BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Cyber Threats; And What To Do About Them

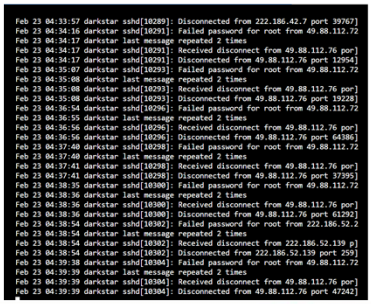
Robert L. Kardell
Ret. FBI, JD, MBA, CPA, CISSP, CFE, CFF, GSEC, A+, Net+,
BKardell@BairdHolm.com

Cyber Security not just for IT!

- IT
- HR
  - Hiring, onboarding, training,
- Management
  - Continuous review and improvement
- Board Issue
  - Liability for no addressing

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Everyone is a target!



BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Part I – Definitions and Threats

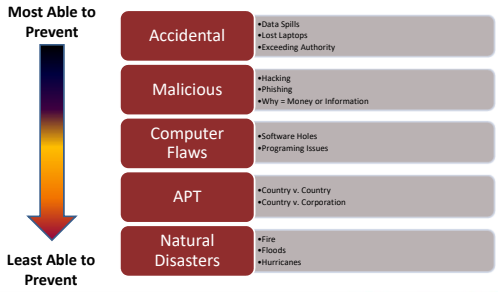
BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Cyber Definitions

- Threat or Vulnerability
- Event
- Incident
- Breach
- Criminality

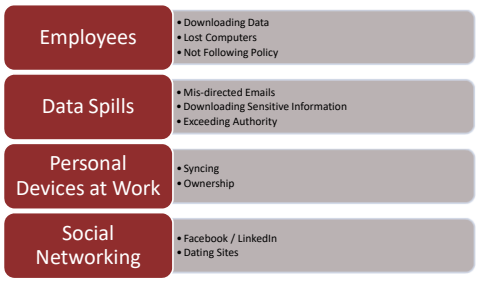
BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Types of Cyber Threats



BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Accidental Cyber Threats Outline



Accidental Threats from Employees

- Downloading
  - Programs
  - Data
- Lost Computers
  - Computers
  - USB Drives
  - Key Fobs / Access Cards
- Policy
  - Circumvention Policy
  - Not Following Policy / Not Aware of Policy
- Passwords

Data Spills

- Definition - the transfer of classified or sensitive information to unaccredited or unauthorized systems, individuals, applications or media. A **spillage** can be from a higher level classification to a lower one
  - Government – UCLAS, CONFIDENTIAL, SECRET, TOP SECRET
  - Private Entities – PUBLIC, SENSITIVE, PRIVATE, CONFIDENTIAL / PROPRIETARY

Personal Devices at Work

- Syncing
- Data Ownership
- Device or Application Management
- Security for device

Employee Threats Prevention Techniques

- **Cyber Security Policies**
- **Create a culture of cyber awareness / security**
- **Talk frequently about cyber security**
- **Make employees part of solution**
  - **Teams of planners - BCDR**
- **Strong password management**
- **Reporting cyber security incidents**
  - **Integrate IT into workforce**
- **Review HR handbook**
- **Make the communication reoccurring!**
- **Don't wait**

Malicious Cyber Threats Outline

Insider Threats	• Disgruntled Workers • Former Employees
Social Techniques	• Changing Trends • Technology Centered
Business Email Compromises	• Type of Man-in-the-Middle • CEO / Vendor / Customer / Attorney
Computer Takeover Schemes	• Ransomware • Malware
Tech Support Scams	• Remote computer access • Study by Microsoft
Identity Theft	• Credit Cards • ATMs

Insider Threats

- Disgruntled Employees
- Ex-employees
- Employees with elevated access
- Remedy
  - Good off-boarding / termination policies

Social Engineering Techniques

Changing Technique

- Con-men with personal interactions
  - Same Goals = Gain Trust & Get Money
- Technology Centered Schemes
  - Computers
  - Email
  - Texting
  - Social Media
- One hacker = many victims
  - Worldwide reach

Infamous Hacker

"The lethal combination is when you exploit both people and technology… it's easier to manipulate people rather than technology.".

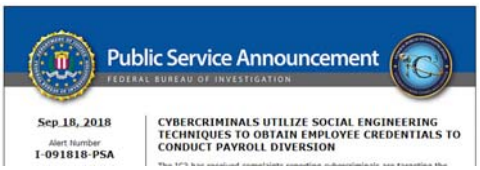
Social Engineering Prevention Techniques

Be Wary Of:

1. Unsolicited business schemes
2. Texts / E-mail / US Mail
3. Any "IMMEDIATE" Requests
4. Uninvited Money Managers
5. And Anything!

