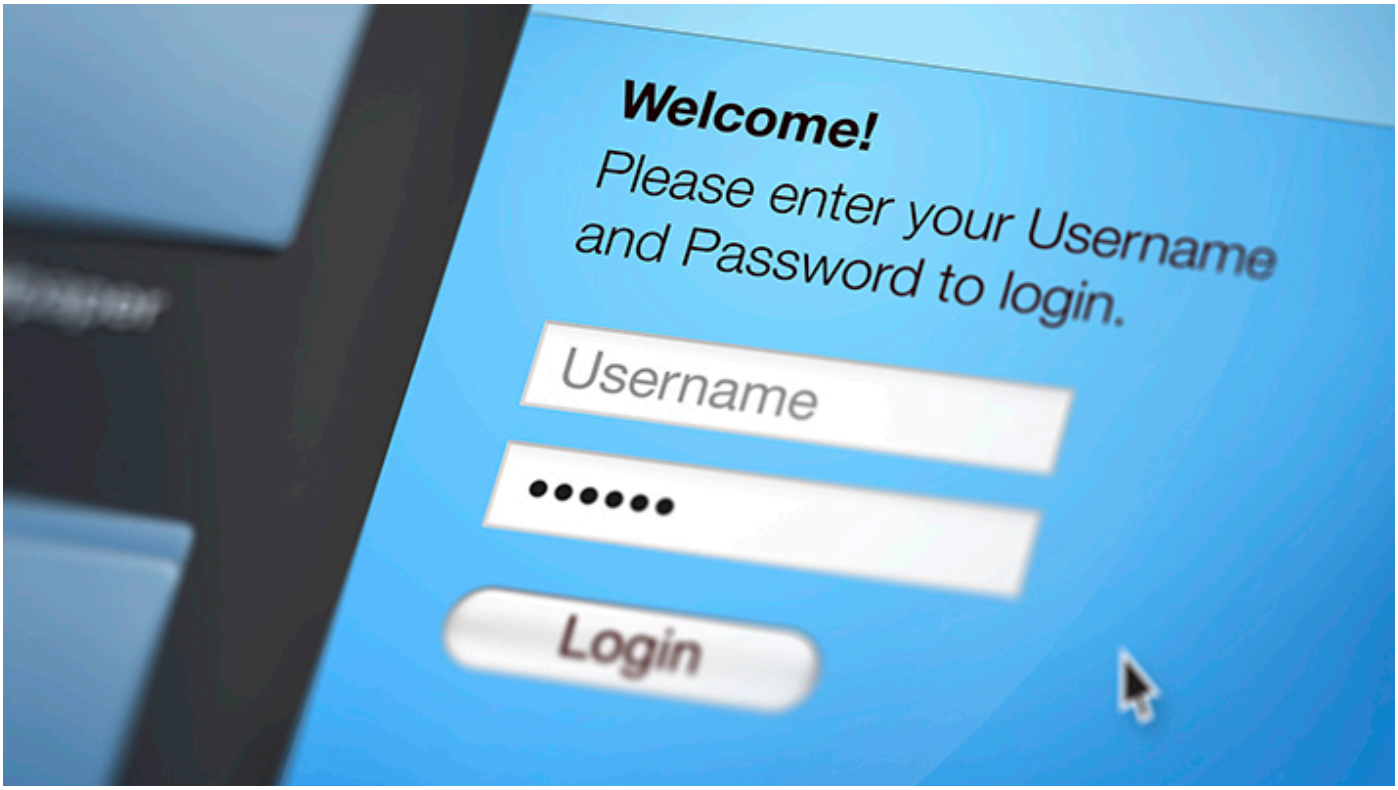
Cybersecurity: Nightmare scenarios and guiding principles

From legacy infrastructure to potential medical device hacks, some of the industry's leading voices opened up about how the industry can begin to combat the inevitable breach.



Some clinicians share their passwords with nurses in order to complete charts with the idea of "a care efficiency: rather than a risk.

