

Medical Record & Device Security in the Hyper Distributed World of Patient Care

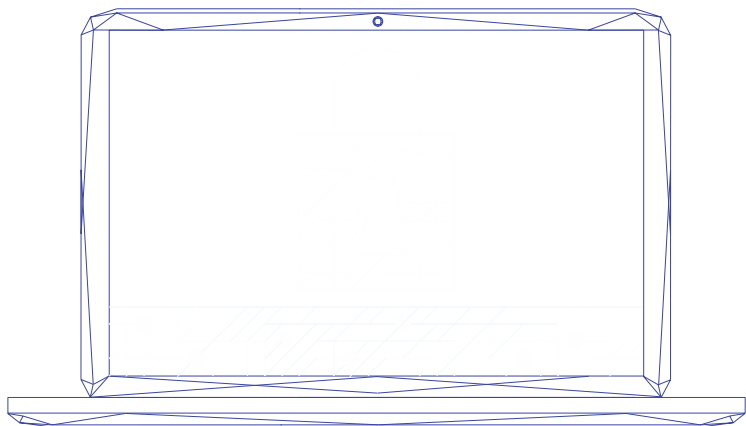
A systematic proactive action plan to
address and mitigate potential risks, and
keep cybercriminals at bay

Dr. Nameer Haider

May 2017

Understanding The Problem

Why is Cybersecurity failing?



1

Networks “fail open”, enabling data theft when compromised.

2

Administration credentials have full access to all data, and so do the hackers that steal those credentials.

3

Individual security solutions are in a silo and don't interact well with each other, if at all.

4

The domain model of networking was created “pre-internet” when physical security was the primary level of security.

5

Mobile / BYOD (Bring Your Own Device) and IoT have made the situation exponentially worse

Significantly Higher Cyber Risk Due To Healthcare's Complexity

Unique industry with a vast 'eco-system' of inter-connected stakeholders with hyper-distributed access to medical and/or billing records:

- Patient - Family / Full-time Care (for dependents)
- Primary Physician
- Specialists
- EMT / Ambulatory
- Hospital / Clinic / Care Facility
- Pharmacist
- Medical Device Manufacturer
- Third-Party Billing Service Providers
- Health Insurance Plan Providers / Medicare / Medicaid
- Life Insurance Plan Providers
- Employers Insurance (Workers Comp, Disability, etc.)
- Benefits Package Provider / Broker / Agency
- Employer / Armed Services
- Schools / Colleges
- Social Security Administration
- Law Enforcement
- Attorneys
- Etc.

Data Breach Incidents Continue to Plague Healthcare; Huge Rise in Internal Data Theft Incidents

Sample News Headlines So Far In 2017

- “Presence Health is the first HIPAA monetary enforcement for a health organization. \$475,000 for less than 1,000 records.” – **HealthcareIT News**
- “In February 2017, external hacking accounted for only 12% of reported healthcare data breaches.” – **Healthcare Informatics**
- “The medical/health care sector is leading again, posting 25.3% (79) of all data breaches as of March 31, 2107.” – **Wall St. Journal**
- “According to data released by KPMG in 2016, medical device hacking has rapidly increased.” – **Bloomberg**
- “Erie County Medical Center plans to have computers running in next 72 hours; FBI still investigating cybersecurity incident“ – **Beckers Hospital Review**

Medical – The Highest Value Information On The ‘Dark Web’

While credentials for popular online services are currently more valuable than credit card info...

PayPal™

\$6.43



\$3.02



U B E R

\$3.78



\$0.22

NOTHING tops medical records for large-scale fraudulent schemes, so sell-on fees are high.

\$20 - \$50 per record*

*Aite Group / Trend Micro 2017 report



Image via Intel Security Report – shows alleged healthcare hacker DarkOverlord advertising a breach

Data Breaches Are Leading To Litigation

Class-action Lawsuits Are Expected To Increase With Incidents



Recent lawsuits have seen impacted individuals, ranging from **identity theft victims and disgruntled shareholders**, go after board members as a result of data breaches at several high-profile companies.



Attorneys for Target, Home Depot, and Wyndham Hotels have recently negotiated significant settlements to keep their officers out of the court room, as lawsuits have challenged their **fiduciary responsibilities**.



