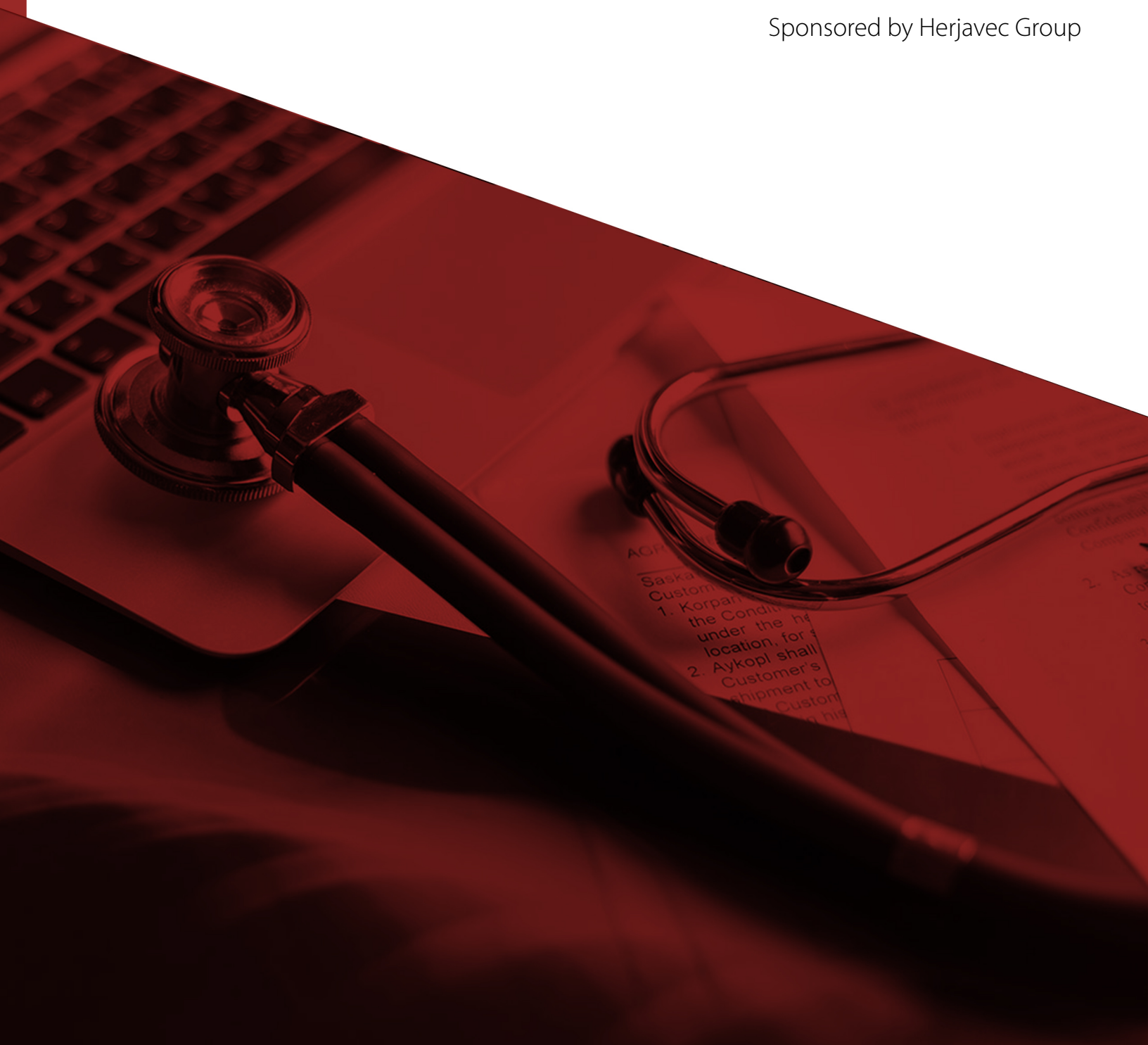
HERJAVEC GROUP

The 2020 Healthcare Cybersecurity Report

A Special Report from the Editors at Cybersecurity Ventures

Sponsored by Herjavec Group



2020 Healthcare Cybersecurity Report

HERJAVEC GROUP

Cybersecurity Ventures predicts that the healthcare industry will spend more than $65 billion cumulatively on cybersecurity products and services over the five year period from 2017 to 2021.

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

The Wall Street Journal reports that cyberattacks on healthcare providers and hospitals have intensified to the point where some doctors are turning away patients.

But wait, it gets worse.

Some healthcare centers have turned off the 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.

"When it comes down to it, at any healthcare organization C-Suite executives are worried about the same thing," says Robert Herjavec, founder and CEO of Herjavec Group, a leading global cybersecurity firm and Managed Security Services Provider (MSSP), "Balancing a security budget, and lack of security personnel in an increasingly sophisticated and broad attack surface."

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).

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:

- Cybersecurity Ventures predicted that healthcare would suffer 2-3X more cyberattacks in 2019 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.
- Ransomware attacks on healthcare organizations are predicted to quadruple between 2017 and 2020, and will grow to 5X by 2021, according to a report from Cybersecurity Ventures.
- In the 2019 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.
- The HIPAA Journal features data from a vendor report that claims healthcare email fraud attacks have increased 473 percent in two years.
- 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. This type of training is aimed at helping users detect and react to phishing scams, which initiate more than 90 percent of all cyber attacks.
- 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 timeframe.
- While 91 percent of hospital administrators consider the security of data as a top focus, 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 recent 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 by 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.
- Medical devices have an average of 6.2 vulnerabilities each; 60 percent of medical devices are at end-of-life stage, with no patches or upgrades available.
- Cybersecurity blogger and author Brian Krebs reports hospitals that have been 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.

Fake Tumors?

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

Earlier this year, researchers in Israel announced 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

"Healthcare is one of our fastest growing verticals," says Herjavec Group CEO, Robert Herjavec. "The fundamental difference between healthcare and other industries," he adds, "is that it's not just about money. It's about lives."

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