Damage Control
In a Hack Crazed World

David Ashley, CISA, CISM, CBCP, CRISC, CHP
Office of the Mississippi State Auditor
Director, IT Audit Section

September 17, 2015

Bio

- 30+ years experience in IT
- 10+ years in Audit
- A believer in continuing education
  - MBA and ME – working toward MA in divinity
- In this business if you are not willing to accept and keep up with change you may be in the wrong business
- Blessed with 6 children (ages 13 to 35 with 3 boys the same age)

Learning Objectives

‣ Audience Should Become Knowledgeable About:
- History of Data Breaches
- Laws of the Land
- Shiny New Things / New Technologies
- Current Threat Landscape
- Planning for a "Hack Attack"
- IT Security Breach Disaster Recovery Best Practices
- Questions Management Should Ask

Large Data Breaches
(Last Year Presentation Slide)

▸ Target (40 million payment card numbers and another 70 million customer records

▸ Second largest breach in history was at the U.S. company eBay (145 million) users

▸ Largest breach was software maker Adobe Systems, Inc. in October, 2013, when hackers accessed about 152 million users .

Significant State Data Breaches (Occurred in 2012, but Mitigation Ongoing)

- South Carolina Dept. of Revenue
  - ¾ of state's population
  - Cost $14M so far ($12M for credit monitoring)
  - 3.8 million instate taxpayers
  - 1.3 million out of state
  - 3 million businesses
  - 72 GB data
  - 1 months (reported by secret service)
  - **Were compliant with IRS Safeguards**
  - Will now encrypt SSN

- IRS Safeguards
  - MDOR, Human Services, Employment Security

Notable Breaches in 2014 Involving Government Entities

- Government (2014)
- 10 Federal Agency Data Breaches in 2014
- U.S. Postal Service – 2014 – Names, SSN, birth dates, and other PII of about 800,000 workers and 2.9M customers. Informed in Sept. by U.S. law enforcement
- Oregon State Employment Office – 850,000 job seekers
- Oregon Secretary of State - Involved Central Business Registry and Campaign Finance Reporting System
- U.S. Dept. of State, White House (non-classified info from website), and Weather Service (affected 4 websites and disrupted satellite info delivery globally - China
- US Investigations Contractor – Exposed highly personal data on 25,000 underground investigators and other staff at Homeland Security

Government Hacks (2015)

- IRS – Pulled data off IRS website to file fraudulent tax returns – Russia – Government claims NOT a hack, went in through front door (Feb. through May 2015 – $50M in fraudulent returns – 330,000 entities involved

- OPM (White House Office of Personnel Management) June 2015 – 21.5 Million records compromised – Job assignments, performance, etc.. Includes current and prior employees and individuals who applied but were not hired. Two distinct breaches 4.2M AND 18M. Since 2007 OPM notified by IG that deficiencies in cybersecurity processes. China. Nearly Year Long – Future senior government leaders and advisors could be targeted even before taking office. Could weaken the U.S. in military confrontation. Information could be given to Chinese Allies or sold by hacker.

- Joint Chief of Staff email server (Russia suspected)

- Federal Audit Clearinghouse (Anonymous in response to trade agreement)

Unusual Hacks

- "Ashley Madison" – 37 Million - July 19, 2015 - 9.7 G of data -
  - Touted as premiere site for married adults seeking affairs, claim dumps are fake but clients admitting.
  - 15,000 Government Employee Addresses Included
  - British government officials, United Nations employees and Vatican staff

- Adult Friend (owned by Penthouse), May 2015 – 3.5M – Information Posted Publicly

- "Adult Player" Android Porn Site takes picture of user and demands ransom

- 1.2 Billion User Names and Passwords stolen from 420,000 websites in 2014 - Discovered by Hold Security in Milwaukee

Other Significant Hacks

- UCLA – 4.5 Million – Personal and Medical Info
  - July 2015 (Did not Encrypt)
- The Trump Hotel - July 2015 - (Credit Card Info) – Number Unknown
- Houston Astros- Possibly hacked by St. Louis Cardinals, June 2015
- Fred's (Headquartered in Memphis, TN) – credit card info – Number Unknown - June 2015
- SONY – China blackmail on film release

Government Spending Red Tape Endangers Cybersecurity

- Procurement rules at the General Services Administration (GSA) requires programs to be on the market for 2 years to be eligible for purchase
- Products for IT can be obsolete in 6 months
- Many companies opt out of selling to the government
- At roughly the same time as President Obama was calling on agencies to shore up security after OPM breach Navy was signing $9M contract with Microsoft for support to Windows XP (14 year old OS).
- What does this say for computerized weapons systems?

