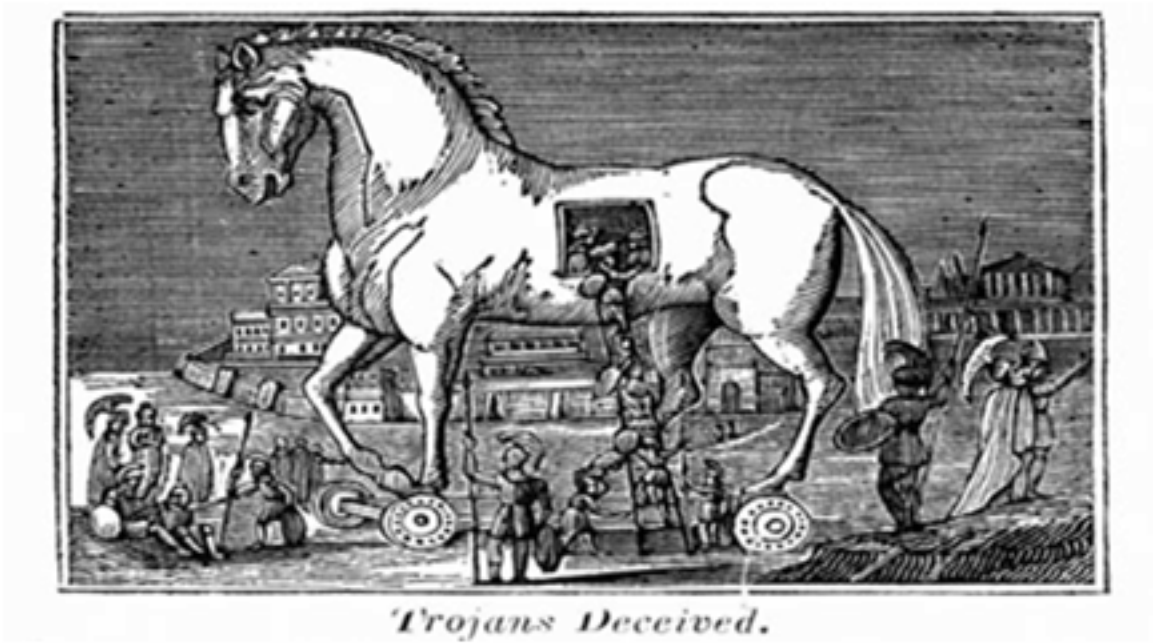

Trojans Deceived.

The Enemy is Inside the Gates

Insider Threats in Healthcare

Deconstructing the Verizon Report

Source

A subset of data from the Verizon Data Breach Investigations Report (DBIR)

https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pdf

Healthcare, a Unique Threat Landscape

58% of incidents involved insiders – healthcare is the only industry in which internal actors are the biggest threat to an organization.

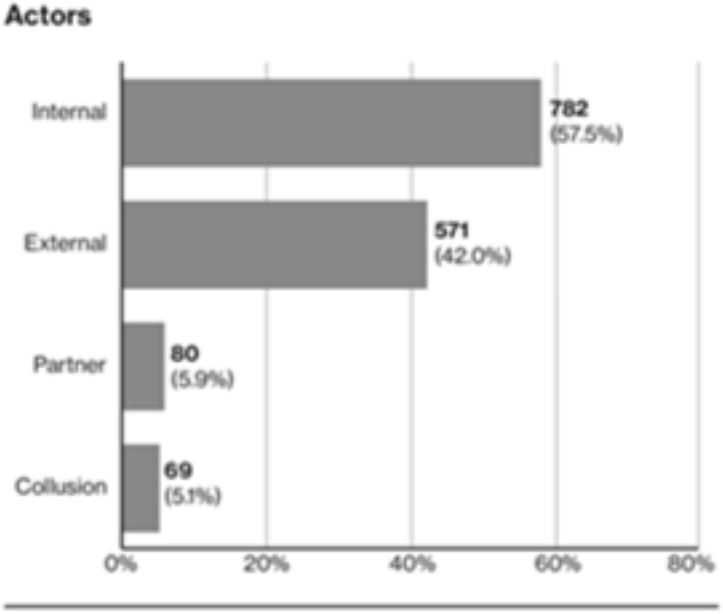

Figure 1.Threat actors within PHIDBR dataset, n=1,360

https://healthitsecurity.com/news/58-of-healthcare-phi-data-breaches-caused-by-insiders

