EMERGING CYBER SECURITY - THREATS AND RISKS

Ron Hulshizer
Managing Director – IT Risk Services
Independent Bankers of Colorado– September 2017
Vail, Colorado
Technology – The Dark Side

Hello, this is the Dogbert Market Research Company. May I ask you some totally harmless questions?

What is your Social Security number, bank pin number and mother’s maiden name?

What exactly are you researching?

Poverty rates. I’m shooting for 100%.
Cybersecurity

• Objectives
  – Review the dark side of security
  – Discuss regulatory hot buttons
  – Top Ten List
IF I WERE A BANKER, WHAT WOULD I ASK MY FOLKS WHEN I GET BACK TO THE BANK?

• Do we have layered security on our email?
• How often are we doing training for our employees and have we considered “Knowbe4.com” or “Security Mentor” or something similar?
• How good are our backups?
• Do we have an open culture where our employees feel comfortable if the “See Something-Say Something”?
• Should our executives review their digital footprints?
IDENTITY THEFT

- Equifax Hack

  - What People can do:
    - File Police Report
    - File Police Report with Three Credit Agencies
    - Consider monitoring
    - Change bank accounts/passwords
    - File ID Theft form with IRS (Form 14039)
    - Annualcreditreport.com (check every four months)
    - Consider extended freeze or 90 day freeze
IT Security – Starts with Threats & 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
IT Security – Starts with Risk

- Employees
  - Weakest link
- Change
  - Enemy of security
Emerging 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
Lottery Ticket

• Sent to NY Attorney Crawford Shaw
Eddie Tipton
• OOPS – Sentenced to 10-25 Years

Was sentenced to 25 years in prison on **August 22, 2017** for rigging the system in several states so he could collect the jackpots.
Malware - Ransomware

- Cryptolocker/WanaCry/Petya
- Email – FedEx package is on its way
- Employee clicks on link
- CryptoLocker - Payload is downloaded
- Spreads to other computers on network
- Extortion message received - Bitcoin
How good is multifactor authentication?

The bad guys on July 4th hacked into the Avanti Market Kiosk system and got not only credit/debit card data, but the fingerprint Biometric data tied to the credit/debit card.
The Internet of Things
Example of Wire Fraud
Security Settings

[Image of Facebook Security and Login settings]

- **Recommended**
  - **Choose friends to contact if you get locked out**
  - Nominate 3 to 5 friends to help if you get locked out of your account. We recommend this to everyone.

- **Where you’re logged in**
  - **Windows PC - Springfield, MO, United States**
    - Chrome - Active now
  - **iPhone 7 Plus - Denver, CO, United States**
    - Facebook app - August 14 at 5:56pm
  - **Mac - Jacksonville, FL, United States**
    - Chrome - July 30 at 7:41 am

- **See Less**
  - Log Out Of All Sessions

- **Login**
  - **Change password**
    - It’s a good idea to use a strong password that you’re not using elsewhere
  - **Log in with your profile picture**
    - Tap or click your profile picture to log in, instead of using a password
Example of Wire Fraud – Part Two

What Money???

Israel Bank

Where is my money???

Manufacturer: Israel

Product

United States Bank

Money

Re-Seller: USA

Kuala Lumpur Bank

What did I do?????
Passwords

• Standard Network Password
  – 8 Characters, complex, 90 days
    • Summer2017$

– 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.
  • G5:22ljppkgfgs
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
    • Getting better in last six months (1-2% to 7-8%)
Social Engineering

• Sometimes the simplest answer is best
  – Thought Exercise
  – Simple & Obvious
IT Security – Best Practices

• Training
  – Employee training
  – Management training

• Layered Security
  – Email – Proofpoint - to company - to employee

• Education
  – Awareness of security risks – to customers

• Third party review
  – External, independent view of organization

• Self assessment
  – Review organization’s security posture
Regulatory Hot Buttons

• Model Validation
  – BSA/AML
  – Other Models
• InTrex Testing
  – Cybersecurity emphasis
• Board Awareness of cybersecurity threats
  – Awareness of security risks
• IT Governance
  – Risk Based Review
• 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/Cost & Ability to do Business profitably

"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 the event a device is lost, compliance mandates may require proof the device was encrypted.*
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
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
About BKD
Total Personnel, approximately 2,600 | Partners & Principals, approximately 270

Employees in Illinois/St. Louis 251
2017 Revenues $550 million

BKD National Financial Services Group
CONTINUING PROFESSIONAL EDUCATION (CPE) CREDITS

**BKD, LLP** is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: [www.learningmarket.org](http://www.learningmarket.org).

The information in BKD seminars is presented by BKD professionals for informational purposes only. Applying specific information to your situation requires careful consideration of facts & circumstances. Consult your BKD advisor before acting on any matters covered herein or in these seminars.
THANK YOU!

FOR MORE INFORMATION

Ron Hulshizer
Managing Director | IT Risk Services
rhulshizer@bkd.com
405.842.7977
BKD THOUGHTWARE®
Sign up at bkd.com/subscribe

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