Courts have remarked that testimony provided by officers and partners, stating that they have given IT staff complete autonomy for cybersecurity programs in their organization, have been **“naive and irresponsible”**.

Healthcare's Also Facing a Ransomware Epidemic

Sector Is Learning How To Deal With It

- Healthcare is **more likely to pay ransomware demands** when it occurs due to critical nature of medical records
- **Hollywood Presbyterian** became the poster child for ransomware after paying \$17,000 to unlock its impacted systems
- **Sutter Health** shared that in dealing with ransomware it had to consider which medical devices were vulnerable
- **Northwell Health** has concluded that both internal and external email contribute to ransomware and that healthcare's fractured systems make them more vulnerable than other industry sectors
- **Catholic Health Initiatives** has taken steps to prioritize their medical devices, so ransomware incident risk can be managed

Medical Devices Introduce Additional Cyber Liability



Abbott acquired St. Jude Medical for \$25 Billion, and is pursuing Alere at a \$5 Billion+ price tag, but medical device manufacturers bring **hidden liability in cybersecurity risk**.



On April 12, 2017 Abbott received warnings from the FDA regarding a range of devices, including the St. Jude Merlin@home product, as **cybersecurity vulnerabilities** may not be adequately addressed.



The FDA gave **Abbott just 15 days to fix the Merlin@home issues**, citing Risk Management obligations, as well as a number of codes under the Food, Drug and Cosmetic Act, which governs these devices.

Why Healthcare tech is particularly challenging

Complex regulatory requirements, often different for record types: EMR / EHR / PHR

Ongoing CME requirements create an ever-changing landscape

Clinics and Hospitals provide 'rolling' access to a wide variety of authorized personnel:

- Permanent
 - Semi-permanent
 - Scheduled / As-required
 - Occasional
-

Varying information format types: Text, Forms, Charts, Graphs, Images, etc.

Healthcare sector is making use of a myriad of inadequately secured, network-connected, medical devices; providing further hack-able entry points into already porous systems

Current Security Technologies don't prevent the end game – Data Theft

| Security tool type | What it protects from | What is doesn't protect |
|-----------------------|------------------------------|-----------------------------------|
| Router / Firewall* | Unauthorized Network Traffic | Data |
| TLS / SSL Certificate | Secures HTTP traffic (HTTPS) | Data |
| Spam Filter* | Unauthorized email | Data |
| Anti-virus* | Unauthorized software | Data |
| Disk Encryption | Data on the disk | Data Moved or Copied |
| Data Loss Prevention* | Data Policy Enforcement | All Data Types (highly selective) |
| Intrusion Detection* | In-network intruders | Data |

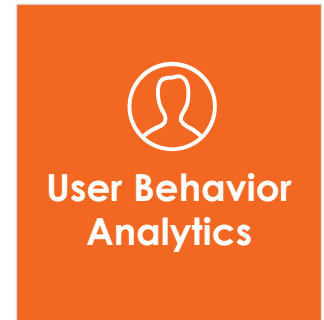
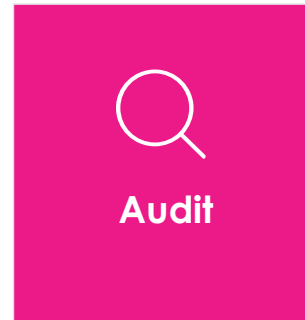
*Security tools which can be spoofed, bypassed, or produce false positives. Require regular vulnerability updates.

The Solution:

Don't Rely On Network Protection; Secure The Data

The network protection model is widely acknowledged as having failed. The solution lies in shifting focus to securing the data at the file or record level.

There are four cornerstones to securing data assets from Theft, Misuse & Loss:



Part 1

Secure The Data At All Times

Encryption



- 256 AES
- Zero-knowledge
- Rotate keys after incidents

- Encrypt data on the network/cloud and endpoint device (Desktop, Mobile, Medical Device, IoT), wherever it travels or resides
- Ensure encryption keys are stored and managed client-side, so system is zero-knowledge to solution provider.
- Revoke access to data, even data taken off the network, at any time by rotating encryption keys.

