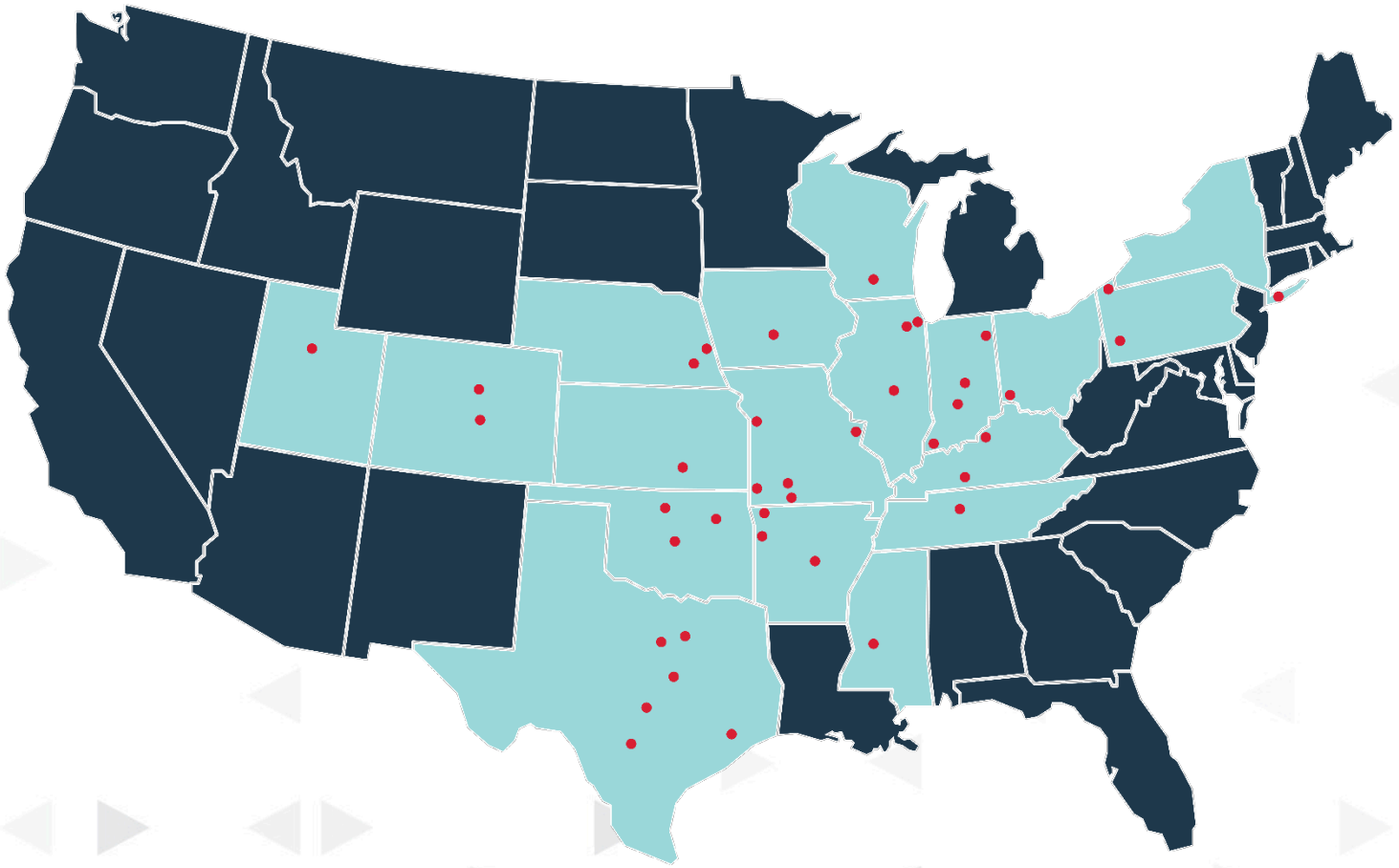
BKD Thoughtware®

- Webinars, seminars & articles
- Many are CPE-eligible
- Financial Services specific

About BKD

Total Personnel – approximately 2,700 | Partners & Principals – approximately 300

40 offices in 18 states | Serve approximately 100 credit unions



BKD CYBER

Questions?

Thank You!

Ron Hulshizer, CMA®, CGEIT®, CISA
Managing Director
BKD Cyber
405.606.2580
rhulshizer@bkd.com

BKD CYBER