VOLUME 2, ISSUE 3
January 2023

iNTERBiT Executive Briefing

THE MOST IMPORTANT STEP YOU CAN TAKE TO MAINTAIN PATIENT SAFETY DURING A CYBERATTACK? ENSURE THAT CLINICAL INFORMATION IS AVAILABLE AT THE POINT OF CARE.

More than ever before, hospitals find themselves in a state of "technical iatrogenesis." The greater the reliance on technological systems, the greater the impact when technology is not available. In a cyberattack, or even a threat on an attack, best practices suggest that you take down your entire network, and then your EMR is not available. It's the absolute worst-case scenario.

- IBM Security's Cost of a Data Breach Report 2022 indicates that the average cost of a data breach in healthcare is now more than $10MM – and the average time to identify and contain a data breach is 277 days.
- Cyber downtimes no longer are only an "IT problem". The American Hospital Association has labelled them as "threat to life crimes."

Solutions that you have relied on in the past may not be appropriate because every workflow has been disrupted.

THE IMPACT ON PEOPLE

Your IT and Security Department will take the necessary steps to lock down the entire network and will be trying to identify and limit the spread of malware.

Your CFO will be working with the insurance company to identify ways to pay the ransom through cryptocurrency and is talking with law enforcement, perhaps even the FBI.

Your CEO will be performing damage control, exploring legal options and perhaps talking with the media to ensure patients and families that care will continue.

Your Clinical team will be scrambling to care for their patients with whatever information is available to them.

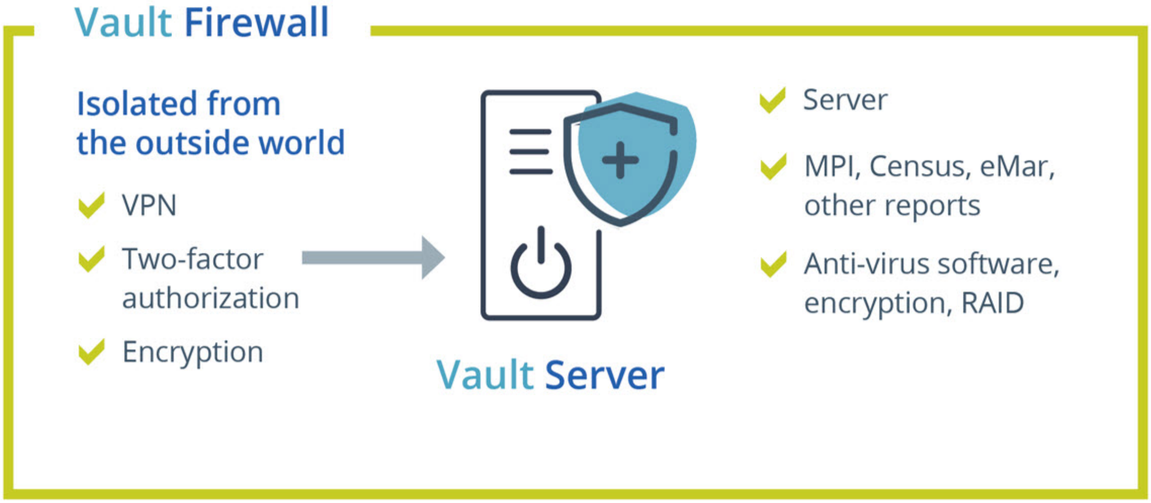
THE IMPACT ON PROCESS

- Your EMR vendor may say that a high availability snapshot of information is enough, but that solution frequently requires network or cloud availability. As a result, your clinical staff may be forced to document on paper, something that they are completely unfamiliar with and that may lead to unintended medical errors.
- You may be forced to turn away patients or even transfer patients which creates reputational loss as well as potential financial impact.
- Your doctors who see patients in clinics may be unable to access any information for those locations.

THE RIGHT TECHNOLOGY CAN LESSEN THESE IMPACTS

Technology is the set of solutions people use to implement processes. For example, your downtime software must be able to allow you to continue to access information from the EHR even if your Trusted Network is completely locked down.

The right technology should allow you to access this critical information on premises using a Zero Trust Network that is not impacted by a cyberattack. While this can be replicated in the cloud, it is of utmost importance that at least one instance is physically located within the hospital. This would be your "CyberVault", and it would be shielded behind a firewall as shown here in the schematic.


Vault Firewall
Isolated from the outside world
✓ VPN
✓ Two-factor authorization
✓ Encryption
Vault Server
✓ Server
✓ MPI, Census, eMar, other reports
✓ Anti-virus software, encryption, RAID

This location is where you send the critical information that you want to make sure is available during an extended downtime. This information might include:

Administrative	**Clinical**	**Financial**
• Personnel Roster • Physician Roster • Vendor List • Employee Contact List • Bed Transfers • Patient Census • All Forms • Policy and Procedures	• EMAR (E-Med Administration Record) • LAB Summary Report • MPI (Master Patient Index) • Outstanding Orders • KARDEX • Problems/Allergies/Meds/ Immunizations • Patient Census • OR Scheduling • Blood Bank	• Charge Capture Reports • Receivables Reports • Payables Reports • General Ledger reports • Cash Report • Consumption Reports

LET’S TALK ABOUT HOW TO MITIGATE RISK AND MAINTAIN PATIENT SAFETY

Cyberattacks will happen. Interbit Data provides solutions that enable our customers to continue to access critical patient and hospital data during any kind of downtime – an important component of cybersecurity risk management. We welcome the opportunity to speak with you to learn about your specific challenges.

Interbit Data
207 Union Street
South Natick, MA 01760
www.interbitdata.com | info@interbitdata.com

1.