Epic

March 14, 2023

Testimony of Stirling Martin
Before the United States Senate
Committee on Homeland Security and Governmental Affairs

Distinguished members of the committee, thank you for the opportunity to provide my testimony today. My name is Stirling Martin, my formal training is as a computer scientist, and I am the Chief Security and Privacy Officer and Senior Vice President at Epic. Since 1979, we've created clinical, financial, and administrative software, including the patient portal, MyChart, for healthcare organizations in the U.S. and around the world. Our customers include academic medical centers, integrated health systems, critical access hospitals, and federally qualified health centers.

Our focus first and foremost is on helping patients. Personal health data is uniquely sensitive if compromised because it cannot be reset like passwords or changed like credit card information. A patient's health information can also be immensely personal, and even just the threat of exposure can create angst for an individual. If exposed, private healthcare data can be leveraged by malicious actors through identity theft and the potential for blackmail. In an extreme case, patient safety could be directly impacted if a bad actor were to manipulate healthcare data.

Within a community, cyberattacks can reduce access to care. In a rural community with only one healthcare facility, patients may need to delay preventative care or elective treatments until an incident is resolved. In a larger community, a cyberattack can have a cascading effect as patients may be diverted to an unfamiliar care team at another facility, and those facilities need to deal with an influx of additional patients.

We've been shoulder to shoulder with our customers as healthcare has become increasingly targeted by cyberattacks. For a health system, a cyberattack disrupts their patient care mission, and causes both reputational harm and financial burden. Organizations often take their systems offline as they mitigate the impact of a security incident. Doing so places stress on staff to provide high quality care without the IT systems that drive their workflows. As organizations may see fewer patients, the financial impact extends beyond the cost of incident response to lost revenue as well.

Organizations face several challenges in improving their security posture. First is staffing, and their ability to hire and retain high-demand security talent.

Second, security is a constant effort, and there are always more steps that can be taken to make systems more secure. In working with healthcare organizations across the country, we see both basic and highly sophisticated security programs in use, and yet there is no defined benchmark of what security practices are considered sufficient.

An additional challenge is the lack of cybersecurity information sharing among healthcare organizations, as well as the limited threat intelligence from government agencies and private industry.

These challenges are exacerbated as many healthcare organizations currently face unprecedented financial and staffing pressures. The costs to improve one's security posture through new technology or staff must be weighed against other needs such as recruiting and retaining nurses at the bedside.

There are a variety of ways the federal government could help healthcare organizations prevent and respond to cyberattacks.

Starting first with prevention, there is a dire shortage of security talent in the United States. To build a deeper bench of skilled IT security professionals, the federal government could develop security training programs and incentivize newly trained professionals working in healthcare. This could be similar to the Rural Community Loan Repayment program for physicians who agree to provide care to rural communities after medical school and residency.

Secondly, the industry needs a single set of prescriptive security practices, whether defined by federal agencies such as NIST or CISA, industry efforts such as HITRUST, or a collaboration such as the Healthcare Sector Coordinating Council. This will raise the overall security posture of healthcare organizations by encouraging them to meet those acceptable security practices. The government should take the further step of establishing a legal safe harbor for organizations that meet the defined benchmark if they fall victim to an incident. This would also encourage information sharing to remediate active issues more quickly and prevent similar issues in the future, and could be bolstered by government agencies sharing deeper threat intelligence.

Lastly, on incident response, similar to how FEMA responds to a natural disaster, at-the-elbow support from the government could help healthcare organizations remediate an attack. For example, an organization recovering from a ransomware attack may need assistance cleaning and redeploying the computers used by their staff. On-the-ground support could help reduce the time it takes to bring systems back online by patching devices or by delivering a strategic reserve of computers and network equipment that can be used immediately. This could reduce recovery time by hours or days, providing tremendous value to healthcare organizations and the patients they serve.

In closing, people often ask me what keeps me up at night. It’s the reality that we have to be perfect 100% of the time, and the bad guys only need to be lucky once.

Thank you for the opportunity to share Epic’s perspective on this important topic.