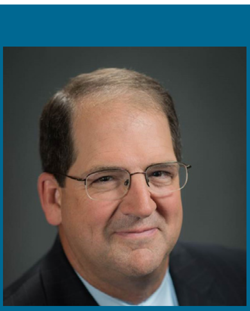
A HIMSS ASIA PACIFIC EXCLUSIVE ARTICLE

# Maximizing BOTH IT and Cybersecurity: Is It Possible?

Brought to you by:

HIMSS CHIME INTERNATIONAL



Russell P. Branzell, FCHIME, CHCIO
President and CEO, CHIME

## The recent "WannaCry" ransomware attacked software in at least 150 countries. What does this mean for the future of cybersecurity?

**RB:** One day we may look back at WannaCry as our Waterloo. **Although one-off security breaches have become a too-common occurrence in healthcare systems, the breadth of the WannaCry attacks and the disruptions it caused catapulted awareness of the threat among the public and the healthcare community.** The WannaCry episode already has prompted hospitals to review their cyber defense systems in an effort to ensure reasonable protections. This should translate into more robust cybersecurity systems in the future.

But it is a mistake to think of cybersecurity as merely a technological fix. It is people who make cybersecurity robust. In the two weeks after WannaCry struck, 26 new members joined the Association for Executives in Healthcare Information Security (AEHIS). This is a group under CHIME for senior IT leaders. WannaCry has elevated the need for CIOs, CISOs and other IT professionals who have not only the technical skills but also the leadership skills to protect healthcare systems and their patients in an increasingly threatened world. Successfully defeating the WannaCries of the future will require this kind of IT leadership.

## How can healthcare computer users protect themselves in this era of rampant (and massive-scale) cyberattacks?

**RB:** In the context of healthcare systems, awareness of the threats and how to mitigate against them should be ingrained in the culture. With that in mind:

1. **Don't think of protection in terms of a training exercise that gets checked off a to-do list** but rather as commonly understood behavior practiced by everyone. Training should be a continuous process.
2. **Update.** A patch is useless unless applied.
3. **Verify before opening a link or file.** It is estimated that more than half of security incidents involve staff.

## What makes the healthcare industry different from all others when it comes to cybersecurity?

**RB:** The difference can be in terms of challenges, level of vulnerability and/or infrastructure needs.

For one, cyber criminals are highly motivated to hack into medical records because patient health information is a valuable commodity on the black market. **A stolen medical record is worth 10 times more than a stolen credit card number.** That makes the healthcare industry an attractive target for criminals.

As healthcare IT becomes increasingly prevalent and complex, it also potentially becomes more vulnerable to cyberattacks. We have evolved from paper to electronic systems with servers and networks, and we are now entering an era of mobile devices and virtual systems. These technologies have the potential to improve healthcare on a global scale, but they entail securing a more dynamic environment.

I visited a remote village on a mountaintop in Nicaragua that had no running water; but it had cell phone reception with a strong signal. It was part of a nationwide initiative to make Nicaragua wireless, allowing the country to leapfrog costly telecommunication systems such as cable. Villagers needing a consult with a physician could conduct it over a cell phone. The challenge for the healthcare industry will be maximizing IT to improve patients' lives everywhere while keeping them safe from cybersecurity threats.

**In addition, while CIOs recognize the threat, historically their CEOs have not made IT or IT security a priority.** IT ranked at the bottom of the list of importance among CEOs in an annual survey by the American College of Healthcare Executives for the last five years. Six years ago, it didn't even make the list. In reality, IT is integrated in every aspect of modern healthcare.

The Health Care Industry Cybersecurity Task Force, which was co-chaired by CHIME member and Cook's Health Care System CIO Theresa Meadows, released a report in June that detailed how healthcare has lagged other industries on cybersecurity. The report offered more than 100 recommendations, including federal incentives to invest in cybersecurity. This and similar efforts will help give CIOs the resources they need.

## Share with us three most critical fundamentals that have to be in place for effective cybersecurity in the healthcare space.

**RB:** **Start from a position of knowledge.** Assess your data and systems to know their value, who and what have access, the data and systems locations, their threats and vulnerabilities, their protections and how well these protective systems function.

**Once you determine your cybersecurity profile, identify gaps and solutions to close them.** Select a standard such as the National Institute of Standards and Technology's Cybersecurity Framework to protect critical infrastructure and apply best practices.

**Consider this an ongoing process.** Cybercriminals look for the easiest targets. If they encounter barriers, though, they will try to adapt. Develop a cybersecurity protocol that can account for adaptations as well as new threats.