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Internet Crime Complaint Center (IC³)



www.ic3.gov

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Business E-mail Compromises

- BEC Definition and Methodology
- Versions of BEC
- Hallmarks of BEC
- Victims and Impact of BEC

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Business E-mail Compromise (BEC)

Definition:

Sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.

How:

Carried out by compromising legitimate business e-mail accounts through social engineering, brute-force, computer intrusions, etc.

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

BEC Methodology
Spoofed

- **Spoofed accounts**
  - Adding an additional letter to the user name
    - abcd@yahoo.com => abcdd@yahoo.com
  - Need to be aware of free domains, i.e., Yahoo, G-Mail, AOL, Hotmail
- **Spoofed Domain**
  - Slight variations of the domain abc@0123.com => abc@O123.com

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

BEC Methodology
Non-Spoofed

- **"Phishing Perfected"**
- **Hacked accounts**
  - Spear phishing
  - E-mail account login spoof
  - **Things to look for:**
    - E-mails forwarded to trash folder or spam folder
    - E-mails forwarded to actor accounts
    - Edited "rules" for account

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

BEC - Hallmarks

- Targets
  - Open source e-mail accounts
  - Accountants, bookkeepers, controllers, etc.
  - CPA firms, law firms

BEC - Hallmarks

- Social engineering, research and information gathering to minimize suspicion
  - Specific to the business being targeted
  - Amount requested
  - Company logos, letterhead, signatures, etc.
  - Coding and phrases (i.e. "Code to admin expenses")

Business Email Compromises

- Coincide with:
  - executive travel
  - close of business day or week
- IP addresses trace back to free domain registrars
- Phishing schemes
- Pressure to act quickly and secretly

Business Impact

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

BEC Prevention Techniques

- Multi-Factor Authentication
- Have Written Pre-approved Instructions
  - Back-up Approval Authority
  - No Wire Transfers Over Weekends / Holidays
  - No Wire Transfers Without Original Signature
- Communicate with Bank on Instructions
- Minimize Bank Information in E-mail

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Computer Takeover - Prevention Techniques

- Maintain Daily Backups
- Keep Backups Offsite / Offline
- Keep Virus Definition Up To Date
- Keep your programs up to date
- Educate Employees
- Review Procedures Yearly

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Part II - Financial Risks
The True Cost of Cyber Security

When a Threat Becomes a Breach

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Definitions of "records" under data breach statutes

PII Definitions	Nebraska Neb. Rev. Stat. § 87-301	Iowa Chapter 715C	South Dakota Chapter 22-40
Individual's first name or first initial and last name in combination with			
SSN	Yes	Yes	Yes
Drivers License	Yes	Yes	Yes
Electronic ID or routing code	Yes		
Financial Account w/ password	Yes	Yes	Yes
Unique electronic ID w/ password		Yes	
Biometric Data	Yes	Yes	
State ID	Yes		
Account Number	Yes		
Credit / Debit Card Number	Yes		
Username or Email w/ password	Yes		
Health Information			Yes
Employee ID with password/ code			Yes

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Investigative Costs of Data Breach

- Notification Expenses
- Crisis Management
- Regulatory Investigation Expense
- Data Breach Liability
- Content Liability
- Data Loss & System Damage (or Data Restoration Coverage)
- Business Interruption / Lost Revenue

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Additional Costs of Cyber Breach

- **Direct Financial Costs**
  - Lost profits
  - Software
  - Hardware and systems
  - Information
- **Intangibles**
  - Reputation
  - Personnel
- **Indirect Third-party Liability**
  - Lawsuits, remediation, on-going monitoring
  - Fines and criminal liability

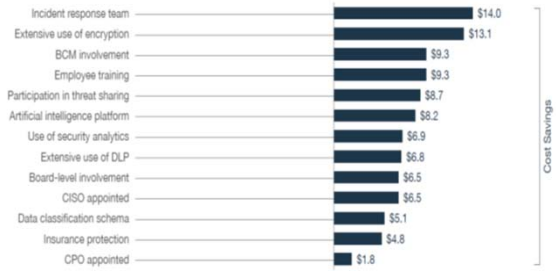
Financial Risks of Cyber Security

- Prevention is always cheaper than remediation
  - Reaction is always more slower / more expensive
  - Investigations
  - Forensics
  - Rebuilding networks
  - Restoring drives
  - Fines and penalties
  - Intangibles
  - Always cheaper to protect what you already have built