Penalties for Non-Compliance

- Damage to or loss of data
- Damage to reputation
- Loss of customers
- Loss of debit/credit card acceptance privileges
- Breach notification costs
- Litigation costs
- Fines and incarceration
- Some HIPAA violations considered felony

Examples of Consequences From Breaches Other Than Fines

- HIPAA allows fines as well as civil action by state attorney generals
- Civil action prominent with identity theft and credit card victims (At least 4 class action suits against Ashley Madison – one $578M in Canada – Also in 3 states)
- Credit monitoring standard consequence
- Example: (Headlines)
  - Heartland Payment Systems Enters into its Third Settlement Agreement Arising From 2008 Data Breach

Laws of the Land

- *HIPAA Privacy and Security Rules (as amended by HITECH Act)*
- *Security Breach Notification Laws (46 States, DC, PR, and Virgin Islands)*
- *Payment Card Industry – Data Security Standard*
- Federal Trade Commission – Red Flags Rule
- Federal Trade Commission – Disposal Rule
- Federal Information Security Management Act of 2002
- Multiple Federal Privacy Bills Introduced Each Year
- Whitehouse Consumer Privacy Bill of Rights (February 2012)

Data Security Issues and Data Breach Notification

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Part 2 – Confidentiality of Alcohol and Drug Abuse Patient Record Regulation
- Sarbanes Oxley
- State Laws and Regulations
- Section 5 of FTC Act for companies who store consumer information on the cloud

International Laws

- European Union (EU) Directive on Data Protection of 1995
    - Some information of residents of EU cannot be stored outside the EU
- Australia's Privacy Laws
- Canada's Privacy Laws

Compelled Disclosure
to the Government

- Electronic Communications Privacy Act (ECPA)
- Stored Communications Act (SCA)
- USA Patriot Act (including National Security Letters; FISA warrants)
- Warrants and Subpoenas Generally - eDiscover y

Compelled Disclosure to the Government – ECPA (Including SCA)

▸ Protects electronic communications while in transit and while held in storage

▸ No One Thinking of Cloud Computing When Enacted (1986)

▸ Problems arise on how to characterize activity involved in cloud computing

▸ Gives different levels of protection to electronic data based on "electronic storage" or "remote computing"

▸ **For example**, information older than 180 days that is stored on a "remote computing service" is subject to government search with just an administrative subpoena

Data Security Issues – Federal Laws, Regulations and Standards

- Federal Laws and Regulations:
  - Healthcare (HIPAA and HITECH)
  - Educational institutions (FERPA)
  - Financial institutions (GLBA)
  - Publicly traded companies (SOX)
- Entities cannot generally contract away its obligations to comply with these
- Some regulations, however, require an entity to pass obligations to cloud providers by contract (e.g., HIPAA)

State Data Breach Laws

- 47 States, DC, Puerto Rico, Guam, and Virgin Islands
- States that don't have include New Mexico, South Dakota, and Alabama
- Mississippi (75-24-29) enacted July 1, 2011
- Name or first initial and last name in combination with any one or more of the following data elements: Social security number; Driver's license number or state identification card number; or an account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial accounts (Several cross foot websites)

Trend Toward Harsher Data Breach Laws

▸ Massachusetts, Florida and California beefed up state laws.

