Ransomware, Viruses, and Hackers in Health Care: Five Steps to Avoid Being the Next Victim

Michael Overly and Chanley Howell

February 29, 2016

FOLEY

FOLEY & LARDNER LLP

16.11866

Agenda

- The current threat
- Rising information security risks
- Why are cybersecurity risks so insidious?
- Why now?
- Five Steps to Mitigate Risk

16.11866

Current Threat

- Imperva reports Cryptowall 3.0 most successful ransomware of all time, causing $325 million in damages so far
  - 44 percent of all ransomware victims have paid to get their data back
  - 39 percent say they expect to be attacked again, in the future
- Negotiation is possible: $3.6M to $17,000
- Unpatched, outdated software and “insiders” are the cause
- Untraceable bitcoin
- Paying doesn’t mean it won’t happen again
- Paying doesn’t mean all elements of the virus have been identified and removed

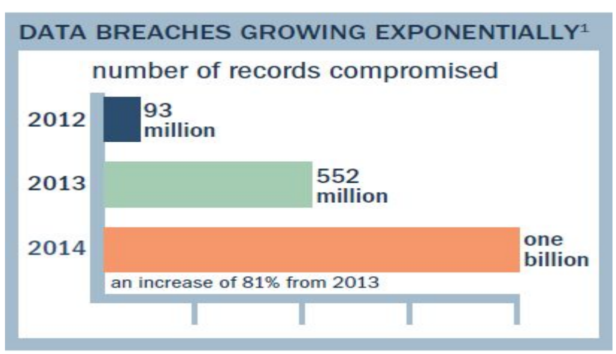
Health Care Vulnerabilities

- EHR benefits can result in heightened risks
- Not necessarily about stealing PHI or other data
- Identity theft typically does not threaten patient care and safety
- Ransomware can bring organization to its knees
- Expert consensus – increase in attacks and devices

Health Care Vulnerabilities

- Not just EHRs – devices (monitors, pumps, etc.)
- Industry push for connectivity adds risk - HIEs, and community physicians
- Common deficiency – lack of effective risk assessments
- Vulnerabilities through vendor relationships
- It's not just IT / technical security – PEOPLE

Rising Information Security Risks: Data Breaches



[1] Steve Ragan, *Nearly a Billion Records Were Compromised in 2014*, CSO (Nov. 17, 2014) http://www.csoonline.com/article/2847269/business-continuity/nearly-a-billion-records-were-compromised-in-2014.html.

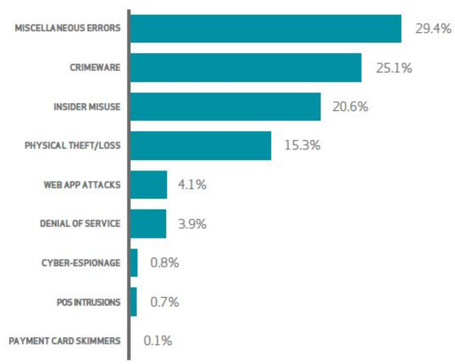
Internet Security Threat Report 2014 (2013 Trends, Volume 19) Symantec Corporation (2014) https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

2/26/2016

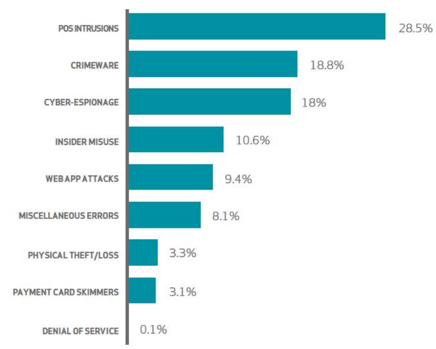
7

Sources of Security Incidents

All security incidents, 2014



Security Incidents with confirmed data breach, 2014



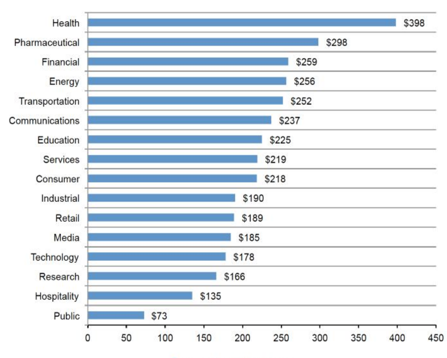
Source: 2015 Verizon Data Breach Report

 16.11866

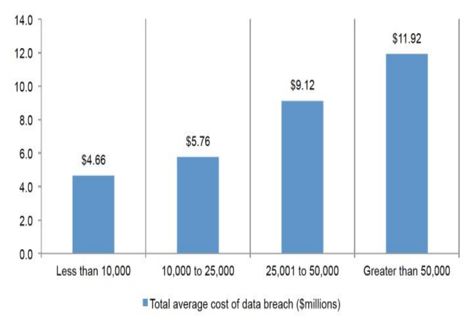
8

Rising Information Security Risks: Cost increases by size and industry

The cost per record varies by industry: Average cost =$217/record (US Data)



Total cost of a breach varies size of the breach: Average cost = $6.53 Million (US Data)



Source: Research Report, *2015 Cost of Data Breach Study: United States*, Ponemon Institute (2015)

 16.11866

Why Cyber Attacks are so Insidious

 16.11866

Why Now?

- Big Data
- Connectivity/Internet of Things
- System Complexity
- Interconnectivity with Vendors, Business Partners, and Other Third Parties
- Ability to steal from many quickly and in many ways

 16.11866

Five Steps to Mitigate Risk

- Step 1: Move Information Security to the Right Level. Information Security is <u>not</u> a technology department issue. It is an enterprise, senior management issue.
  - Ultimate responsibility rests with senior management, with the correct governance, management and culture throughout the business.
  - Senior management should seek assurance that key information risks are both assessed and prioritized, and that there is regular monitoring where threats and vulnerabilities are constantly changing.
  - Senior management may face direct liability for failure to exercise reasonable judgment with regard to information security governance.

Five Steps to Mitigate Risk

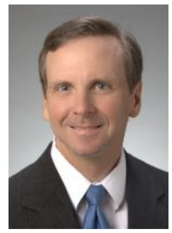
- Step 2: Inventory Your Data. Understand where data resources are located and how they are used.
  - Risk cannot be controlled until this step is completed.
  - Complex task, particularly in a cloud environment.
  - <u>Focus on backups, disaster recovery, and business continuity</u>
- Step 3: Conduct a top-to-bottom review of existing information security policies and procedures.
  - Update, as necessary.
  - Personal responsibility of individual users is critical for success. Training and clarity of policies is key.

Five Steps to Mitigate Risk

- Step 4: Update Systems, Avoid End-of-Life Products, Remove Unsupported Software.
- Step 5: Be Vigilant of Your Vendor and Partnering Relationships.
  - The importance of diligence activities.
  - Ensure appropriate contractual information security obligations. A BAA is not enough.

Questions?

Speakers



Michael Overly
Partner, Privacy & Security
(213) 972-4533
moverly@foley.com

Chanley Howell
Partner, Privacy & Security
(904) 359-8745
chowell@foley.com

16.11866