Some clinicians share their passwords with nurses in order to complete charts with the idea of "a care efficiency: rather than a risk.

By now, the healthcare sector is fully aware of the looming target placed on its back by hackers. The issue is that legacy infrastructure, staffing shortages and

insider threats can make it tough to tackle these issues.

The biggest threats lie within the legacy infrastructure of healthcare itself. This includes medical devices operating on outdated platforms, along with IoT devices. We have not have seen it happen frequently but, if those devices are hacked cybercriminals can actually put patient lives at risk.

Threats to patient safety

Potential attacks on basic infrastructure like life support are equally troubling. That's a view shared by others during Thursday's #HITsecurity tweetchat ahead of the HIMSS Healthcare Security Forum.

"That's the thing about healthcare and healthcare security - when your imagination runs wild with the possible attacks people die," said Nick van Terheyden, MD, founder and CEO of Incremental Healthcare.

> T1 That's the thing about Healthcare and #HITSecurity - when your imagination runs wild with the possible attacks people die
>
> — Nick van Terheyden, MD (@drnic1) May 10, 2018

But security risks go beyond a breach. In healthcare, when a hacker gets in it often interrupts patient care, throws clinicians back to pencil and paper and downtime can last for weeks.

Consider the WannaCry attack that crippled the U.K. National Health Service last year.

Hackers are hitting EHR vendors, as well, which impacts providers operating on the impacted platforms. Allscripts was hit earlier this year, and some of its providers were unable to access patient records for up to a week.

"Breaches are always a concern, but lack of access to data and extended downtime with no access to records has huge impacts for revenue, patient care and community trust," said Max Stroud, lead consultant with Galen Healthcare Solutions.

For some, the crux of security issues lies with the users. Often seen as the biggest threat, "user threats have the potential to cause significant losses and evade detection."

Indeed, insider threats have been the biggest vulnerability to healthcare security for more than a year. Verizon's April breach report found insider threats and human error were the biggest risks to security. In fact, healthcare is the only industry where insider threats outnumber outside threat actors.

Incremental steps and human-centric design

What can be done given the attack surface and seeming inevitability of a breach?

"A viewpoint has emerged in the last few years that organizations should just assume they are going to be compromised, so they should focus their efforts on detection and response for when an attack inevitably happens," said a spokesperson from health IT firm Cognosante.

Detection and response, however, only comprise half the equation: "It's a huge mistake to back off on preventive controls like strong access control, web application security, adaptive firewalls and user awareness training."

Several experts said security needs to be designed with the user in mind. According to Stroud, she's seen doctors share their passwords with nurses in order to complete charts, as it's seen as "a care efficiency and not a risk."

Even worse, Stroud said, “I've also seen EHRs delivered with standard admin logins. It's not pretty out there.”

“Human-centered design should account for human-centered tendencies,” said Geeta Nayyar, MD, Femwell Group Health’s chief healthcare and innovation officer. “Understanding how we can help our folks develop an internal motivation to actively embrace the role of our first line of defense.”

To get there, organizations need to build a culture of compliance, explained attorney David Harlow, principal at the Harlow Group. “It's all about human factors. Technical solutions need to be implemented by people, and they have to want to do the right thing.”

With that in mind, organizations need to make it nearly impossible to do the wrong thing, Harlow added. “Very important to reduce exposure, reduce public face, limit internal access on role-based need-to-know basis.”

Organizations should also conduct pen testing and bug bounty programs on the regular to make sure they’re not susceptible to attacks.

“You can try to predict the future, or you can just continually review and improve your systems, processes, personnel, training, etc. including doing new risk assessments as changes are made,” said Harlow.

“We plan for what we can plan for - but there are many unknowns in this business,” said Nayyar. “Keep solid post-event contingency and crisis plans current.”

Experts will address these and other pressing cybersecurity topics at the HIMSS Healthcare Security Forum in San Francisco June 11-12.

Twitter: @JessieFDavis
Email the writer: jessica.davis@himssmedia.com