IT Security – Recent Data Breaches, Lessons Learned and Best Practices

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Goals

- Review recent data breaches
- Highlight lessons learned
  - 9 patterns of attacks
- Best practices

Recent Data Breaches

Recent Data Breaches

- Verizon – 1,500,000 records exposed on 3/24/16
- 21st Century Oncology – 2,200,000 records exposed, a hacker gained access to a patient database
- Centene – 950,000 records exposed because of 6 missing hard drives with PHI
- JP Morgan - 76 million households and 7 million small businesses

Easy to share large volumes of data!

ID Theftcenter Data Breach Reports 2016

Recent Data Breaches – Healthcare

- Aventura Hospital and Medical Center – an employee improperly accessed 82,601 patient records
- Central Utah Clinic – notifying 30,000+ patients of a potential data breach after discovering hacker's had accessed on of the clinic's servers
- Duke University Health System – notified patients due to a stolen thumb drive that contained unencrypted patient names and physician names
- Memorial Hermann Health Systems – notifying 10,000+ of a security breach due to an employee accessing unauthorized patient information
- St. Elizabeth's Medical Center –notified patients of a potential data breach after a laptop and thumb drive were stolen from a physician's home
- Cedars-Sinai Medical Center in Los Angeles – notified 500+ patients that their protected health information may have been compromised due to an unencrypted laptop being stolen from an employees home
- Beth Israel Deaconess Medical Center to pay $100K to settle data breach

Beckers Health IT & CIO Report - Sept. 19, 2014

Recent Data Breaches – Healthcare

- **Hollywood (Calif.) Presbyterian Medical Center** staff declared an internal emergency after hackers forced the hospital's IT systems offline - The hackers demanded the hospital pay 9,000 in Bitcoin, a digital payment system, equivalent to $3.6 million - ended up paying 40 Bitcoins or ~$17,000 to get systems back
- An unauthorized party gained access to an employee's credentials at Boston-based **Brigham and Women's Hospital**, possibly compromising the protected health information of 1,009 individuals
- Cincinnati-based **UC Health** notified 1,064 patients of a data breach after learning emails containing protected health information were inadvertently sent to an incorrect email address.

Beckers Health IT & CIO Report - Jan 4, 2016, Jan 20, 2016, Feb. 19, 2016

Recent Data Breaches – Small #, Big Impact

- In 2015, there were 255 data breaches affecting 500 or more individuals reported to HHS Office of Civil Rights, and these breaches affected a total of more than 112 million health records
- With the United States population at ~ 322.8 million, ~ 34.7 percent of the population's health records were compromised last year.
- The three biggest healthcare data breaches of all time were reported in 2015, and the five biggest breaches of the year including the cyberattacks on Indianapolis-based Anthem and Mountlake Terrace, Wash.-based Premera Blue Cross — alone affected 108.2 million individuals

Beckers Health IT & CIO Report - Jan 5, 2016

Recent Data Breaches – Other HC Notes

- Out of the 90,000+ HIPAA breach cases OCR has received since 2003 – 17% have resulted in fines
- HHS Office for Civil Rights Director indicates that most HIPAA-covered entities fail to perform a comprehensive, thorough risk analysis and fail to apply the results of that analysis

Healthcare IT News – February 6, 2014 article "HIPAA data breaches climb 138 percent"

Recent Data Breaches – General Costs

- Lost customers and reputation–$$ to replace
- Ponemon Institute - $201/breached record**
  - 20% probability of 10,000 record breach in HC
- The forecasted average for 1,000 records is between $52,000 and $87,000***
- Juniper Networks - $2.1 Trillion by 2019*

*Becker's Health IT & CIO Report – May 20, 2015, **Ponemon Cost Study – May 2014,
***Verizon Data Breach Investigations Report - 2015

Recent Data Breaches – Cost Components

- Immediate Response Activities
  - Conduct investigation/forensics to determine root cause
  - Determine probable victims
  - Organize Incident Response team
  - Prepare notification and disclosure documents for victims and regulatory authorities
  - Ramping up call center
- Aftermath Activities
  - Audit and consulting services
  - Legal services for defense and compliance
  - Free or discounted services to victims
  - Identity theft protection services
  - Lost customer business or customer churn

Ponemon Institute Cost Study – May 2014,

Recent Data Breaches – OCR Penalties

- New York and Presbyterian Hospital agreed to pay OCR $3,300,000 to settle potential violations by failing to secure thousands of patient's electronic protected health information (ePHI) held on their network. Columbia University paid $1,500,000 for their part in the joint breach
- Parkview Health System has agreed to pay $800,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program in medical records dumping case
- Concentra Health Services agreed to pay $1,725,220 to settle potential violations after unencrypted laptop was stolen from one of its facilities. Concentra had taken steps to begin encryption but the efforts were incomplete and inconsistent over time

2014 HIPAA Enforcement Case Examples – www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/

Recent Data Breaches – Health Hazards

- ECRI 2015 Top 10 Health Technology Hazards

2. **Data integrity:** Incorrect or missing data in electronic health records and other health IT systems

