The Last Watchdog
on Privacy & Security
by Byron V. Acohido



GUEST ESSAY: 6 steps any healthcare organization can take to help mitigate inevitable cyber attacks



By Don Boian

The headlines are disturbing: *Breach of patient records*; *Surgeries and appointments cancelled due to IT outage*; and even, *Death attributed to ransomware attack on hospital*.

Related: *High-profile healthcare hacks in 2021*

The risks are real, and the impact of cybersecurity events continues to grow.



A cyber catastrophe may seem inevitable, but there are basic practices and actionable steps any healthcare organization can take to begin reducing the clear and present risk of being impacted by a cybersecurity event.

Note that I say, "reduce your risk," not eliminate it. While some product and sales professionals may try to convince you they can eradicate the chance your data will be breached or systems infected with malware, that's unfortunately too optimistic and short-sighted given today's threat landscape.

However, all is not lost if your healthcare organization is starting its cybersecurity journey, or even if you have a mature cybersecurity program. Focusing on or revisiting these six cybersecurity basics will help reduce your risks and strengthen your defense.

•**Evaluate data inventory.** Start by assessing what critical information your organization needs to protect and maintain access to in order to provide services. A data inventory allows you to focus the greatest security (and monitoring) where it needs to be.

Healthcare organizations often single out Personal Identifiable Information (PII) and Protected Health Information (PHI). Those data categories are necessary to protect but most likely not sufficient to keep your organization running smoothly in the event of an outage or cybersecurity crisis.

What additional business information is critical? Billing? Scheduling? This inventory will vary based on your business model and function. Failing to have a valid data inventory means every database and system becomes critical to your organization's resiliency and defense. That can be costly and ineffective.



Boian

•**Create an asset inventory.** Financial professionals are usually first to want to track capital equipment – after all, it's an organization's primary investment. Knowing what Information Technology (IT) hardware exists is a good place to start (servers, laptops, desktops, tablets, etc.).

An accurate asset inventory gives you the ability to identify items that may need updating, including operating systems, application versions, or patches. Timeliness in closing these holes can reduce your exposure.

•**Map data**. It's critical to know where data is stored and processed. Once your data and asset inventories are complete, it's important to map flows and storage locations for your data.

This data map should also include exchanges of information with third parties or service providers, including cloud services. Maps like this can also improve processes and limit exposure (Why are we still sending 'that' data to the vendor whose contract is terminated?).

•**Educate employees**. Many security programs focus on employee education (creating a strong password, being aware of phishing, etc.). Your employees can be your first line of defense or your weakest link.

Make any digital training personal and relevant to employees by providing programs about how to protect themselves and their families. Increasing security savvy at home can motivate employees to go further to protect your organization's network and the customer information on it.

In healthcare, it's a wise investment because more professionals are working remotely. In addition, make it easy to report security concerns (phishing, data leaks, social engineering, password compromise, etc.).

•**Develop plans and playbooks**. Codify procedures and processes. As your program matures, implement automation for those playbooks or plans that are a part of your response protocols. Today's threat environment dictates that mitigating an event quickly will significantly limit the damage and scope of the crisis.

One example of this is isolating or quarantining systems with malware (virus or ransomware) from the remainder of the network.

Some of these playbooks can be deeply technical, but don't forget to handle the administrative portions of crisis response: Who in your organization needs to be informed of a breach? What federal, state, or local laws demand actions be taken? At what point do you need to involve a legal team or your board?



•**Practice to improve response**. Playbooks, plans, and processes are wonderful, but the experiential learning of rehearsing what happens during an event will dramatically improve the efficacy of your plans. There is a reason organizations like the U.S. military exercise their plans often – it builds human muscle memory and increases comfort and resiliency in the people working through these crises.

These six areas will help improve your security program. Be brilliant at these basics, but don't stop there. Remember to implement and enforce these suggestions with the traditional Information Security principles we all need to remain secure: good access control (passwords, multifactor authentication, least privilege rights), patch management, frequent backups, and audit logs. After all, the process of security involves never-ending learning and improvement. As technology and threats evolve, so must the security organization.

About the author: *Don Boian is the Chief Information Security Officer at Hound Labs, Inc., which supplies ultra-sensitive, portable marijuana breathalyzer technology. He worked at the National Security Agency for 30 years on defensive and offensive cyber operations, and most recently served as CISO for a large regional bank.*

February 21st, 2022 | For technologists | Guest Blog Post | Privacy | Top Stories

The Last Watchdog © 2024
Privacy Policy | Terms of Use