NTT DATA Services

Cybersecurity in- Healthcare

Dr. Vivek Mahadevan

Apr 2019

The Current Scenario

- Healthcare organizations are digitalizing patient medical records
- Access to clinical information at the POC
- Clinicians are using devices to access patient information remotely
- Hospitals are being targeted by cyber criminals that have a huge reputational and financial impact
- Healthcare organizations are being targeted by three types of attackers:
  - Nuisance attackers: such as the creators of commodity malware
  - Advanced persistent threat (APT) attackers
  - Cyber criminals

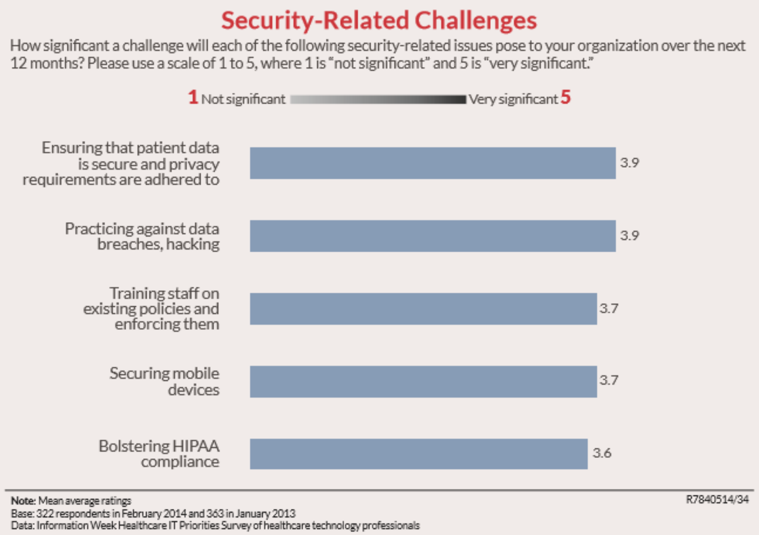
The Demand for EHR Information in the Black Market

- According to the FBI, EHRs are more valuable than financial data
- EHRs have an average value of $50 compared to $1-15 for credit card information
- EHRs contain demographics, diagnosis codes, billing information and prescriptions
- Fraudsters can use EHR information to order controlled medications or file false claims
- EHR theft takes almost twice as long to detect then normal theft. Gives fraudsters that much more time to milk the information
- EHR leaks more difficult to resolve than credit cards that can be swiftly cancelled
- The demand for EHR information is fueling the increased cyber attacks on healthcare organizations

Prognosis

- Since 2009, more than 1,185 data breaches have been reported as being in violation of the Health Insurance Portability and Accountability Act (HIPAA).
- Breaches to date have affected more than 133 million patients.

Figure 1: Security challenges facing healthcare organizations

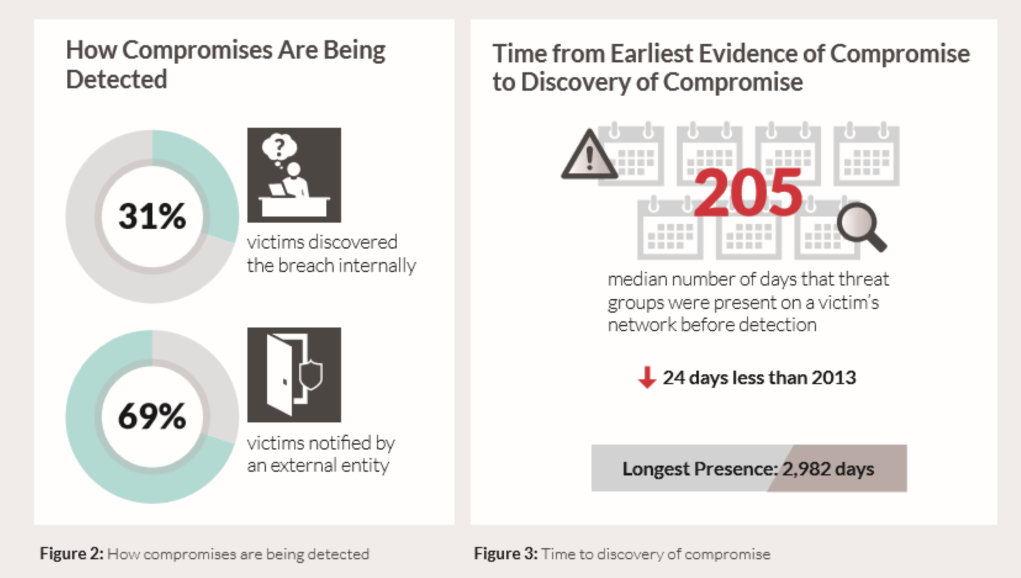


Note: Mean average ratings
Base: 322 respondents in February 2014 and 363 in January 2013
Data: Information Week Healthcare IT Priorities Survey of healthcare technology professionals

The U.S. Department of Health and Human Services, Office for Civil Rights, Breach Portal. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Cont..

- Healthcare organizations have become prime targets for attacks. Security incidents in the industry have more than doubled over the past five years.
- The average data breach costs $2.1 million, and the total cost to the healthcare industry in 2014 exceeded $6 billion.



How Compromises Are Being Detected

Time from Earliest Evidence of Compromise to Discovery of Compromise

Figure 2: How compromises are being detected

Figure 3: Time to discovery of compromise

Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2015
Ibid..

Healthcare’s Security Challenges

- Many doctors resist onerous security mechanisms that stand between them and the information they need to do their jobs.
- IT leaders at many healthcare organizations have difficulty in attaining adequate funding for security.
- Their security staff is stretched thinly.
- The Security models tend to be reactive rather than proactive.
- The average cost of a healthcare breach is $363 per exposed record, more than twice the average across all industries.

How do you Bulletproof Yourself?

- Healthcare organization to have data security strategy in place
- Identify and secure critical data
- Data encryption
- Data access to be controlled
- Perform detailed logging and alerting
- Use token-based two-factor authentication for remote access
- Segment the network to limit the attacker’s ability to move through the environment
- Protect privileged accounts with unique passwords using a password vault
- Proactively hunt for evidence of compromise
- Have an enhanced incident response (IR) plan in place

NTT DATA

Trusted Global Innovator