▸ Massachusetts (Covered if have data of resident of state

▸ Florida (expands definition of PII and data breach (access), shorter deadline for providing notice (30 days) and creates unique document disclosure requirements (to state))

▸ California (extended definition of PII to user name of email in combination with info to permit access and require identity theft protection from companies that maintain data in addition to those that own data, i.e. cloud)

▸ Very likely that federal law will be enacted very soon (concern for privacy as organization will be forced to share data with federal government under some proposals)

New Technology, New Risks

- Flash Drives, Memory Cards, and other Removable Media
- I-Pods, MP3 players, Digital Cameras
- Smart Devices: Cell phones, PDAs, Tablets
- Instant Messaging, Text Messaging, Media Messaging
- Remote Access: (BYOD) employees, vendors, clients
- Wireless Networks: work and home
- Voice over Internet Protocol (VoIP), Unified Messaging
- Storage Area Networks, Electronic Data Vaulting
- PC Virtualization, Server Virtualization
- Software as a Service (SaaS), Cloud Computing
- Infrastructure as a Service (IAS)
- Advanced Persistent Threats (APTs)

Upcoming Audit Expectations
(MS State IT Auditors Look at the Following)

- Items To Look for in IT Audits
  - Policies and Procedures (IT and HIPAA)
  - Security Plan
  - Risk Assessment
  - Disaster Recovery Plan
  - Penetration Test / Vulnerability Scan
  - Password Management
  - Backups
  - Encryption (In Transit and At Rest)
  - SSAE16 (Old SAS70)
 - Access (Physical, Logical, and Reviews)

Policies and Procedures

- Policies we like to see:
  - Acceptable Use, Backup and Recovery, Business Continuity/Disaster Recovery, Hardware, Software Inventory, Computer Center, Operations, Encryption, Segregation of Duties, VPN, Virus Protection, Data Breach, Change Management/Patch, Network Monitoring, Logging, Risk Assessment, Password, Data Retention
- P&P Must Be Specific to Agency and they must adhere to policies
- If you have specific requirements such as HIPAA you should have a separate set of P&P

CRIMINALS AT THE GATE
(How Breaches Happen)
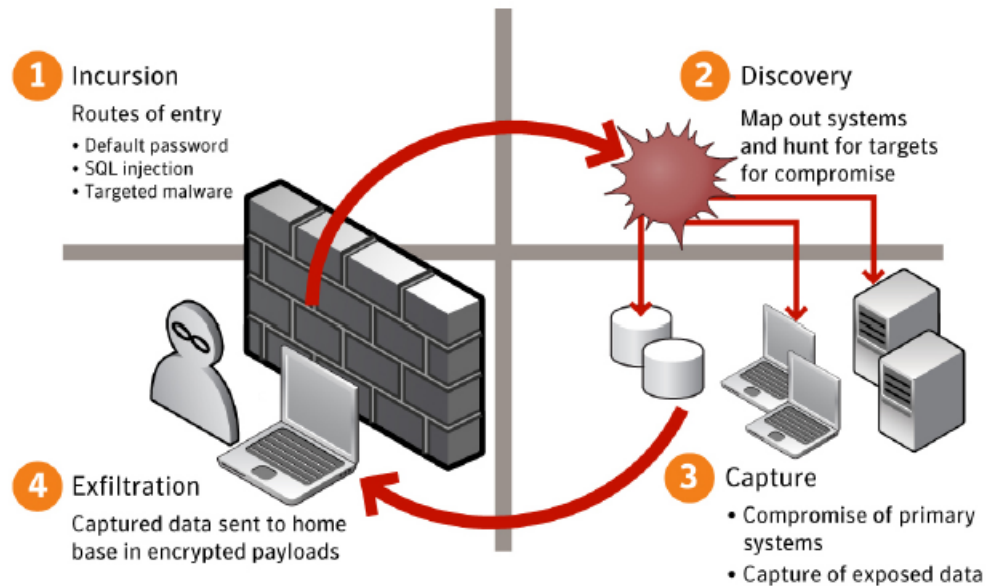
Four phases of targeted attacks: incursion, discovery, capture, exfiltration

BUSINESS ACCOUNT TAKEOVER

▸ **Best Practices**
  - Up-to-date anti-virus software
  - Properly configured firewall
  - Intrusion detection and prevention software
  - Educate employees about risks of unknown emails, web sites, and storage devices
  - Utilize dual control for ACH and wire transactions
    - Restrict functions for PC used for ACH and wire initiation (Strict physical security)
    - No removable media, no email, no other internet use
  - Perform daily reconciliation of bank account(s)
  - Provide prompt notification to bank about suspicious activity