https://www.beckershospitalreview.com/cybersecurity/healthcare-the-only-industry-where-insider-threats-outnumber-external-threats.html

http://www.verizonenterprise.com/verizon-insights-lab/phi/2018/

Data Types Effected

79 percent of reported incidents involved Protected Health Information (PHI), 37 percent involved Personally Identifiable Information (PII) and 4 percent involved Financial (FIN)

Percentages > 100% due to the fact that some breaches effected multiple types of data

https://healthitsecurity.com/news/58-of-healthcare-phi-data-breaches-caused-by-insiders

https://www.beckershospitalreview.com/cybersecurity/healthcare-the-only-industry-where-insider-threats-outnumber-external-threats.html

http://www.verizonenterprise.com/verizon-insights-lab/phi/2018/

A Breakdown of Threats

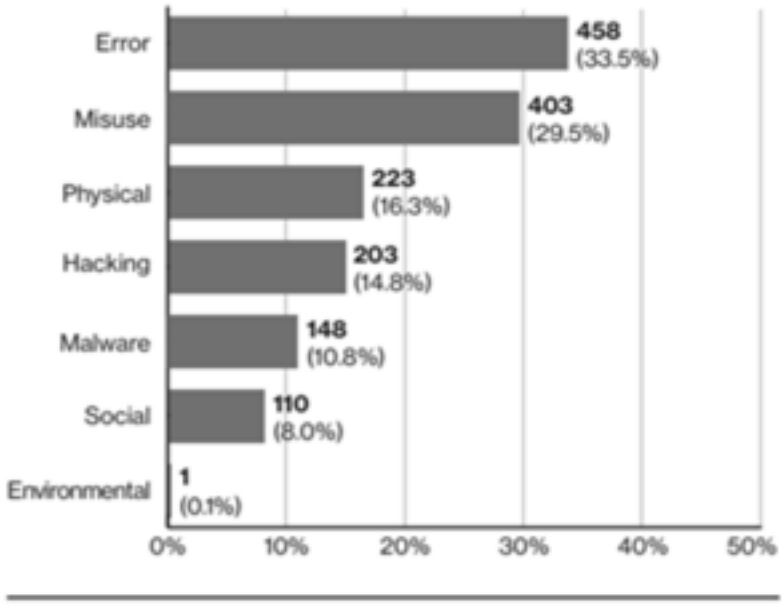

Figure 2. Threat action categories within PHIDBR dataset, n=1,368

https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pd