9. **Cybersecurity:** Insufficient protections for medical devices and systems

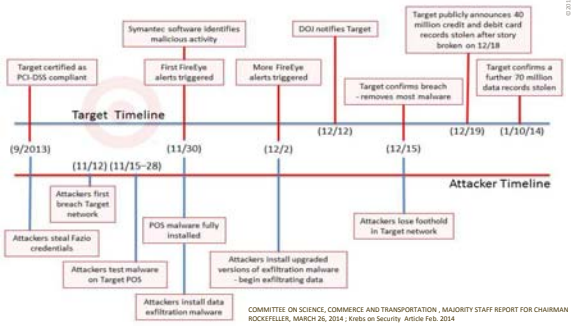
ECRI Institute web-site press release - https://www.ecri.org/Press/Pages/ECRI-Institute-Announces-Top-10-Health-Technology-Hazards-for-2015.aspx

Recent Data Breaches - Target

- Target
  - On December 19, 2013, Target publicly confirmed that 40 million credit and debit card accounts were exposed in a breach of its network
  - Thieves were able to sell information from these cards via online black market forums known as “card shops.”
  - The websites list card information including the card type, expiration date, track data (magnetic stripe), country of origin, issuing bank, and successful use rate
  - Malware new variant of “**BlackPOS**” (a.k.a. “Kaptoxa”) designed to steal data from cards when swiped at infected point-of-sale systems running **Microsoft Windows**

COMMITTEE ON SCIENCE, COMMERCE AND TRANSPORTATION , MAJORITY STAFF REPORT FOR CHAIRMAN ROCKEFELLER, MARCH 26, 2014

Recent Data Breaches - Target



COMMITTEE ON SCIENCE, COMMERCE AND TRANSPORTATION , MAJORITY STAFF REPORT FOR CHAIRMAN ROCKEFELLER, MARCH 26, 2014 ; Krebs on Security Article Feb. 2014

Recent Data Breaches – Physical Impact

- Cyber Attack Caused Damage at German Steel Mill
  (January 8, 2015)

  A cyber attack on a German steel mill caused damage to the facility. The attackers disrupted the plant's control system to make it impossible to shut down a blast furnace properly. The damage was described as "massive". This is the second documented case of a cyber attack causing physical damage – the first was Stuxnet.

- Polish Airlines LOT System Delayed Flights by DoS attack on ground computer systems

Wired Magazine – Jan. 8 article "A Cyber Attack has caused confirmed physical damage for the Second Time Ever" by Kim Zetter
via Jan. 13 SANS Institute NewsBite; SANS

Lessons Learned

How do hackers and fraudsters break in?

- Social Engineering
- Email Phishing
  – “Spear Phishing”
- Remote Access
- Third-Party

“The identity I stole was a fake!
Boy, you just can't trust people these days!”

The Fine Art of “People Hacking”

- Social Engineering uses non-technical attacks to gain information or access to technical systems:
  – Pre-text telephone calls

  “Hi, this is Randy from Comcast. I am working with Mike, and I need your help…”

  – Building penetration
    ◊ Seeding
  – Email attacks

Physical (Facility) Security

Compromise the site:

- "Hi, Joe said he would let you know I was coming to fix the printers…"

Plant devices:

- Keystroke loggers
- Wireless access point
- Thumb drives ("Switch Blade")

Phishing attacks

- Phishing heavily used in espionage attacks – targeting executives – **"inevitability of the click" – 3 e-mails to get a click!!**
- 'Ands' –
  - User **needs to take action <u>and</u>**
  - Need a vulnerability **<u>and</u>**
  - Software needs to be quietly installed **<u>and</u>**
  - Needs a communication path back to attacker

Verizon Data Breach Investigations Report (DBIR) 2013

Spear Phishing

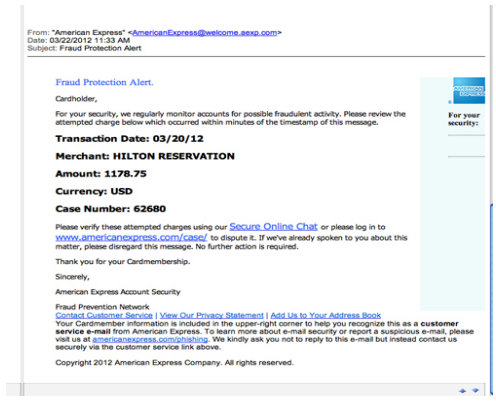
"Second Generation" phishing

Goal is to "root the network"

Install malware

- Log system activity to harvest passwords
- Use automated tools to execute fraudulent payments

Trick Administrative system users or Executives into supplying privileged userids and passwords



From: "American Express" <AmericanExpress@welcome.aexp.com>
Date: 03/22/2012 11:33 AM
Subject: Fraud Protection Alert

Fraud Protection Alert.

Cardholder,

For your security, we regularly monitor accounts for possible fraudulent activity. Please review the attempted charge below which occurred within minutes of the timestamp of this message.

