Cybersecurity

THE TELEMEDICINE AND HOLISTIC RISK BACK STORY

October 17, 2017

Telemedicine: Post by Peter Sheingold and Catherine Barrett

Catherine's Telemedicine Story: In 2014, I accompanied a friend to an appointment at a private hospital in Turkey.

What I saw was something special.

A completely paperless hospital where doctors care for patients from around the world, remotely via the Internet. The entire hospital runs on a digital platform, eliminating the need for paper medical records and paper-based administrative processes. Patients, for example, sign paperwork using digital tablets, and doctors use iPads to access patient records and take notes.

Doctors spend a portion of each week reviewing medical records of remotely located patients and consulting with them online. A patient from another country uploads his or her medical record for review using a secure connection and discusses diagnosis and treatment options via a platform that allows doctor and patient to see each other.

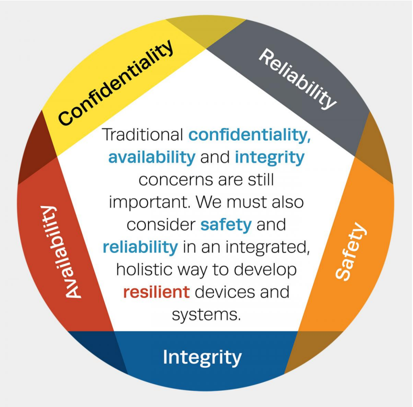
The service offerings in the hospital are enabled by a web of telecommunications infrastructure, mobile devices, and applications. The desire to have a paperless, digitally run hospital influenced the design of the hospital, from the size and layout of patient rooms to the power supply and telecommunication cables supporting the physical structure.

I left the hospital feeling inspired about the future of medical care delivery, about how patients and healthcare providers can benefit from using networked technologies to improve quality of care and patient outcomes. My visit to that hospital inspired me to write a book about Telemedicine services, which use telecommunications technology to remotely deliver healthcare.

My visit also made me wonder how the telemedicine services provided by the hospital present vulnerabilities that could be exploited. What risks did they present to the trusted doctor/patient relationship? What about the health and safety of patients? What about the confidentiality of medical records?

Peter's Holistic Risk Story: Telemedicine services that could help doctors diagnose and treat you from anywhere and that could also be exploited to harm you from anywhere. How should we address the associated risks that go beyond traditional information security considerations of data confidentiality, availability, and integrity and include human safety and infrastructure reliability risks (i.e., holistic risk)?

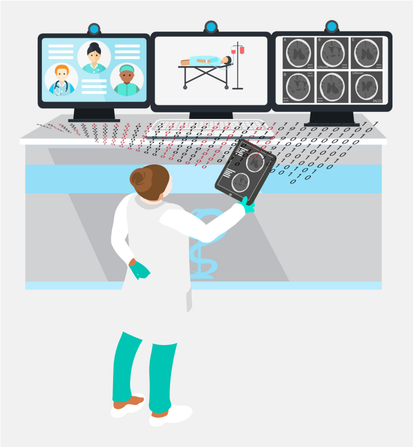
In our previous CyberPhysicalHuman series, we began exploring holistic risks that come from converged technologies, which can both inform human decision making and have an impact in the physical world. Telemedicine is an example of this technology convergence and offers a great way to explore the holistic risk question more fully.


Confidentiality
Reliability
Safety
Integrity
Availability
Traditional confidentiality, availability and integrity concerns are still important. We must also consider safety and reliability in an integrated, holistic way to develop resilient devices and systems.

Holistic Risk

The scale of interconnectedness found in telemedicine, where so many devices, people, systems, and services are needed to deliver healthcare, means potential cyber-attacks or disruptions could both physically harm patients and expose highly sensitive personal data.

