Verizon DBIR

REPORT ANALYSIS

Michael Miller

- IT Security Administrator at Henry County Hospital
- Certified Ethical Hacker (CEH)
- Background in Networking, Security, and Computer Programming

Threats to Healthcare

- 458 Incidents 296 with confirmed data disclosure

Threat actors:

- 32% External
- 68% Internal

Motives:

- 64% Financial
- 23% Fun
- 7% Grudge

Data Compromised:

- 69% Medical
- 33% Personal
- 4% Payment

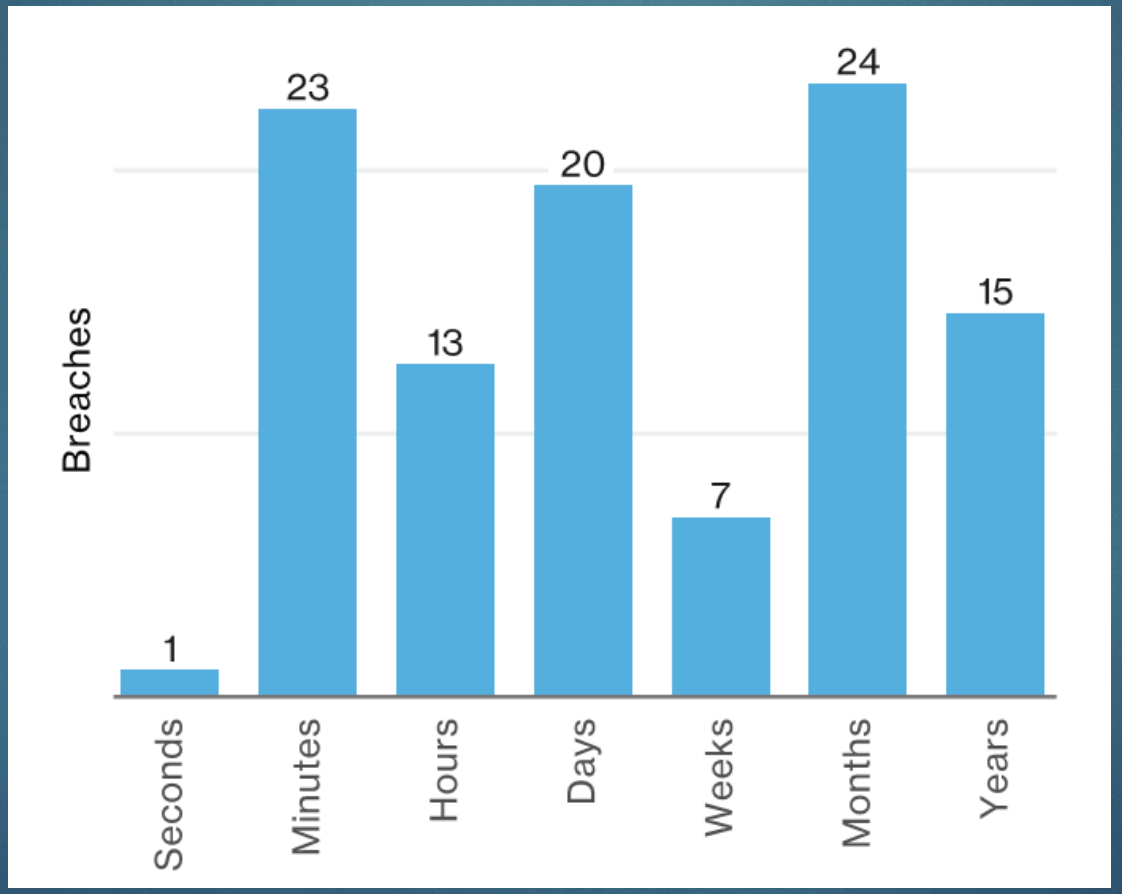
81% of Healthcare Breaches Were Caused By:

- Privilege Misuse
- Miscellaneous Errors
- Physical Theft and Loss

Other Notable Threats:

- Social Engineering / Phishing
- Business Email Compromise (BEC)
- Ransomware

Breach Detection



Privilege Misuse – All Industries

- 60% of cases insiders were hoarding data in the hopes of converting it into cash in the future
- 17% of cases insiders were just doing unsanctioned snooping
- *“Personal information and medical records (71%) are targeted for financial crimes, such as identity theft or tax-return fraud and occasionally just for gossip value.”*

