Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

Patient Safety Depends on Cyber Safety

October 1, 2019

As industry chair of the Health Sector Coordinating Council's Joint Cybersecurity Working Group, I am pleased to kick-off October's National Cyber Security Awareness Month for the Health Sector. This annual series of events is observed by official proclamation from the President of the United States and 50 governors, and by initiatives and activities that emphasize the importance of cybersecurity in our personal lives, our business operations, and government services.

Much like the patients we treat, the health sector is prone to illness.

Unlike humans, who can suffer from bacterial, viral, and parasitic blights, our ailments consist of cyber viruses and self-propagating worms, infectious ransomware, and seemingly endless vulnerabilities that plague our systems and networks. Scourges like these are used by cybercriminals who seek to steal our data for their own economic benefit, hacktivists who wish to deny us the ability to operate normal business functions as part of personal or political vendettas, well-funded and organized nation states that hunt our intellectual property for the benefit of their indigenous industries, and insiders who leak data either intentionally with malice, unintentionally due to a lack of cyber-awareness, or as a targeted attack vector in a larger campaign.

It's for these reasons that health organizations have been investing enormous amounts of capital into creating resilient and robust security operations centers and cybersecurity programs throughout our country. In recent years the healthcare sector has become one of the most attacked industries in the nation, with some organizations being infected daily or weekly by attackers. As a result, cybersecurity and patient safety are no longer mutually exclusive topics. When these infections occur, and if we are unfortunate enough to be subject to one, it is not just the shareholders, partners, and product or system owners who feel the burden. Ultimately, it's the patients who will suffer. The stoppage of our ability to manufacture lifesaving medications, network outages that hinder a healthcare provider's ability to treat patients, and vulnerabilities in key systems such as clinical or diagnostic equipment can all have grave consequences for the sector and patients that we serve.

As a critical infrastructure, the health sector is deemed so vital to the United States that our incapacitation or destruction would have devastating effects on national public health or safety.

Because of this, a comprehensive cybersecurity posture is paramount when considering the treatment of patients. Accordingly, the Health Sector Coordinating Council, the public-private partnership of industry and government health sector stakeholders, is working diligently to identify and mitigate the cyber threats we face through collective action and best practices to strengthen our systems, data security and workforce expertise.

While we need to have national cyber security awareness every day and all year, this is a time for us to take stock of and redouble our efforts toward the sector-wide mission of health industry cybersecurity. This is our responsibility; get involved!

After all, patient safety depends on cyber safety.

Terry Rice, Chair, Health Sector Coordinating Council Cybersecurity Working Group;
Vice President of IT Risk Management & Security and Chief Information Security Officer, Merck