▸ **BUSINESS ACCOUNT TAKEOVER**

- Best practices (continued):
- Make sure you are following the terms and conditions in the ACH /treasury management agreements that stipulate your responsibilities
- Utilize multifactor authentication using something you know and something you have
- Utilize out-of-band alerts and out-of-band authentication
  - Utilize optional services if available ACH debit block (pay no ACH debits)
  - ACH debit filter (pay only pre-authorized ACH debits)
  - ACH transaction review (review and pay authorized debits)

HOLES IN THE ARMOR
(Common Privacy and Security Issues)

- Informal user access provisioning
- Exceptions to role based security
- Minimum necessary access not used
- Segregation of duties not analyzed across systems
- **Removal of access not timely**, especially on hosted/cloud apps
- **Periodic access reviews not performed**
- Vendor access and activity not monitored and controlled
- No controls over ad-hoc reporting (direct access to data)
- Security as an afterthought on new systems
- Security not tested after upgrades
- Default vendor passwords not changed
- Weak and trivial passwords, complexity not required
- Not using passphrases, biometrics, hardware and multifactor authentication when prudent

HOLES IN THE ARMOR
(Common Privacy and Security Issues)

- Thinking that network security will protect applications
- Thinking application controls restrict access to data
- Allowing access to social media networks at work
- Not training employees on the risks of social networks
- Allowing unsecure instant messaging
- Poorly secured wireless access points and client portals
- Portable devices – laptops and PDAs -- not physically secured
- Portable devices and backup media not encrypted or otherwise secured
- USB ports and CD/DVD drives not controlled
- Transmissions not encrypted
- Fax and email destinations not validated prior to first use
- Outbound data not monitored (data leak detection)
- Not verifying security at cloud and other 3rd-party providers

Current Threat Landscape

- Threat Agents are more sophisticated
- Attack Patterns now being applied to mobile devices
- Cyberwarfare – Multiple nation states have capabilities to infiltrate government and private targets
- Cloud computing results in large concentrations of data
- Social networks now a primary channel for communication and knowledge collection
- Big data allows for big data breaches

Advanced Persistent Threats

- Defining Characteristics
  - A targeted threat
  - Composed of various complex attack vectors
  - Can remain undetected for an extended period of time.

- Well-researched, Sophisticated, Stealthy, Persistent

Other Trends

▸ Seeing Considerable Activity on "Investigative" Penetrations on Infrastructure (Electricity Grids, water, etc.) and Manufacturing (Pipelines, Chemical Plants, etc.)

Related Facts

- Mississippi has 1400 rural water associations
    - (Only Texas and California have more)
- Mississippi has more than 500 bridges
- Some transformers like those at substations have a several month manufacturing lead time
- Many states have websites that have detailed information of bridges, pipelines, etc.

Personal Experience
Pipeline Explosion in My Back Yard

Personal Experience

Hurricanes Personally Witnessed

- Camille (1969)
- 200+ mph winds and 24 foot storm surge

- Andrew (1992)
- <u>hurricane damaged or destroyed</u> 9,500 traffic signs and signals, 3,300 miles of powerlines, 3,000 watermains, 59 health facilities, 31 public schools, 32,900 acres of farmland and 82,000 businesses.

- Katrina (2005)
- 1833 dead

Planning and Recovering From a Data Breach

- Disaster Recovery Planning Becoming Even More Important
- Near certain that attack or data breach will occur
- According to Mandiant's 2014 Threat Report it takes an average of 243 days to discover a breach
- Should make data breach plan
- A data breach plan lays out the key steps and key personnel to involve when a data breach occurs
- Data breach plan needs to incorporate
  - Forensics and Evidence Collection
  - Identifying Regulatory Mandates Impacted
  - Managing Notification of Breach

