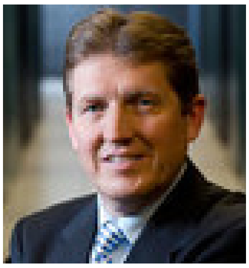
A HIMSS ASIA PACIFIC EXCLUSIVE ARTICLE

SECURITY ESSENTIALS

Theresa Z. Meadows and Karl J. West tell all.



Theresa Z. Meadows, MS, RN, CHCIO, FHIMSS, FACHE, Senior Vice President & Chief Information Officer, Cook Children's Health Care System, USA

Karl J. West, Chief Information Security Officer and Assistant Vice President, Information Systems, Intermountain Healthcare, USA

Healthcare is one of the most vulnerable industries to cybercrime yet one of the least prepared for it. Why is progress so slow relative to other industries?

KW: Healthcare's vulnerability to cybercrime is much higher than other industries; yet, it's one of the least prepared to deal with cyber events. In general this vulnerability is related to healthcare's Primary mission which is delivery of care and treatment above all else. As we in Healthcare move beyond basic delivery of care, we focus on patient safety and lowest appropriate cost for care. Reducing cost is a National focus that pres. Obama spoke on and shaped the affordable care act around. Further, 80% of healthcare is comprised of small clinics and hospitals. It's extremely difficult for small clinics and hospitals to devote the resources (people and money) to cybersecurity measures. That's why cybersecurity needs to become a community and National effort.

What are three common challenges for clinicians/C-suites in securing medical information? What is one piece of security advice you have for them?

TM: One of the most common challenges with clinicians/C-suite member is the belief that appropriate security will slow down their productivity. There have been many advances in technology (e.g. single sign-on) that have allowed strong security around medical information but also enhanced clinician productivity. The second challenge is the belief that with appropriate security in place, it will limit the amount of medical information the clinician will have access to which will impact patient care. This is no longer true with the sophistication that has been built into role based access systems. The last challenge is creating a Culture of Security that begins with the C-Suite and Board Members. A great program starts with ownership and buy-in at the highest levels of the organization for good security practices and ongoing education about security. Without this type of commitment most security programs will not be successful. One piece of security advice that I would provide clinicians/C-Suite members is that security is a patient safety issue. It is important that we all understand the security risks to our patients and how to prevent issues from occurring. This approach creates awareness and patient context for the clinicians so if an issue occurs they know how to react.

How can team-based care help to achieve security? Can you share three ways?

TM: First, team-based care can help achieve security by understanding that patient is the reason why strong security is important. In team-based care the patient is the center of the team. If the team sees good security hygiene as part of keeping the patient safe, that is step one. With team-based care the entire team is responsible for security which promotes a culture where all team members are aware and monitoring for potential security issues. Lastly, team-based care can promote a culture of reporting potential issues early, so that mitigation plans can be created when issues arise much like the plan of care created for the patient.

KW: Cybersecurity must be about people. That means that in a team-based care model, caregivers must understand that data is an extension of the patient and therefore needs to be handled securely. Physicians need to be trained to appreciate the trust that is placed in them extends to the use and protection of very personal information they share with care givers. Organizations must promote a culture of cybersecurity and expect users of their systems and networks to practice good cyber hygiene and not put those resources in additional risk. Finally, a culture of, if you see something, say something needs to be part of the Cyber strategy. Someone on the team always knows when errors occur.

HIMSS CHIME
INTERNATIONAL

Theresa and Karl are two of the workshop leaders for the **Cybersecurity Essentials for Healthcare Executives Workshop** on 11 September (pre-conference day) at HIMSS AsiaPac17. Attend to learn about:

1. Opportunities to incorporate cybersecurity awareness and risk management into the fabric of an organization and the employee mindset.
2. Engaging stakeholders to secure needed resources and funding to support the plan.
3. Identifying key steps in preparing an organization against cybersecurity threats and breaches including security frameworks and control measures.
4. Defining key components of an effective cybersecurity plan including prevention, response and recovery approaches for successful implementation and staff adoption

See you there!