rubrik

building cyber resilience

a healthcare leader's guide

Ransomware attacks show no signs of slowing down. Below are some key insights from cybersecurity experts on how to prepare for the worst and preserve patient care continuity.

before the compromise

Insights

You Must Begin Many organizations fail to make forward progress on cyber resilience because mutually dependent uncertainty results in analysis paralysis.

Organizations Are Surprised By What Doesn't Work Some organizations have been surprised by things they assumed would work, but didn't, like HVAC, doors, or other low-level automation.

Think Timeline and Priority, Not Importance Many organizations myopically focus on the EMR, and think that's their most important application. You might want to start elsewhere.

Many DR Plans Go Untested Because everyone works long days and then has upgrades and patching to do after hours, it's difficult to find time for DR drills, but testing is important.

Preparatory Steps

Accept Incomplete and Imperfect We learn by doing. When an organization moves with urgency ("if I only had one week, what would I do?"), they start building and learning.

Consider What Are Key Services in Light of Cyber vs. DR Context If during a cyber event the network is taken down, what needs to be considered regarding facilities automation, access, HVAC or pressure?

Think Beyond the EMR There are over 12 categories of capability in which you might want a subset of applications—such as communications, hours tracking, payroll, labs—beyond EMR.

Isolated Recovery Environments Are Isolated Testing recoveries into an Isolated Recovery Environment during business hours is feasible because the isolation prevents production impacts.

lateral movement

Insights

Your Data Estate Is a Blind Spot Monitoring within your data is a necessary measure to see when malware or remote access tools are introduced, providing advance warning.

Active Directory Is a Predictable Target Attackers will exploit misconfigurations and inappropriate delegation. Cached Domain Admin credentials are an easily sought item.

Predictably The Worst Timing The attackers will choose a time when they feel the fewest people are paying attention - Friday night, Saturday morning, eve of major holidays.

Preparatory Steps

Ensure Monitoring Is Integrated Ensuring alerts are seen is important. Confirm that all monitoring and security tooling is sending the appropriate alerts to the SIEM/SOC.

Monitor Your Data Layer Automated threat monitoring gives organizations warning if any known piece of malware or tooling is found in its data estate.

Be Prepared For A Shock Know how to recall people, know tools and connectivity will be impacted, and train for an overwhelmed feeling post-incident.

encryption event

Insights

Loss of Connectivity Almost all organizations sever themselves from the internet, and many shut down internal links in an effort to contain the spread.

Expect To Be Cutoff If You Do Still Have Connectivity Many organizations have experienced being cut off by their SaaS vendors out of "an abundance of caution." Even EMR vendors may cut you off.

Legal Complicates Recovery Some organizations have struggled to communicate with key vendors and 3rd parties due to legal concerns, and this has delayed recoveries.

Backup Data Is Frequently Compromised Despite universal claims of "immutability" 94% of cyber attacks feature a stab at backup data, and at least partially succeed around 73% of the time.

Preparatory Steps

Consider standby connectivity Even if imperfect, even bandwidth constrained, you'll want the ability to connect with key vendors in the immediate aftermath.

Expect It & Discuss It Work with your vendors. Discuss their standard operating procedures. Know their requirements around attestation.

Whitelist Key Vendors & 3rd Parties for Communication Do the slow thinking now so you can take fast action later. Whitelist with legal all the key vendors and 3rd parties you will need for a recovery.

Immutability Claims Should Be Questioned It's very hard to secure a data protection solution after 20 years of enhancements. Most architectures were not built to withstand attack.

contain

Insights

Time Lost When Initiating A Response Organizations may never have communicated with 3rd party Incident Response (IR). IR Teams may not know what tools the organization has.

Cyber Insurance Has Requirements Cyber insurers can require extensive documentation about the impacts and timeline of the event in order to calculate what they will pay out.

What Network Equipment Will You Trust? Some organizations are concerned about the usability of networking equipment in the immediate aftermath of an incident.

Preparatory Steps

Joint TableTops and Drills Drill together on the initiation and management of an incident. Insist parties meet, discuss what capabilities they have and will need, share information.

Document Everything Personnel not involved in the restoration effort should be identified and tasked with documenting what came back online at what times, and steps.

Sterile Network Equipment If you intend to not trust routers and switches, know where to obtain them and the design of the network you'll deploy.

respond

Insights

Successful Recovery Isn't About Fast Restoration of Data Many organizations waste the most time in a cycle of restoring data only to find out that it has malware in it. "Finding clean" can be a major delay.

Restores != Recovery Restoring files doesn't mean an application works. Effectively recovering applications requires knowledge about the app structure, testers, docs, etc.

Practitioners Need Access When you've recovered your datacenter, you'll still need to connect endpoints and practitioners to those applications, securely.

Preparatory Steps

Have A Threat Hunting Practice Know you are able to threat hunt for custom Hashes, YARA rules and file patterns within backup data without needing to perform any restores.

Develop Recovery Automation for Applications Deploy automation to reliably recover all the aspects of the application in the correct order, and schedule routine restores to ensure recoverability.

Alternative Networking & Access Have a plan to sanitize endpoints, carry traffic, and access applications recovered into the IRE, which roles require access and which can wait.

To download a full version of these insights and to watch the YouTube series, *Building Cyber Resilience: A Healthcare Leader's Guide,* visit youtube.com/@RubrikInc or scan the QR code. You can also visit rubrik.com/industries/healthcare to learn more.

rubrik