CliftonLarsonAllen

CyberSecurity – Trends, Risks, and Practices

Jim Kreiser, CISA, CRMA, CFSA; Principal, Business Risk and IT Services

Data Breach Headlines

Other Headlines

- **California Hospital Pays $17,000 To Hackers In 'Ransomware' Attack**
- **Main Line Health employees snared in security breach**
- **Breached Credit Union Comes Out of its Shell**

  – **<u>Non Profit & Government</u>**

- **University of Maryland**
- **State of South Carolina**
- **Office of Personnel Management**
  - ◊ 2 attacks? Perhaps as many as 21 million records
- **US Postal Service**
- **Ireland**
  - ◊ 19 published case studies for 2013

Pension Headlines (from AICPA of actual reported breaches)

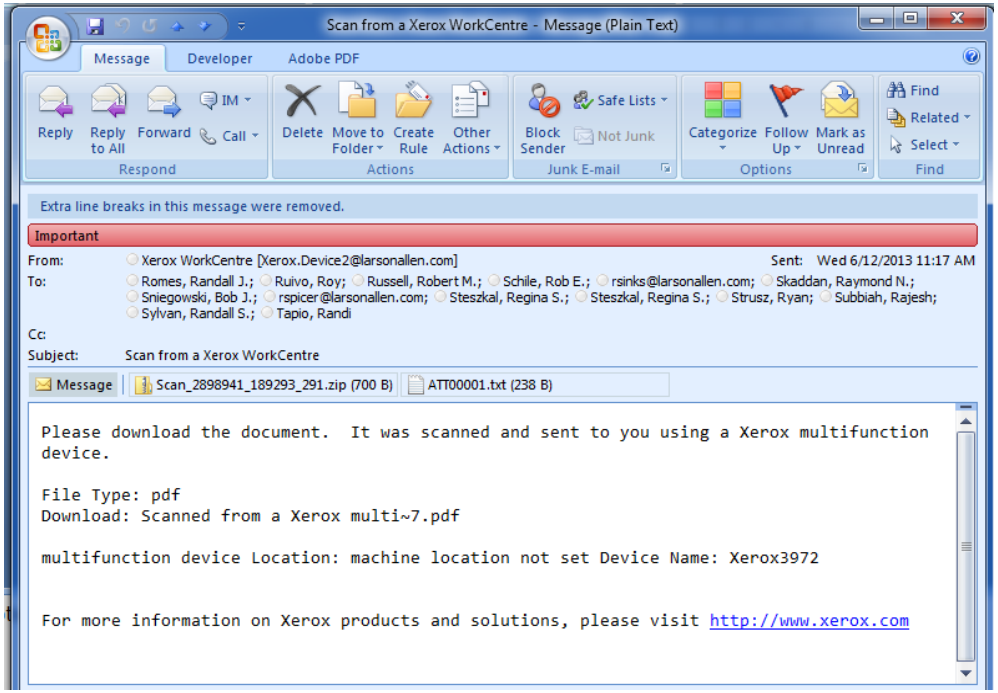
- Unauthorized user hacking into the plan administrative system after gaining administrative rights. The hacker gained access to the system by planting a virus on the company's computer. It is believed that the virus was of a type that enabled the hacker to capture keystrokes when made by an authorized person;
- Unauthorized person logging into broker website, entering ID and password, and securing payment which was sent to a name different from the name on the account;
- Person hacking into database to gain access to more than 500,000 participants' PII due to failure of the plan (and administrators) to install security system updates;
- E-mail hoax (phishing attack) that directed participants to a look-alike website prompting participants to share personal data including Social Security numbers (SSNs);
- Employee downloading confidential information for more than 450,000 participants to a home computer;
- Employee stealing electronic tapes that contained PII of plan participants and/or beneficiaries;
- Payroll provider using the same password for all clients when the payroll system was established.

Sources of Risk

- Retirement plans are an extensive source of valuable personal data about participants and beneficiaries
  - Social Security numbers
  - Dates of birth
  - Addresses
  - Bank Account Information
- Pension plans are targets due to the sources of data, number of external and remote access connections/authentications, perceived susceptibility of constituents, and financial access

Ransomware

- Microsoft reports over 500,000 PCs were infected in first half of 2015



- Zip file is preferred delivery method
  - Helps evade virus protection
- Working (tested) backups are key