Part 2

Integrate ID Management With Access Controls

**Identity
Management**




- User ID
- Device ID
- Rule enforcement
- Multi-factors

- Explicitly control access to data, as required by function
- Require multiple ID tokens to ensure credentials are not compromised
- Restrict IT Administrator access to data records not covered by their role

Part 3

Audit Interaction With The Data

Audit



- Every transaction
- Encrypted
- Tamperproof
- Irrefutable
- Back-up and version controls

- Audit access to data at all times, record all interaction with data by individual users:
 - Read-only
 - Write / Edit
 - Copy
 - Rename
 - Print / Screen Print
 - Download
 - Move
 - Attachment to Email
 - Etc.

- Create versioning for back-up and restore

Part 4

Analyze User Behavior For Superior Data Management

User Behavior Analytics



- Deterministic
- Time aware
- Automated response

- Understand the who, what, when, where, and how data is created, managed, and accessed
- Revoke / Block access data when irregular or exaggerated activity occurs
- Automate threat remediation, from both external and internal threats.
- Without user behavior analytics there is no reliable method to prevent data theft by authorized users.

Vendor Selection

Chose Wisely – Not All Cyber Vendors Are Suitable For Healthcare

Cyber security is a rapidly expanding vertical, with many new entrants, so screen for certification in risk areas:

- PHI
- HIPAA
- State legislation

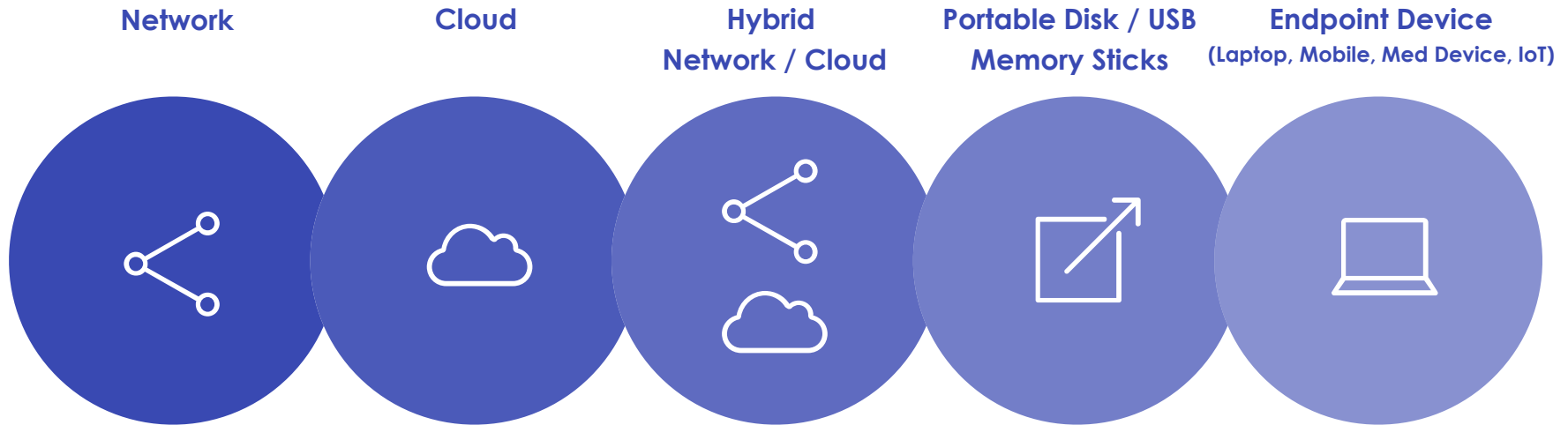
Look for HITRUST and similar healthcare industry certifications. Vendors should have in-house compliance expertise and follow CME programs.

**IF THEY HAVEN'T INVESTED IN UNDERSTANDING THE HEALTHCARE
INDUSTRY, DO NOT RISK WORKING WITH THEM!**

Finally: Sit back, And Relax

Once records are protected, with controlled and monitored access, records can be securely stored literally anywhere!

Confidently make use of storage on any network or device, with data revocation available at any time:



THANK YOU

Dr. Nameer Haider

Founder – Mice 360 Cybersecurity

E nameer@mice-360.com

C +1 202.731.2577

Mice 360

502 W. Broad St.

Falls Church, VA 22046

mice-360.com