Cyber Security Costs - Information

- Study by IBM and Ponemon Institute LLC

Key Security Techniques



- Study by IBM and Ponemon Institute LLC

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Key Security Techniques

- Study by IBM and Ponemon Institute LLC

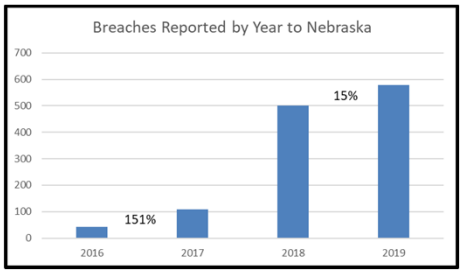
BH | BAIRD HOLM LLP ATTORNEYS AT LAW

Nebraska Breach Statistics

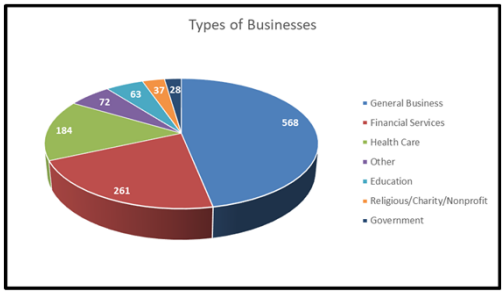
Data Description	Total Records	Nebraska Records
Cost per Record (IBM Report)	$ 250.00	$ 250.00
Total Number of Breach Reports	1231	1231
Total Number of Records	5,730,377,134	2,376,143
Total Estimated Cost	$ 1,432,594,283,500.00	$ 2,925,032,033.00
Average Records per Report	4,655,059	1,930
Total Average cost per incident	$ 1,163,764,649.47	$ 482,563.57
2019 Breaches Only	578	578
Victims	118,321,349	326,933
Average Victims	204,708	566
Total Average Response Cost	$ 51,177,054.07	$ 141,407.01
2019 for Nebraska Companies	34	34
Victims	106,767	58,631
Average Victims	3,140	1,724
Total Average Response Cost	$ 785,051.47	$ 431,110.29

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

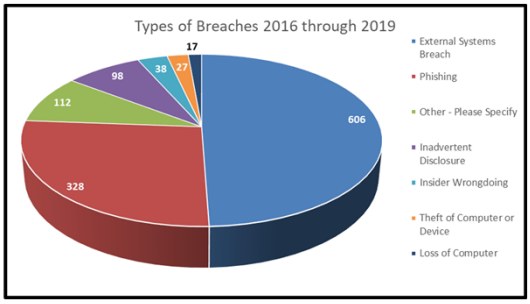
Nebraska Breach Statistics



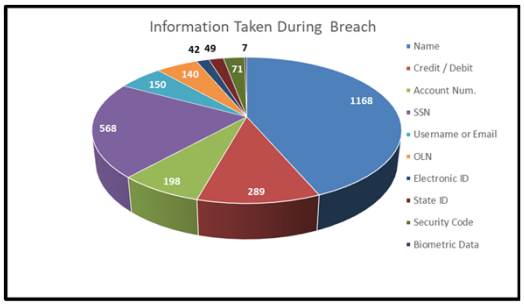
Nebraska Breach Statistics



Nebraska Breach Statistics



Nebraska Breach Statistics



BAIRD HOLM LLP ATTORNEYS AT LAW

Summary

- **Prevention Steps**
  - Permanent Plan
    - Create a Cyber Response Plan
      - Board level involvement
    - Create a Cyber Response Team
      - Stakeholder involvement
    - Create HR policies regarding personal tech
      - Practice good policies
    - Create a data map
    - Create a hardware inventory
  - Quarterly
    - Train employees
    - Create a culture of cyber awareness / security
    - Talk frequently about cyber security
    - Reinforce management buy-in
  - Annually
    - Test the plan – table-top
    - Review and Update policies and procedures
    - Update data map
    - Update inventory

BAIRD HOLM LLP ATTORNEYS AT LAW

Questions?

Disclaimer: This presentation is provided as a public service for informational, educational, or reference purposes. It is not designed to give individual advice. It is not legal advice or a substitute for legal advice. It does not create a lawyer-client relationship. Do not attempt to solve individual problems based upon the information contained in this presentation. Please seek the advice of an attorney for advice on all legal matters. No endorsement, warranty, or claim is made with respect to this presentation.

BAIRD HOLM LLP ATTORNEYS AT LAW

Thank You

Robert L. Kardell
Bkardell@BairdHolm.com
www.BairdHolm.com

BH | BAIRD HOLM LLP ATTORNEYS AT LAW

References:

- Cost of a Data Breach Study, IBM and Ponemon Institute
  - https://www.ibm.com/security/data-breach
- Global Tech Support Scam Research, Microsoft
  - https://news.microsoft.com/uploads/prod/sites/358/2018/10/Global-Results-Tech-Support-Scam-Research-2018.pdf

© 2020 BAIRD HOLM LLP

BH | BAIRD HOLM LLP ATTORNEYS AT LAW