Hospital Network Security Requirements: 5 Steps Beyond Compliance

"You can be 100 percent compliant and still be insecure. Shooting for compliance only is like shooting for a D grade in class."

Christopher Frenz
Director of Infrastructure
Interfaith Medical Center

Hospitals have long known the importance of protecting against cyberthreats, but the WannaCry ransomware attack from March 2017 reinforced how essential it is to have a comprehensive cybersecurity solution. This attack affected organizations in more than 150 countries, with healthcare being the most severely affected industry. "It was the first time a ransomware attack didn't just affect the PCs, it encrypted medical devices, too, which created a threat to patient safety," said Christopher Frenz, Director of Infrastructure at Interfaith Medical Center, a 287-bed hospital in Brooklyn, New York.

The attack came through email, which is notoriously difficult to defend against because it means either altering human behavior or filtering how your organization handles communication. "If you look at phishing stats, malicious links have a 13 percent click-through rate," Frenz pointed out. "That means if a hacker sends a malicious email to just 10 of your employees, there is a greater than 90 percent chance that someone in your organization will click."

Hospitals understand they must comply with privacy requirements, but Frenz considers HIPAA and PCI the bare minimum. "You can be 100 percent compliant and still be insecure. Shooting for compliance only is like shooting for a D grade in class," he said.

To boost your cybersecurity grade, you need to follow these five steps.

1. Know what's on your network.

Take inventory of your network, including every device, from computers to HVAC equipment to medical equipment to door locks. Also, know what data your systems house. "Hospitals often have data they are unaware of, especially with the cloud. For example, you might find your finance department is uploading data and you don't even know. Go around and identify everything," Frenz said.

2. Identify the flow of data.

"Identify how data flows into and out of those systems and between those systems," Frenz said. It is essential that you know how the data is supposed to flow if you are going to write rules about it. Plus, if you have a good idea about what data is supposed to be going across the network, it's much easier to spot something that should not be there. Would you know if something was out of place? "Map it out and learn," he advised.

Produced in partnership with
HIMSS Media

"The more layers of security you have, the more effective you will be."

Christopher Frenz

3. Segment your network.

"Ideally, you should push for a zero-trust model," Frenz said. Zero trust restricts lateral movement along a network. Essentially, it means that no two systems trust each other or can talk to each other, unless you have written a rule that they can. "We use ExtremeControl network access control, a product that allows us to apply a set of policies that control what each device plugged into network can or can't communicate with," he said. For example, a doctor can view and print medical records, or look at imaging scans, but her computer or tablet cannot communicate with devices on the network other than that. That way, if her device becomes infected, the virus won't be able to spread. It takes time and focus to build a zero-trust solution, especially when you are dealing with thousands of devices. But with each device that you add, it offers that much more protection from lateral movement.

4. Build as many layers of security as you can.

"The more layers of security you have, the more effective you will be," Frenz said. Organizations need technology-based layers as well as layers that deal with human behavior, such as awareness training for employees about phishing. Layers may include a spam filter to try to catch the malicious email, user training to try to prevent them from clicking, web filters that don't allow the link to work if a person clicks it, anti-virus software on the computer, and then if all that fails, network segmentation to contain the threat. In an anti-ransomware guide,[1] which he co-authored, Frenz identified more than 40 layers of security organizations should consider.

5. Have an instant response plan.

If your organization is compromised, you should know ahead of time how you would deal with it and contain it as quickly as possible. One way to prepare is to conduct simulated incidents. There are a few different ways you could do this, including launching a faux-phishing campaign against employees, or trying a simulated malware outbreak using an EICAR string test. This is a harmless string that anti-virus software treats as a virus, and should detect, Frenz explained. "Put your defenses to the test: Launch an incident and see how staff responds."

[1] Christopher M. Frenz and Christian Diaz. Anti-Ransomware Guide. Open Web Application Security Project. September 12, 2017. https://www.owasp.org/images/c/ca/Anti-RansomwareGuidev1-6.pdf