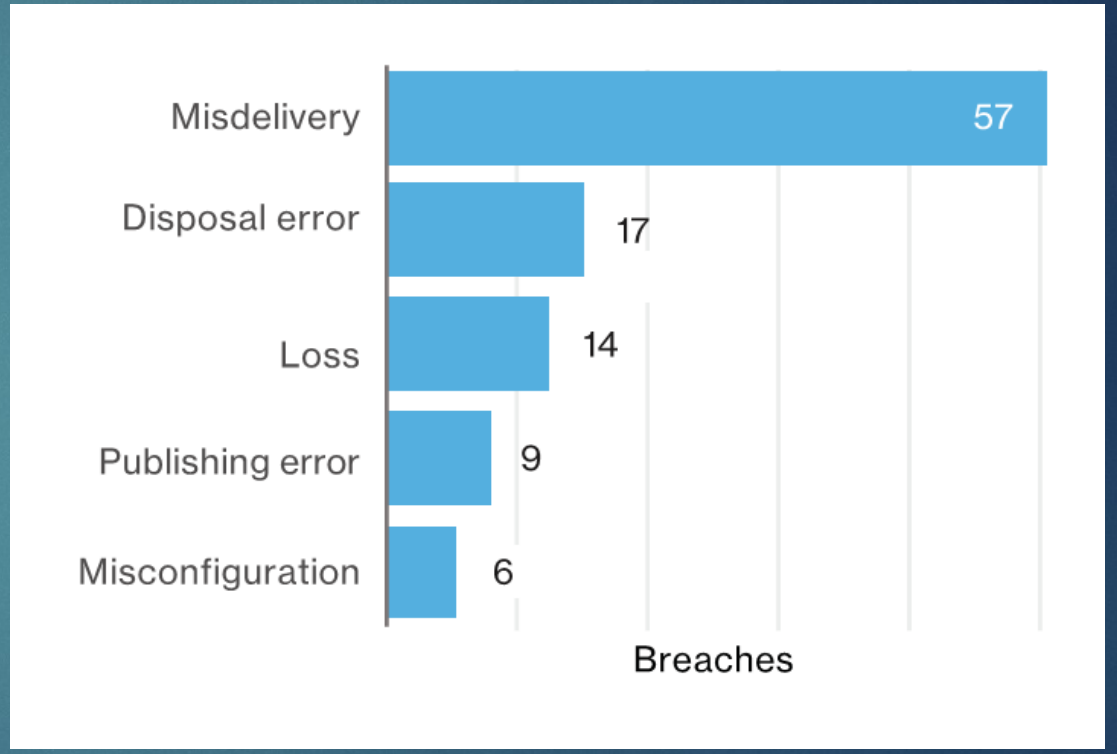
Privilege Misuse – Mitigation

- Limiting access to “need to know”
- Provide acceptable use training
- Log everything and regularly audit for misuse
- Monitor privileged accounts for excessive access
- Monitor device connections (USB) and use DLP scanning on writes

Even if your employees are all “model employees” these controls can help catch external attackers masquerading as privileged users

Miscellaneous Errors – All Industries

- Not all incidents and breaches require malice
- Misdelivery was most common source of breaches for miscellaneous errors
- Improper disposal is also still a major concern
- Devices are more often lost than actually stolen



Miscellaneous Errors – Mitigation

- Have a second individual verify accuracy before sending out information (by postal service, or publishing in media)
- Have formal procedures for discarding **ANYTHING** that may contain sensitive information
- Use mistakes as learning opportunities and discuss them in training
- Encrypt all mobile devices and storage

Have documentation for ALL of the above

Physical Theft & Loss – All Industries

- 5,698 Incidents, 74 with confirmed data disclosure
- People will inevitably lose things, the only thing we can really do is take measures to **reduce the impact of loss** of physical assets

Physical Theft & Loss – Mitigation

- As with miscellaneous errors, do full hard disk encryption on mobile devices (ensure this is documented)
- Use encrypted media (e.g. flash drives) for transporting sensitive information in digital form outside of the network
- **Discourage printing of sensitive information unless absolutely necessary as a majority of loss was physical documents**
- Implement print management software

Social Engineering – All Industries

- Credentials were stolen in 61% of breaches involving social engineering
- Social attacks were used in 43% of all breaches investigated
- Phishing variations composed 93% of social incidents
- Often followed by malware installation

Social Engineering – Mitigation

- **Educate, Educate, Educate!**
- Focus on detection and reporting
- If possible run phishing simulations
- Prepend external emails with an [External] flag in the subject line or body so that staff know the email is from an outside source

Ransomware

- Ransomware attacks were not counted as breaches in the DBIR as they cannot confirm that data was violated
- HHS has given guidance that ransomware incidents should be treated as a breach for reporting purposes, because if the data was able to be encrypted, there is no way to prove it wasn’t exfiltrated
- In 2016, ransomware accounts for 72% of malware incidents in the Healthcare industry
- Healthcare was the number two industry targeted by ransomware

Ransomware – Mitigation

- **Backup, Backup, Backup!**
- Regularly test backups to ensure they actually work
- Implement least privilege – helps mitigate reach of impact
- Use privileged accounts only when absolutely necessary
- Install behavioral based anti-malware (can stop ransomware in its tracks, and in some cases roll back)
- https://www.nomoreransom.org/

Key Takeaways

- “Never let a breach go to waste”
- Log and audit everything
- Make people your first line of defense – train & educate staff
- Flag external emails so staff know they are from outside sources
- Keep data on a “need to know” basis
- Patch early, patch often (average patch cycle is 60 days)
- Encrypt sensitive data
- Where possible, have a second individual verify information
- If possible, join an information sharing organization (e.g. Infragard)

Questions?