As a recent report from the U.S. Department of Health and Human Services-led Healthcare Industry Cybersecurity Task Force noted, "the risk of potential cybersecurity threats increases as more medical devices use software and are connected to the Internet, hospital networks, and other medical devices." As cybersecurity threats and vulnerabilities cannot be completely eliminated, "manufacturers, hospitals, and facilities have to work to manage them to protect patient safety." As our society grapples with addressing an evolving technology landscape where devices pose both traditional information security risks and human safety and infrastructure reliability risks, these blog posts offer a way to inform how these holistic threats and vulnerabilities are managed.
[i]



Tele-ICU

Telemedicine services includes many different technologies and devices. A growing number of insurance companies include telemedicine medical services in their benefit packages to reduce costs. Our next posts will explore the holistic risk profiles of two different telemedicine services—a Tele Intensive Care Unit (Tele-ICU) and Mobile Medical Application (mobile-app). We will then explore how these different risk profiles can inform the types of risk management and resilience strategies that different stakeholders can take.

Our goal in doing so is not to make our readers experts in telemedicine nor to evaluate the current state of risk management in telemedicine.

[ii]

Instead, we hope to demonstrate how to apply the concept of holistic risk to real devices in real business environments in a way that can inform risk management and resilience strategies by a variety of stakeholders. In doing so, both policy and technology considerations will be vitally important.

Mobile-App

Telemedicine: A Three-Part Series about Technology Convergence and Holistic Risk
Post #2: Applying Holistic Risk to Telemedicine—Different Uses, Different Risks
Post #3: Managing Holistic Risk in Telemedicine: A Stakeholder Perspective

About Catherine Barrett

Catherine Barrett is a cyber policy principal with MITRE and co-author of *What Is...Telemedicine?*, a health law primer on telemedicine published by the American Bar Association. She received her JD and MBA from the American University Washington College of Law and Kogod School of Business, respectively. She may be reached here.

About Peter Sheingold

Peter Sheingold is a Principal who has worked on a range of cybersecurity challenges that lie at the intersection of strategy, policy, organization, operations, and technology. For questions or to comment, Peter Sheingold can be contacted here.

[i] The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is helping healthcare delivery organizations (HDOs) address potential cybersecurity risks associated with medical devices. HDOs, for example, can access free guidance documents and best practices regarding how to apply commercially available cybersecurity technologies to protect wireless infusion pumps and electronic health records on mobile devices. National Cybersecurity Center of Excellence at the National Institutes of Standards and Technology, U.S. Department of Commerce, *Securing Wireless Infusion Pumps* (NIST SP 1800-8A), May 2017 and *Securing Electronic Health Records on Mobile Devices* (NIST SP 1800-1a), October 2015. Available: https://nccoe.nist.gov/projects/use-cases/health-it

[ii] These blogs refer to telemedicine industry participants, hospitals, and healthcare providers merely to illustrate cybersecurity risk management concepts and do not evaluate how the telemedicine or broader healthcare industry, or individual organizations, are or are not using risk management concepts to address cybersecurity risks.

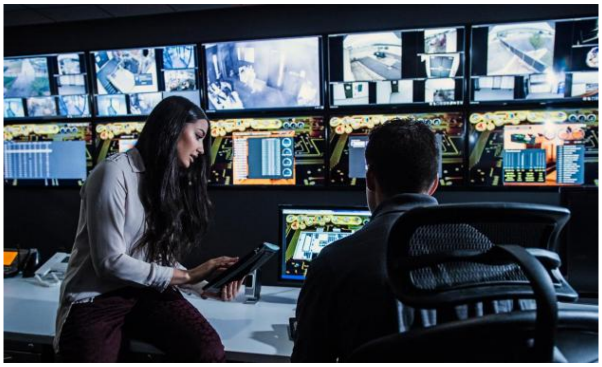
Related Technical Papers

Eight Recommendations for Congress to Improve Federal Cybersecurity

Breaking the Ransomware Cyc National Policy Options

SEE ALL TECHNICAL PAPERS

Related Projects



Pioneering New Ways to Protect Our Nation

Paving the Way for Automated Dı Systems

SEE ALL PROJECTS