HERJAVEC GROUP

The 2020-2021 Healthcare Cybersecurity Report

A Special Report from the Editors at Cybersecurity Ventures

Sponsored by Herjavec Group

Cybersecurity Ventures predicts that the healthcare industry will spend upwards of $125 billion cumulatively on cybersecurity products and services from 2020-2025.

Cybercriminals are taking advantage of hospitals and medical practices focused on COVID-19.

Healthcare spending in the U.S. — which is the highest among developed countries — accounts for 18 percent of the nation's gross domestic product, or about $3.5 trillion, the Centers for Medicare & Medicaid Services estimate, and that figure is projected to soar over the next decade.

One report predicts that global healthcare spending will rise from nearly $8 trillion (USD) in 2013 to more than $18 trillion in 2040.

By and large, the tantalizing target on healthcare's back has been attributable to outdated IT systems, fewer cybersecurity protocols and IT staff, valuable data, and the pressing need for medical practices and hospitals to pay ransoms quickly to regain data.

Cybersecurity Ventures predicts the global healthcare cybersecurity market will grow by 15 percent year-over-year over the next five years, and reach $125 billion cumulatively over a five-year period from 2020 to 2025.

What's driving this astronomical investment into cyber defense? Cyber offense. Namely, a vast number of wide-ranging hacks and data breaches launched on hospitals and healthcare providers.

A year ago, well before the COVID-19 pandemic, The Wall Street Journal reported that cyberattacks on healthcare providers and hospitals had intensified to the point where some doctors were turning away patients.

But wait, it gets worse.

Some healthcare centers turned off their lights and pulled the plug on their operations altogether. Apparently they couldn't handle the post-attack disruption to their operations.

A medical clinic in Simi Valley, Calif. recently shut its doors after being infected by a ransomware attack. An ear, nose, throat (ENT) and hearing center in Battle Creek, Mich. closed after a data hack wiped out all of its files.

"Healthcare organizations experience very particular security challenges and it's not because the cyberattacks are unique, but because of what's at stake," says Robert Herjavec, founder and CEO of Herjavec Group, a leading global cybersecurity firm and Managed Security Services Provider (MSSP).

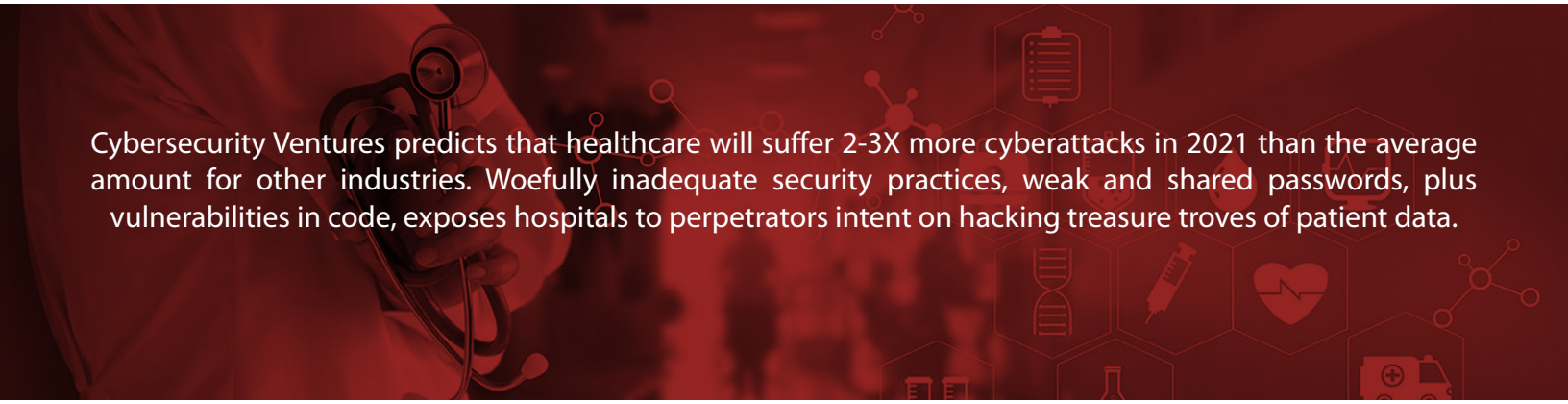
IoT insecurity

Kathy Hughes, CISO (chief information security officer) at Northwell Health, one of the nation's largest healthcare systems, told Cybercrime Magazine that IoT (Internet of Things) devices are, in her opinion, computers with operating systems (OS), similar to other types of computers — and those devices are susceptible to the same cyber threats. She added that IoT devices have a small OS and that security is a bolt-on rather than built-in.

Inside jobs

The insider threat is the number one security challenge for hospitals, according to Hughes, who is responsible for protecting 68,000 employees, which makes Northwell, a non-profit, New York state's largest private employer.

More than half of insider fraud incidents within the healthcare sector involve the theft of customer data, according to CMU SEI (Carnegie Mellon University Software Engineering Institute).



Cybersecurity Ventures predicts that healthcare will suffer 2-3X more cyberattacks in 2021 than the average amount for other industries. Woefully inadequate security practices, weak and shared passwords, plus vulnerabilities in code, exposes hospitals to perpetrators intent on hacking treasure troves of patient data.

