The Importance of Cybersecurity Training for HTM Professionals

Axel Wirth

The cybersecurity posture of our medical device ecosystem is a growing concern. At the same time, we are painfully aware that today’s cyberthreats are increasingly sophisticated and attacks are highly targeted and purposeful.

In a world where cybercriminals are reinvesting 40% of their profits into developing new techniques, the gap between what we know about medical device vulnerabilities and the attackers’ capabilities is growing rapidly. Yet, at the same time, medical devices are not as easy to secure (or upgrade to a more secure state) compared with traditional information technology (IT) equipment; in fact, one might even argue that the traditional security paradigms we have developed for IT cannot be applied directly to the medical device space.

Certain issues lie in the nature of the problem—no doubt, it is more difficult to implement iron-clad security with always-on, high-reliability, life-sustaining systems. Traditional security approaches, which rely on a combination of antivirus and patching, are not feasible or practical. (One could argue that with today’s sophisticated threats, this approach is doubtful even in the traditional IT space; however, this topic is beyond the scope of the current article.) Even though alternative security technologies exist for embedded systems and Internet of Things–like devices, they are not (yet) widely adopted in the medical device industry. Further, today’s complex security challenges cannot be solved by technology alone.

Reliable processes, careful handling, and security-aware users are equally important. And that means that in this day and age, anybody who uses any network-connected device, whether at home, at work, or in your hospital’s clinical engineering department, needs to have a fundamental understanding of cybersecurity. Consequently, security training for biomedical engineers is a must, and not only because HIPAA (Health Insurance Portability and Accountability Act) requires it [§164.308(a)(5)(i), “Security Awareness and Training”]. Because biomedical engineers make daily decisions that affect cybersecurity—from specifying new equipment, connecting it to the network, and maintaining its security posture, to the device’s end of life (EOL)—they need to be cognizant of how those decisions affect device security and ultimately patient safety.
Here are several examples on how human behavior can pose a security risk to medical devices:

- A device returning from repair is connected to the network without assessing whether it may have been infected with malware while it was out.
- A third-party service technician provides a software upgrade via a USB thumb drive of unknown provenance; it may previously have been used at other hospitals, airports, coffee shops, hotels, etc. and may contain malware.
- Clinical staff connect their personal smartphone to a device's USB port to recharge it.
- Clinical staff use a digital X-ray system's QC workstation to browse the web or check their personal email.
- Devices are EOL and discarded (and potentially resold or donated) without removing protected health information or enterprise network credentials.

Although technical controls could be applied to address these specific risks, human creativity beats technology many times over. In other words, while technical controls are available and necessary, we can’t possibly anticipate and plug all holes.

To make matters worse, we are facing a serious and global shortage of cybersecurity skills. It is estimated that the current global job market for cybersecurity professionals has more than 1 million openings—and rising.

One way for organizations to offset at least part of the problem is to train other technical professionals in cybersecurity. Although dedicated experts remain sorely needed, by training their colleagues, we can distribute the workload more effectively and better prevent security crises from occurring.

Cybersecurity training for HTM professionals also builds bridges, allowing them to speak the same language as their IT peers. It can help overcome some of the traditional disconnects and differences in objectives between the two departments. (Of course, one could make the reciprocal argument that health IT professionals should also receive basic biomedical engineering training to help enhance their understanding.) In short, training also enhances communication, planning, and decision making.

In my job, I have the privilege of working with many healthcare organizations and device manufacturers. Many have built top security programs that very effectively minimize their risks and exposure. However, too many are still treating security as a secondary operational function with no clear value to the business.

The case for security training of HTM professionals also applies to medical device manufacturers. These companies have brilliant engineers who design highly reliable, safe, and effective devices that are saving countless lives, but I often find that their security awareness is not in line with today’s threat landscape and risks—both from a technical perspective and in relation to the business case for better security. But change is happening.

The sidebar (next page) sketches out the key attributes of a cybersecurity training program for HTM professionals. This outline is a work in progress, and I welcome input from organizations that have already implemented, or are in the process of implementing, such training. Using this outline as a starting point, we can begin the process of achieving consensus on industry best practice.

**Summary**

As cybercrime has become a business conducted by professional gangs and one can now hire hackers or attack services, buy any type of data, or order custom malware, we need to prepare our businesses and our infrastructure so that we can safely and securely operate in an increasingly hostile environment.

We cannot delegate cybersecurity responsibility to a few specialists in our organization who “take care of it.” Cybersecurity has to
Current-day cybersecurity is not a tactical function buried somewhere in IT; it is a strategic business responsibility to enable an organization to be as secure as it can be.

Cybersecurity training is one of the critical components of that responsibility. Depending on their role, all employees need to be trained appropriately: clinical users so they don’t compromise devices and are able to detect unusual behavior, biomedical engineers so they can make the right technical decisions, and management so that the business supports security on a strategic level.

References