Analysis of Errors

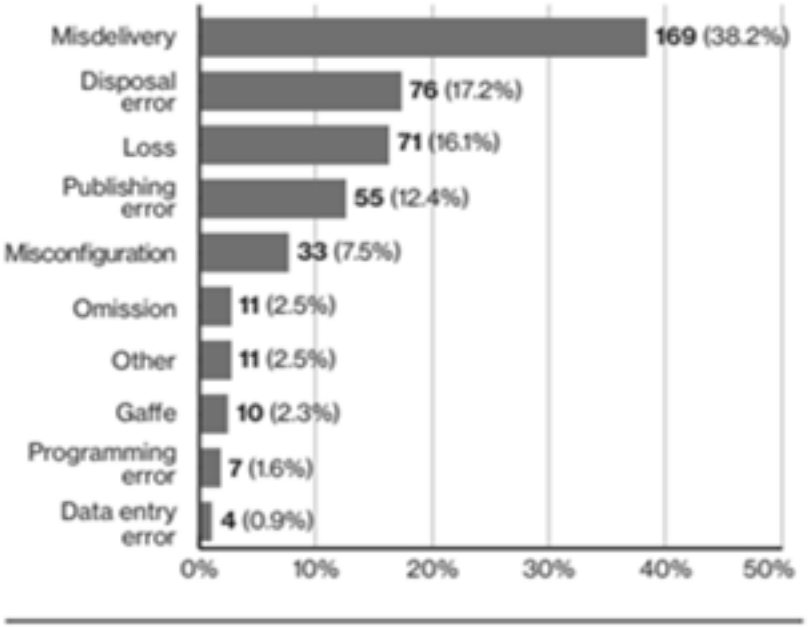

Figure 3. Top threat action varieties within Error, n=442

Top 5 – Healthcare has a “paper problem.” (43%)

https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pd

Data Misuse by Users

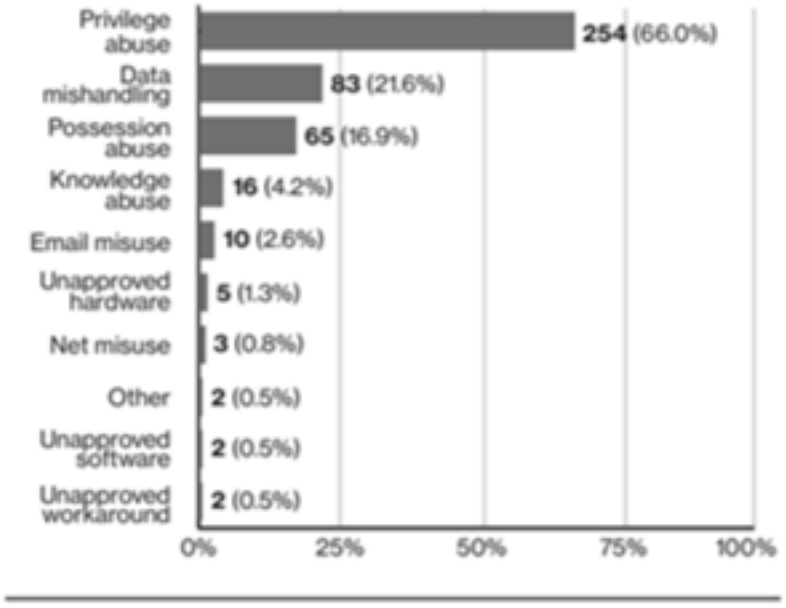

Figure 4. Top threat action varieties within Misuse, n=385

Misuse requires a “distinct motive”

https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pd

Physical

95.2% - Stolen unencrypted laptops

https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pd

“Hacking”

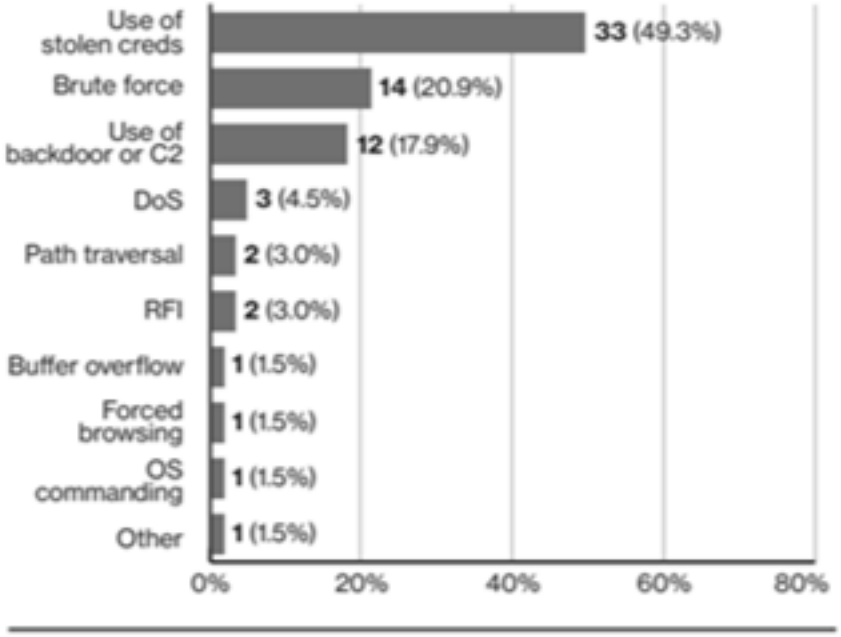

Figure 6. Threat action varieties within Hacking, n=67

49.3 % - Phishing, Social Engineering, etc. (14.8% Overall)

https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pd

Malware

70.5% - Ransomware (10.8% Overall)

https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pd

Social - “The Carbon Layer”