Business Continuity
And Disaster Revocery

- Hacking is a very real, very present risk to consider
- In today's world, probably more realistic to accept that your organization **will experience** a breach, **not if**
- According to Ponemon Institute, the 2014 Cost of Data Breach Study sponsored by IBM estimates the average cost of a data breach at $3.5 million
- As with any other disaster, it is important to have a DR plan in place in the case that such an event may occur
- The level, development and testing of your response plan prior to the breach can make all the difference in how sever it impact will be

Cybersecurity Insurance

- Cybersecurity insurance may help to offset costs and liabilities from data breach incidents as well as provide contracting services that address forensics, data breach notifications, and credit monitoring

- Insurance provider may help promote the adoption of preventative cybersecurity measures that reduce the risk of cyberattacks

- Gartner advocates that IT organizations shift their mentality to a continuous response where systems are assumed to already be compromised

Should Gain Visibility of Full Attack Continuum

- Before: Defenders need comprehensive awareness and visibility of what's on extended network to implement P&P as well as controls to defend it.

- During: The ability to continuously detect an attack and block it is critical

- After: Defenders need to identify point of entry, determine scope, contain the threat, eliminate the threat of re-infection, and remediate disruption.a

Development of Today's Attack Continum

- PC virus appeared more than 25 years ago
- For nearly 10 years, viruses endured as primary method of attack.
- Approximately every 5 years attackers would launch new types of threats
- Today we are faced with advanced malware, targeted attacks and advanced persistent threats (APTs)
- Difference in this era from the past are motivatins and the tools behind the attacks, making them particularly challenging to detect, understand and stop.

Develop a Comprehensive Plan

- Identify your risks and reassess at least annually
- Test plan yearly
- Recognize that:
  - Most security tools today focus on providing visibility into network and blocking malware at the point of entry.
  - Advanced attacks now employ tactics such as port hopping, encapsulation, zero-day attacks, sleep techniques, encrypted traffic, and sandbox evasion.
  - If file is not caught or it evolves and becomes malicious after entering environment, point-in-time detection technologies cease to be useful.

Planning a Hack Attack

‣ Hacking Recovery Plan should be part of any Comprehensive DR Plan. Some steps to be included are:
  ▪ Disconnect external lines
  ▪ Perform a wireless sweep.
  ▪ Scan for compromised machines
  ▪ Disable or delete rogue users
  ▪ Change passwords
  ▪ Preserve the data
  ▪ Identify and address the vulnerability (After machine is hacked it is almost impossible to completely clean it)
  ▪ Rebuild the machine (Do NOT restore registry, OS files, or programs from files)
  ▪ Bring network back up
  ▪ Perform forensic analysis
  ▪ Notify law enforcement

DR and BIA (Business Impact Analysis)

- Depending on the complexity of the organization, there could be one or more plans to address the various aspects of BCP and DRP
- First step of BCP is to identify business processes of strategic importance and determine time frames, priorities, resources and interdependencies needed for key processes (Management must be involved)
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
- BIA should identify resources that support key processes, list of vulnerabilities, probability of occurrence of threat (risk assessment), efficiency and effectiveness of risk mitigation controls

- Frequent Risk Assessments Are Important
- Management Must Own DR
- Upper Management Must Ask Key Questions

Upper Management Key Questions

- What was most significant recent cybersecurity incident?
- What was the most significant near miss. How was it discovered?
- How is the performance of the security team evaluated?
- Do you have relationships with law enforcement?
- Do you work with business partners and leaders on due diligence?
- What process is in place to ensure proper escalation of issues?

Things to Do

‣ Read and Understand the Applicable Laws and Regulations

‣ Revise Policies and Procedures to reflect regulations and guidelines

‣ Devise a tool for documentation of risk assessment

‣ Schedule Penetration Test / Vulnerability Scan if needed

‣ Produce Security Plan

‣ Disaster Recovery Plan (Development, Test, and Revise)

‣ Revise Business Associate Agreements and Secure New Agreements (HIPAA)

‣ Revise Training and Train appropriate staff

Thank You

David Ashley,
Office of the
Mississippi State Auditor
P.O. Box 956
Jackson, MS 39205
Ph: 601-576-2800
800-321-1275 (statewide)
david.ashley@osa.ms.gov
Web: www.osa.ms.gov