The Impact

McAfee: 2014 costs of global cybercrime: **$445** billion

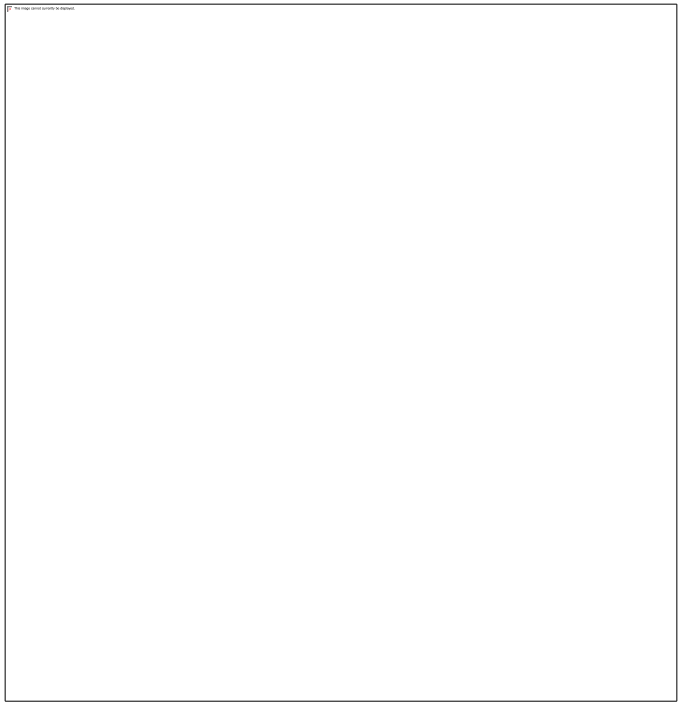
- The global cost of Cyber Crime for 2015 is estimated by the Center for Strategic and International Studies to be up to **$575bn** in it's report sponsored by McAfee.

Recent studies from the Identity Theft Resource Center report that there were **781** breaches in 2015 impacting more than **169** million records. They indicate over **6,000** breaches in the last decade, affecting over **878** million records

The Fine Art of "People Hacking"

"Amateurs hack systems, professionals hack people."

Bruce Schneier



- Social Engineering uses non-technical attacks to gain information or access to technical systems
  - Pre-text telephone calls
  - Building penetration
  - Email attacks

- Majority of attacks and breaches (reported estimates of 50% to 75%) are related to social engineering

CliftonLarsonAllen

Assessment & Validation

Risks

- Vendor Risks
- Governance Risks
- Data Risks

- **Who/what is performing transactions or processing for you?**
- **Who has your data?**
- **Where is your data?**
- **Who has access to your data?**

Models for Assessment

- Considerations of how to assess risk and controls from vendors or services providers?
  - COSO & COBIT
  - Trust Service Principles
  - Service Organization Control Reports (SOC)
    - ◊ SOC 1 vs. SOC 2
  - Service Level Agreements (SLA) and Compliance Items
  - Other key reports/metrics include PCI, other security/compliance reports (i.e. ISO, NIST, CSF, etc.), contractual

CliftonLarsonAllen

Leading Practices

Leading Practice(s) to Consider

- Fiduciary Standard of Care
  - Strict (and high) standard of care – fiduciaries must carry out their responsibilities with the level of attention, care, skill, prudence, and diligence under the circumstances prevailing at that time, which a prudent person acting in a similar capacity and familiar with such matters would use.
  - Negligence is also a form of exception. Not acting (or ignorance) can be as bad as a specific inappropriate or unauthorized action.
- "Commercially Reasonable"
  - Some state privacy laws and regulations are using the standard of "commercially reasonable". Agents or organizations must apply commercially reasonable efforts to mitigate risks/breaches. In the financial sector, this is often construed to mean an employee and constituent/member perspective.
- In some situations, personal liability, and/or other criminal and civil penalties may apply, as well as organization liability, penalties, and reputational risk

Leading Practice(s) to Consider

- Test, Test, Test

  Social Engineering Internal Vulnerability Penetration Testing

- Other Critical Items to Consider

Incident Response	Intrusion Detection	Intrusion Prevention
Email/Server Hardening	User/Employee Awareness	Customer Awareness
IT General Controls	Access Management	Network Segregation
Distribution Interfaces	Authentication/Access	3rd Party & Remote Access

- Security as a CULTURE*: Security should not be treated as an IT department responsibility, but rather a culture that permeates the entire organization. IT controls and tools are effective, but unaware or irresponsible employees/users may circumvent those controls.*

Questions?

Appendix – Links/References

California Hospital Ransomware
http://sanfrancisco.cbslocal.com/2016/02/18/california-hospital-ransomware-attack-hackers/

Main Line Health
http://www.delcotimes.com/article/DC/20160302/NEWS/160309907

Breached Credit Union Comes Out of its Shell
http://krebsonsecurity.com/2016/02/breached-credit-union-comes-out-of-its-shell/

University of Maryland
http://www.umd.edu/datasecurity/
http://www.baltimoresun.com/news/maryland/education/bs-md-umd-data-breach-audit-20141210-story.html

State of South Carolina
http://www.pcworld.com/article/2015543/irs-blamed-in-massive-south-carolina-data-breach.html

- **Office of Personnel Management**
  - http://www.nationaljournal.com/tech/hack-opm-office-personnel-management-cyber-million-20150709
    - ◊ 2 attacks?
- **US Postal Service**
  - https://about.usps.com/news/fact sheets/scenario/customerFAQs_Final.pdf
- **Ireland**
  - Data Protection Commissioner
    - ◊ https://dataprotection.ie/viewdoc.asp?DocID=1441&ad=1
- http://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx