When a security breach is your disaster:

3 essential steps to protect your healthcare organization

cbts

Consult Build Transform Support

With all the malicious attacks and security breaches in the news these days, you can almost expect to be attacked—if you haven't been already. That's why so many hospitals, clinics, and private practices join forces with security vendors and managed services providers to fend off cybercriminals and keep their networks, infrastructure and data, protected and secure.

When you're dealing with patients' network-connected medical devices, doctors' and nurses' smartphones, third-party vendors' vulnerabilities, and countless other risks, it makes sense to hire outside experts to harden your cyber defenses. All those variables can be too much for IT teams that are already overworked.

This eBook from CBTS, leaders in data protection, including managed IT services and disaster recovery, explains the value in developing an incident-response program—preparing for breaches, identifying vulnerabilities, formulating a plan, and vetting your IT security vendor.

3 foundations of a robust security incident response program

Most of the time, without the basics put in place before a breach or attack, no security services vendor is going to be able to truly or quickly identify an apparent root cause (and what has been compromised) as there are simply not any bread crumbs to follow. So, in this case: an ounce of preparedness reduces the pound of discovery time.

Here are a few simple steps to have in place to help improve the time to recovery:

- Centralized event logs to start looking for traces of the intruder
- Thorough preparation that anticipates likely—and unlikely—points of attack
- An incident response plan that puts your preparations to work identifying malware and intrusion points, and determines whether to bring in law enforcement

Part 1: Centralized event logs

Event logs reveal almost everything about your intruders. The trouble is, you have hundreds or maybe thousands of apps and devices logging every bit and byte they encounter. In a 24x7x365 environment like a hospital, logs soon amass oceans of data.

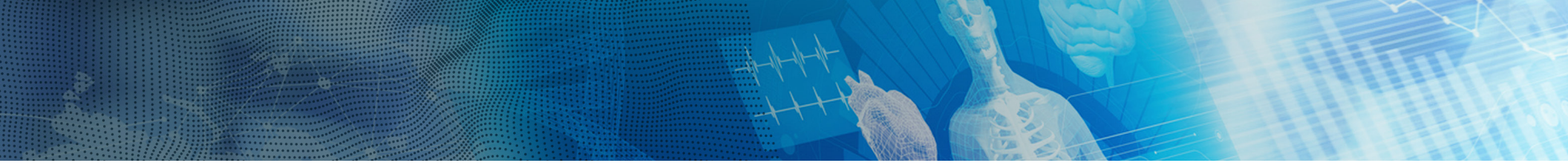
Creating a central logging location gives your security partner access to all of your logs. That's an excellent start, but keep in mind that not all logs store equal value. To save time and find an intruder sooner, your security partner must be able to separate the gold from the garbage.

So, you want to segregate logs by type, and answer questions like:

- Which logs and alerts require the most attention, and which ones are less important?
- Which logs should be saved the longest, perhaps even forever? You can't afford to delete your most important logs too soon, because malware can remain dormant for weeks or months before an intruder executes it.

Event logs help you and your security partner quickly track down the root cause of an intrusion so you can discover, diagnose, and defend yourself within the first 48 hours, before things spin out of control.

You don't want your security provider wasting precious hours tracking down logs in far-flung locations. Centralizing logs and establishing which ones matter the most can prevent these delays.



Watch out for soft spots and backdoors

Locking down your most critical patients' personal identifying information (PII) is mandatory. But hackers typically have enough sense to avoid a frontal assault on your most well-protected data. Instead, they want to sneak in through unguarded backdoors and soft spots in your cyber defenses.

Intrusion-detection technology looks for anomalies, so cybercriminals avoid anomalous behavior once they get inside your networks. Thus, you need to approach healthcare security from a "blind spot" perspective—identifying the lower-level vulnerabilities of authenticated users.

Rather than resort to brute-force intrusions, cybercriminals are more likely to:

- Sneak in and figure out how to compromise the access levels in your authentication controls.
- Gain entry-level access and work their way up to each successive level of access.
- Use spear-phishing to gain an employee's login credentials and exploit a trusted user account, then turn off alerts or subvert them in some other way.

Your cyber defense partner can help you identify these kinds of vulnerabilities and implement controls that reduce your risk of exposure.

Part 2: Thorough preparations with your security partner

It might happen like this: Somebody steals the laptop of one of your patients, who logs into your system to track health data and appointments. The thieves sell his log-in credentials to cybercriminals who use them to find a backdoor into your network via an obscure exploit somebody forgot to patch.

Hackers take care not to draw any attention to themselves, so intrusion-detection software doesn't always notice their behavior. Over the course of months, they navigate around the back corners of your networks, snooping for ways to upgrade access, turn off alarms, and exfiltrate lucrative patient data.

In a moment of carelessness, they reveal their presence. Now, you have to stop them as soon as possible, limit their ability to inflict damage, find out how much damage they've done, and create mechanisms to prevent further breaches.

And you want all this in the next 30 minutes, if not sooner.

At this point, preparation can shave hours off your response time. If you and your security partner have worked out a plan anticipating a breach, you can jump into action almost immediately. If you haven't prepared, you can lose hours your adversaries can spend exfiltrating private data.

Preparing for a breach forces you to answer questions such as:

- Have you conferred with your legal department to ensure compliance?
- Do you have cyber risk and liability insurance, and does it provide the coverage you need? (Some policies have so many exclusions that you might never be able to collect on a claim.)
- Have you consulted with your security partner to make sure both of you are adequately equipped to defend a cyberattack together?

During the preparation phase, your security partner should identify and recommend what you must have in place to enable a rapid response to your concerns. This means your partner has inspected your networks for vulnerabilities, flagged unpatched software, reviewed your authentication processes, and suggested ways to harden your network.

All this prep work culminates in a plan outlining your security response program.

People, processes, and technology: It takes all three

You must remember that technology alone will not make your healthcare applications more secure. Fighting cybercriminals requires a three-point strategy addressing people, processes, and technologies.

Start with processes: Build sound cyber-hygiene programs requiring strong passwords that must be changed frequently. Implement two-factor authentication where it's appropriate. Make sure authentication policies limit access only to people who absolutely need it. Plug any gaps in application-to-application communications.

Weigh technology complexity: You may be dealing with so many applications, devices, and users that you feel overwhelmed. And complex cyber-defense technologies may require more expertise than you have available. You could get so many alerts and warnings that you can't tell which are important and which aren't. That's when it pays to work with an experienced security expert.

Address human limitations: It takes just one human slip-up to infect your systems. It could be a nurse's aide or the chief of cardiology. A supplier could get hacked, inviting cybercriminals into your systems.

Ultimately, people are your greatest asset and your biggest security threat. If you train them well and insist on proper cyber defense processes, you'll do much more than any tool or process can achieve. People must work together to address common threats—that includes you and your cyber defense partner.

Part 3: Security incident response plan

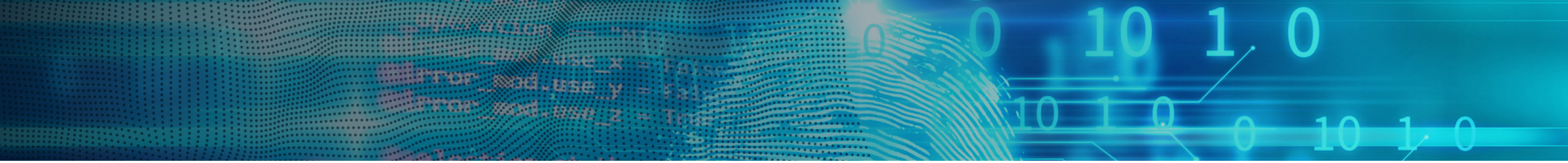
Your preparations will find a home in your security incident response plan. This document will give you and your security partner a roadmap for springing into action at the first sign of a breach.

Your response plan should include:

- **Your partner's damage-assessment process.** Your security partner must be free to figure out how much damage has been done as quickly as possible. Nailing down the damage assessment process early helps you formulate the most effective response.
- **Defense priorities.** Your partner must be able to diagnose the severity of the threat. Some breaches may need to be shut down regardless of the cost, while others might be relatively benign.
- **Root-cause analysis.** Your partner needs to identify entry points, search for evidence of malware, and identify the "patient zero" who allowed the breach.
- **Mitigation tactics.** When you understand why the breach happened and how it is spreading, you start reducing harm by shutting out the hackers and figuring out how to prevent them from coming back.
- **Law-enforcement protocol.** Breaches may be serious enough to warrant contacting the FBI or other authorities. Make sure your plan spells out who contacts the authorities—and under what conditions.

It's best to create a detailed plan that lists all the steps for flagging a breach, limiting damage, and keeping vital business systems running.

If a breach seems like a certainty these days, then having a security incident response plan can help you and your partner be certain you'll be ready when it happens.



How to vet your security partner

Many companies provide managed security services. They may have certified security experts well-schooled in the art of thwarting cybercriminals and hardening networks. They could have an impressive list of name-brand clients.

But what you really need to keep your healthcare network secure is a partner who will take the time to fully understand your patients, specialties, and business models.

Your partner should be able to:

- Spell out exactly how they will help you respond to a security incident. They should be able to show you documented standard operating procedures.
- Review your network environment at the beginning of the service engagement.
- Document how they will respond to a breach in your systems.
- Recommend how you can help them speed up response times.
- Clarify the conditions when a breach is considered a disaster that requires the implementation of a disaster-response program.

Remember that every delay on your end creates further delays on your security partner's end. Most likely, you'll be billed for that time.

At CBTS, we have the professionals on staff to ensure your healthcare facility's networks are secure and difficult to breach. Our experts can help you create a security incident response plan that can speed up your response to a breach and reduce the likelihood of a damaging data loss.

About CBTS

CBTS is a wholly owned subsidiary of Cincinnati Bell (NYSE:CBB) that serves enterprise and midmarket clients in all industries across the United States and Canada. From Unified Communications to Cloud Services and beyond, CBTS combines deep technical expertise with a full suite of flexible technology solutions that drive business outcomes, improve operational efficiency, mitigate risk, and reduce costs for its clients.

Contact us today at cbts.com