Transaction Date: 03/20/12
Merchant: HILTON RESERVATION
Amount: 1178.75
Currency: USD
Case Number: 62680

Please verify these attempted charges using our Secure Online Chat or please log in to www.americanexpress.com/case/ to dispute it. If we've already spoken to you about this matter, please disregard this message. No further action is required.

Thank you for your Cardmembership.

Sincerely,

American Express Account Security

Fraud Prevention Network

Contact Customer Service | View Our Privacy Statement | Add Us to Your Address Book

Your Cardmember information is included in the upper-right corner to help you recognize this as a **customer service e-mail** from American Express. To learn more about e-mail security or report a suspicious e-mail, please visit us at americanexpress.com/phishing. We kindly ask you not to reply to this e-mail but instead contact us securely via the customer service link above.

Copyright 2012 American Express Company. All rights reserved.

For your security:

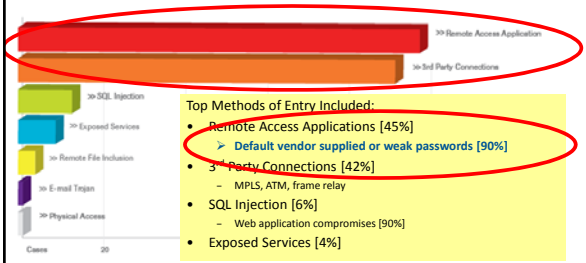
3 Primary Motives for Attacks

- Financial Gain – Organized-crime/worldwide
- Espionage/Intellectual Property (IP) – China
- Hacktivism/activism

Verizon Data Breach Investigation Report (DBIR) 2013

TrustWave – Intrusion Analysis Report

Top Methods of Entry Included:



Top Methods of Entry Included:

- Remote Access Applications [45%]
  - **Default vendor supplied or weak passwords [90%]**
- 3rd Party Connections [42%]
  - MPLS, ATM, frame relay
- SQL Injection [6%]
  - Web application compromises [90%]
- Exposed Services [4%]

NIST Authentication Factors

- Single-Factor Authentication – something you know -- password
- Two-Factor Authentication – something you physically have (i.e., a secure ID token or cell phone for Phone Factor authentication)
- Three-Factor Authentication – something you are – biometric authentication (retina, palm veins)

"2 Factor is any 2 of the above"

NIST Special Special Publication 800-51-1 Electronic Authentication – December 2011

9 Key Patterns of Attacks

- Point-of-sale (POS) Intrusions
- Crimeware
- Cyber espionage
- Insider misuse
- Web app attacks
- Misc. errors
- Physical theft/loss
- Card skimmers
- DoS attacks

Verizon Data Breach Investigations Report (DBIR) 2015

9 Key Patterns of Attacks related to HC

- Miscellaneous errors 32%
- Insider misuse 26%
- Physical theft/loss 16%
- Point-of-sale intrusion 12%
- Web app attack 9%

Frequency of data disclosures by incident patterns and victim industry

Verizon Data Breach Investigations Report (DBIR) 2015

9 Key Patterns of Attacks related to HC

- Miscellaneous errors
  - Sending sensitive info to wrong people
  - Publishing confidential information to public servers or web-sites
  - Insecure disposal of confidential information and medical data
- Insider Misuse
- Physical theft/loss

Verizon Data Breach Investigations Report (DBIR) 2014

Lessons Learned – Boston Children's Hospital

In reflecting on the Anonymous attack, the BCH CIO noted:

- Distributed Denial of Service (DDoS) countermeasures are crucial. BCH shut down all web-sites and e-mail. Staff communicated using a secure text messaging application the hospital had recently deployed
- Know which systems depend on external Internet access. In BCH's event, the EHR system was spared, but the e-prescribing system wasn't
- Make no excuses when pushing security initiatives. Children's had to shut down email, e-prescribing and external-facing websites quickly
- Separate signals from noise

CIO.com article – Sep. 14,2014 "How Boston Children's Hospital Hit Back at Anonymous"

Risk Mitigation Best Practices

Overall Approach - TK²

- Train your people - Users and Executives who are knowledgeable and savvy
- Know your network –
  - Make your networks resistant to malware
  - Segment your network
  - Make it visible to Executive management
- Know your data - data first approach
  - minimum necessary access – know access paths

Ten Keys to Mitigate Risks

1. Strong policies and training – e-mail use, strong password requirements
2. Defined user roles and permissions – minimum necessary
3. Hardened internal systems – change default passwords, media limitations (CD, USB devices), disallow local admin rights on workstations

Ten Keys to Mitigate Risks

4. Encryption strategy – mobile
5. Vulnerability management process – patch and test
6. Well defined perimeter security layers: "Know Your Network" and audit your third-party technology service providers

Ten Keys to Mitigate Risks

7. Data classification strategies "Know Your Data"
8. Defined incident response plan and procedures
9. Centralized audit logging, analysis, and automated alerting capabilities
10. Test, Test, Test

Questions?

Hang on, it's going to be a wild ride!!

Juli Ochs, Health Care Director
CliftonLarsonAllen
juli.ochs@claconnect.com
***
(612)397-3011

Lee Painter, Manager
CliftonLarsonAllen
lee.painter@claconnect.com
***
(309) 202-9531