Healthcare Cybersecurity Statistics

To sum up the state of cybersecurity in the healthcare industry, the editors at Cybercrime Magazine have compiled the following data points:

- Ransomware attacks on healthcare organizations were predicted to quadruple between 2017 and 2020, and will grow to 5X by 2021, according to a report from Cybersecurity Ventures.
- The Secretary of U.S. Department of Health and Human Services (HHS) Breach of Unsecured Protected Health Information lists 592 breaches of unsecured protected health information affecting 500 or more individuals within the last 24 months that are currently under investigation by the Office for Civil Rights. 306 of the breaches were submitted in 2020.
- In last year's edition of the HIMSS Cybersecurity Survey, nearly 60 percent of hospital representatives and healthcare IT professionals in the U.S. said that email was the most common point of information compromise. This refers to phishing scams and other forms of email fraud.
- 24 percent of U.S. health employees have never received cybersecurity awareness training, but felt they should have, according to a report analyzed by Health IT Security last summer. This type of training is aimed at helping users detect and react to phishing scams, which initiate more than 90 percent of all cyberattacks.
- More than 93 percent of healthcare organizations have experienced a data breach over the past three years, and 57 percent have had more than five data breaches during the same time frame.
- While 91 percent of hospital administrators considered the security of data as a top focus last year, 62 percent feel inadequately trained and/or unprepared to mitigate cyber risks that may impact their hospital, according to research from Abbott.
- Hospitals spend 64 percent more annually on advertising after a breach over the following two years, according to a Dec. 2018 report from the American Journal of Managed Care.
- Four to seven percent of a health system's IT budget is in cybersecurity, compared to about 15 percent for other sectors such as the financial industry, according to Lisa Rivera, a former federal prosecutor who is now focused on advising healthcare providers and medical device companies on matters related to civil and criminal healthcare fraud and abuse, as well as government investigations and enforcement.
- IT research firm Gartner predicts that in 2020, more than 25 percent of cyberattacks in healthcare delivery organizations will involve the Internet of Things (IoT). To be clear, in medical terms, that means wirelessly connected and digitally monitored implantable medical devices (IMDs) — such as cardioverter defibrillators (ICD), pacemakers, deep brain neurostimulators, insulin pumps, ear tubes, and more.
- Research from Oct. 2018 indicates that medical devices have an average of 6.2 vulnerabilities each; 60 percent of medical devices were at end-of-life stage, with no patches or upgrades available.
- Cybersecurity blogger and author Brian Krebs reported late last year that hospitals hit by a data breach or ransomware attack can expect to see an increase in the death rate among heart patients in the following months or years because of cybersecurity remediation efforts. This is according to a study by Vanderbilt University.

COVID-19

Hacking patients' medical devices is a common cyberattack during the COVID-19 pandemic because more patients are using remote care, according to Natali Tshuva, CEO and co-founder of Sternum, an IoT cybersecurity company that provides medical device manufacturers with built-in security solutions.

The temporary and makeshift medical facilities being used to care for people infected with the novel coronavirus have created more vulnerabilities for hackers to exploit.

COVID-19 phishing exploded earlier this year, according to research from KnowBe4, a leading security awareness training provider. Many of the scams seemed to come from organizations such as the World Health Organization and the Centers for Disease Control. Already overburdened healthcare IT and cybersecurity teams have been tasked to keep up on these new threats.

Fake tumors?

The scariest of all cyber malintent in the healthcare space may lie ahead.

Researchers in Israel announced last year that they'd created a computer virus capable of adding tumors into CT and MRI scans — malware designed to fool doctors into misdiagnosing high-profile patients, according to a story by Kim Zetter in The Washington Post.

Saving lives

"If a cyberattack happens in healthcare, then health records can be stolen, life-saving devices can be disrupted and the intricate networks needed to support our health severely impacted," says Herjavec. "Unfortunately, these challenges are only intensifying as the COVID-19 pandemic accelerates digital transformation."

Herjavec has been warning about ransomware attacks on hospitals and healthcare providers for more than three years.

Healthcare providers, boards and C-suite executives need to take the cyber threat as seriously as Herjavec does. Nobody wants a patient death to be a wake-up call for cybersecurity.

About the Author

Steve Morgan is Founder and Editor-In-Chief at Cybersecurity Ventures. He oversees all of the editorial for Cybersecurity Ventures which includes our research, quarterly and annual reports, and directories.

About Cybersecurity Ventures

Cybersecurity Ventures is the world's leading researcher and publisher covering the global cyber economy. Our firm delivers cybersecurity market data, insights, and ground-breaking predictions to a global audience of CIOs and IT executives, CSOs and CISOs, information security practitioners, cybersecurity company founders and CEOs, venture capitalists, corporate investors, business and finance executives, HR professionals, and government cyber defense leaders.

For more information, visit http://www.cybersecurityventures.com/

About Herjavec Group

Dynamic entrepreneur Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. Our service expertise includes Advisory Services, Technology Architecture & Implementation, Identity Services, Managed Security Services, Threat Management and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom and Canada.

For more information, visit **www.herjavecgroup.com.**

Follow Us
Herjavec Group
@HerjavecGroup