Testimony of Dr. Christian Dameff MD

Before the Committee on Energy and Commerce
Subcommittee on Oversight and Investigations

U.S. House of Representatives

“Stopping Digital Thieves: The
Growing Threat of Ransomware.”

July 20th, 2021
Washington, DC

Introduction

Madam Chair DeGette, Ranking Member Griffith, distinguished members of the subcommittee, thank you for the opportunity to testify today on the effects of ransomware on healthcare. My name is Dr. Christian Dameff and I am a practicing Emergency Medicine Physician. I am also an assistant professor of Emergency Medicine, Biomedical Informatics, and Computer Science at the University of California San Diego. I also serve as the Medical Director of Cybersecurity for UC San Diego Health, the first position of its kind in the United States. Early in my adolescence, my fascination with computers and networks led me to the hacking community, who taught me to appreciate the complexity and fragility of modern computer systems. Today, I use that knowledge to improve the cybersecurity of healthcare. My research focuses on the patient safety and care quality effects of cyber attacks.

At my core, I am an Emergency Medicine doctor. I am trained to care for any patient who comes through the doors whether they suffer trauma, heart attack, stroke, or COVID. I am here today to tell you healthcare is not prepared to defend or respond to ransomware threats.

Technological Dependence

Our hospitals today are increasingly dependent on technology. Doctors admit patients into the hospital, order and review test results, prescribe medications and prepare for surgeries all while using computerized workflows. We have come to implicitly trust and rely on these systems, and when they fail healthcare grinds to a near halt.

Patient Safety

We know ransomware attacks affecting the healthcare sector are increasing in frequency, sophistication, and disruptive potential. In addition to the exposure of sensitive data, severe financial losses, and reputational damage, a cyber attack on a hospital has the potential to threaten life and limb.

When patients suffer from strokes, heart attacks, or severe infections, minutes matter. The best outcomes for patients with these time-dependent crises depend on the immediate, continuous availability of the same digital systems that ransomware can disrupt. When critical medical systems go offline, our opportunity to save lives diminishes. Our risk of error or misdiagnosis increases.

We are now learning that cyber attacks impact not just infected hospitals, but the surrounding healthcare ecosystem at large. Two months ago, a ransomware attack disabled five large hospitals in the San Diego area for an entire month. Adjacent hospitals were quickly overwhelmed with unprecedented numbers of emergency room patients, many of whom had serious, time-dependent illnesses. Wait times skyrocketed. Hospital beds rapidly filled. Clinicians caring for very sick patients lacked vital medical records from the infected hospitals. I saw firsthand the “spill-over” effects and understood that the vulnerability of one hospital is the vulnerability of many hospitals.

Recommendations

You have heard today from experts with technical and policy recommendations that, if enacted, will improve ransomware defenses across all sectors. However, as I hope you now recognize, healthcare has unique challenges which necessitate additional actions.

First, the effects of ransomware attacks on patients’ health should be scientifically studied, just like diseases such as diabetes. Most hospitals are not currently equipped to measure or report the impact of these attacks. I recommend the development of standardized metrics of cyber attack severity on hospitals. Mandatory reporting of patient safety and care quality outcomes should occur for severe attacks. I recommend that federal agencies such as the National Institutes of Health (NIH) and the National Science Foundation (NSF) prioritize funding for research on this topic.

Second, identifying cybersecurity vulnerabilities before they are exploited will protect patients. There is currently a disparity between what I call the healthcare cybersecurity haves and have nots. Lesser-resourced critical access and rural hospitals need help increasing their preparedness. As we seek to protect vulnerable hospitals, we must also avoid overly punitive measures for those unfortunate enough to fall victim to highly complex or novel cyber attacks, understanding that stiff fines or penalties may worsen

an already devastating operational impact. We are only as strong as our least defended communities.

Third, I support software bill of materials (SBOM) as one mechanism to increase transparency around cybersecurity vulnerabilities. SBOM enables manufacturers and healthcare delivery organizations to take more proactive steps to manage their cybersecurity risk. Furthermore I recommend ongoing support and legal protections for security researchers engaging in good-faith security research, otherwise known as coordinated vulnerability disclosure. We need help from ethical hackers if we are going to defeat the malicious ones.

Lastly, we must prepare hospitals for inevitable attacks. The ability to rapidly deploy backup manual patient care systems is key to reducing harms to patients. Such contingency planning takes resources and expertise.

Conclusion

In conclusion, I applaud this committee's leadership on ransomware response and remain optimistic about improving cyber resilience in healthcare. Our patients deserve excellent care. Ransomware and other cyber attacks targeting hospitals threaten our ability to deliver that care, as it's needed- when minutes matter.

Thank you for this opportunity to testify today and I welcome any questions you may have.