81.6% - Phishing & pretexting (8% overall)

https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pd

Privilege Escalation & Abuse

"Two-thirds of all incidents involved unapproved or malicious use of organizational resources." This entails in most cases hospitals not properly restricting and assigning access to PHI/PII

"You can consider authentication and access control to be the two foundations of security. If you don't do a good job on these tasks it's unlikely that the rest of your security strategy will be effective." – Dulaney & Easttom

https://healthitsecurity.com/news/58-of-healthcare-phi-data-breaches-caused-by-insiders

Dulaney & Easttom, CompTIA Security + Study Guide, Sixth Edition, Sybex

Data Mishandling

16.9 percent of incidents involved "Possession Abuse,"

Essentially nurse A tells Nurse B who is not assigned to a particular patient "did you hear about…?'

https://healthitsecurity.com/news/58-of-healthcare-phi-data-breaches-caused-by-insiders

Fraud in the Healthcare Sector

The healthcare sector has the third highest fraud ranking in the United States just behind the government sector. Finance was number one

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf

Breach Discovery

"Approximately one-third of data breaches were not discovered for years, with another third going undiscovered for months."

https://healthitsecurity.com/news/58-of-healthcare-phi-data-breaches-caused-by-insiders

Budget & Staffing Realities

It's a commonly cited fact by hospital CISO's that 3 percent of a hospitals budget goes towards IT infrastructure and 3 percent of that budget goes to IT security

It's also common to have over 10 percent of hospital staff at any given time on a hospital floor be "agency staff," temporary, per diem employees from an outside staffing agency not trained in cybersecurity best practices or even organizational policy

What is the Effect of all of This?

"You should consider our hospital networks to be a toxic environment."

- CISO for a large Cyber Aware, Health Delivery Organization (HDO)

Before We Blame Hospitals

Working in healthcare is hard

It's literally a life or death profession

Food for Thought

Medical staff assure the patients well being over their data security but are those two mutually exclusive?

What is the happy medium between safe and secure?

Is it that healthcare organizations are doing a poor job of preventing data breaches or does it only appear that way because they are required to report them and some other industries aren't?

https://healthitsecurity.com/news/58-of-healthcare-phi-data-breaches-caused-by-insiders

Small Likelihood / Big Consequences

While the precedence of hackers attacking medical systems to cause patient harm is still forthcoming the threat is real

https://ucsdnews.ucsd.edu/pressrelease/how_unsecured_obsolete_medical_record_systems_and_medical_devices_put_patient_lives_at_risk

What Can be Done to Remedy This?

Medical Device and Software Manufacturers can build technology with human factors and the realities of current hospital networks in mind.

(International Standard IEC 62366 – Application of Usability Engineering to Medical Devices)

- Performing an incorrect action
- Incorrectly omitting a necessary action
- Excessive workload
- Environmental distractions
- Fatigue
- Inattention
- Insufficient experience/training
- Lack of familiarity with technology
- Lack of fluency in language
- Working at a fast pace

What Can be Done to Remedy This?

Hospitals can work to properly segment access to sensitive data

Hospitals can implement strong audit processes

Hospitals can allocate more resources to security and security related employee training

Academic Institutions can incorporate cybersecurity training into their clinical programs to expose clinical staff to cybersecurity considerations BEFORE entering the field

Questions / Thoughts

Interactive discussion

If you were a hospital CISO what would you do to combat this?

Who's responsibility is hospital security?

Contact Info

Matthew McMahon

Matthew.McMahon@Salve.edu

@InfoSec617

linkedin.com/in/mcmahonconsulting/