HERJAVEC GROUP

Cybersecurity Ventures Global Healthcare Cybersecurity Spending Will Exceed $65 billion Cumulatively Over the Next Five Years, from 2017 to 2021

2017 Healthcare Cybersecurity Report

A Special Report from the Editors at Cybersecurity Ventures

Sponsored by Herjavec Group

Cybersecurity Ventures predicts global healthcare cybersecurity spending will exceed $65 billion cumulatively over the next five years, from 2017 to 2021.

Ransomware attacks on healthcare organizations are predicted to quadruple by 2020.

Robert Herjavec has been warning about ransomware attacks on hospitals and healthcare providers for more than a year. In 2016, his firm, Herjavec Group, collaborated with Cybersecurity Ventures on a report that indicated ransomware damages would reach $1 billion for the year.

In 2017, healthcare providers are the bullseye for hackers.

As the healthcare industry continues digitizing its information, it continues to attract more attention from cybercriminals. This dynamic will be one of the many contributors to the growth of the healthcare security market over the next decade.

Data thieves used to set their sights on stealing financial records or bank account numbers. They focused on laptops with unencrypted hard drives and simple spam or phishing scams. Now they're deploying advanced techniques, such as SQL injections, Advanced Persistent Threats, Zero Day exploits, and ransomware.

Ransomware — where an organization's data is held captive by an attacker who promises to release it for a price — has become such a lucrative revenue source for hackers that IDC predicts that attacks on healthcare organizations will double by 2018.

In fact, Cybersecurity Ventures predicts ransomware attacks on healthcare organizations will quadruple by 2020.

In its 2017 data breach forecast, Experian, which provides identity protection services to consumers, predicted that ransomware will be a top concern for healthcare organizations this year, particularly because those attacks have the potential to be catastrophic.

"Ransomware presents an easier and safer way for hackers to cash out; given the potential disruption to a company, most organizations will opt to simply pay the ransom," the report notes, adding, "This has unintended consequences of funding more research and development by attackers who will in turn develop more sophisticated and targeted attacks."

"Healthcare is the most hacked vertical we're seeing right now and what makes this industry different is that it affects everyone not just financially but personally," says Atif Ghauri, CTO at Herjavec Group, a global information security company.

Ghauri warns about the Internet of Things (IoT) risk in healthcare. "Knowing your disease history, physical limitations, and other personal details exposes everyone to risks. Consider the IoT risks alone – healthcare compromises could result in fatality from a compromised Wi-Fi heart pump or a dysfunctional smart bed in the surgery room. It's scary stuff."

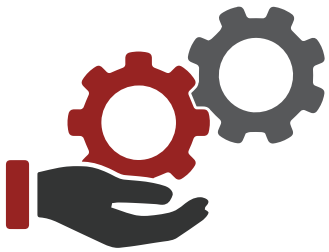
"We often educate our customers in this space on the risks of ransomware," adds Ghauri. "Over the last year we saw multiple hospitals taken "hostage" and actually pay out the ransom in an effort to regain control of their systems. We never advocate for payment in the event of ransomware. There is no effective law enforcement for cybercrime today and no way of knowing that even if a ransom is paid, you will get your data back."

"Paying a ransom is a desperate measure," says Steve Morgan, founder and Editor-In-Chief at Cybersecurity Ventures. "Ransomware damage costs result not only from cybercriminal activity, but from healthcare organizations who fail to train their employees on spear phishing and ransomware attacks, fail to backup data, and a general unpreparedness to cyber defend."

Ghauri encourages healthcare organizations to increase their defenses – and to invest in employee training, technologies, processes, and incident responses plans to get ahead of ransomware attacks.

"Ransomware is exploding and it will continue to plague the healthcare organizations who fail to train their employees on how to spot and react to phishing attacks and other detectable cyber threats."

–Kevin Mitnick, Chief Hacking Officer at KnowBe4



Hospitals are Most Vulnerable

When the Locky strain of ransomware infected Hollywood Presbyterian Medical Center in Los Angeles, Calif. early last year, the initial media coverage was around Locky itself — and the fact that the hospital paid a $16,000+ ransom. Worse though, was the negative press, and a report that the hospital was effectively on lock-down with staff unable to turn on their computers and radiation and oncology departments unable to use their equipment.

Dozens of ransomware attacks on hospitals followed the Hollywood Presbyterian debacle.

A Symantec infographic on cybersecurity in healthcare — which includes data from Cybersecurity Ventures, the FBI, The White House, HIMSS, Bloomberg, and others — states that healthcare data is unique, which makes its privacy and security so critical. While credit cards can be canceled when lost or stolen, medical records can be compromised for years.

The FBI's Cyber Division warned in a Private Industry Notification nearly three years ago that electronic healthcare records were selling for $50 per chart on the black market, compared to $1 for a stolen social security number or credit card number. The Notification stated, "The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely."

HIT Consultant, a leading source of healthcare technology news, recently reported that personal health information is 50 times more valuable on the black market than financial information, and stolen patient health records can fetch as much as $60 per record.

"Hospitals are more vulnerable than any other type of organization right now," says Morgan. "Outdated systems, lack of experienced cyber personnel, highly valuable data, and added incentive to pay ransoms in order to regain patient data, are magnetizing hackers to the healthcare market."

> **"Unfortunately, too many of [healthcare providers] wait until they've suffered a hack or data breach before turning to outside firms for help."**
>
> –Atif Ghauri, CTO, Herjavec Group

FBI On Healthcare

James Comey, Director of the FBI, recently delivered the keynote address at the Boston Conference on Cybersecurity (BCCS, 2017). When asked about the biggest cyber threat facing healthcare providers, Comey answered "ransomware", according to a story in the National Law Review.

Comey also advised that healthcare organizations should not pay ransoms as doing so emboldens hackers and encourages more ransomware attacks. To avoid paying ransoms, Comey recommends preparedness – namely data backup and business continuity plans.

The FBI's Cyber Division is alerting the healthcare industry on other cyber threats as well.

A new Private Industry Notification aimed at healthcare organizations advises that the FBI is aware of criminal actors who are targeting FTP servers associated with medical and dental facilities to access protected health information (PHI) and personally identifiable information (PII) in order to intimidate, harass, and blackmail business owners.

That FBI Notification stems from a 2015 study published by the University of Michigan that found more than 1 million anonymous (no password required) FTP servers were connected to the Internet – exposing 600 million files and directories to the open Internet.

FTP servers are low hanging fruit for hackers to obtain health data (insurer, employing company, social security, birth date, etc.) — which can be used to commit insurance fraud, buy drugs or medical equipment or steal an identity, according to a blog post from Ipswitch, an IT management software provider.

Ipswitch notes that FTP servers are everywhere. Smaller medical and dental practices likely have them embedded in turnkey software provided by a reseller some 5 years ago. They are in Ricoh and Xerox printers. Ipswitch customers have told stories of finding them unattended in some forgotten corner or closet.

Director Comey wants (U.S.) healthcare organizations to report all cyber attacks and data breaches to the FBI. Healthcare industry and law enforcement collaboration is essential to combatting cybercrime.

Risk and Rules Drive Spending

Because the risks to healthcare data are growing, government regulators will be required to increase their scrutiny of the industry. The threat of fines from those regulators, along with the jump in cyberattacks on healthcare organizations, will nudge them to spend more on cybersecurity to protect the electronic health information of their clients.

What's more, because the attacks on healthcare organizations will continue to grow in sophistication, providers will be demanding more from their IT assets. They will be demanding, for example, that applications include strong, baked-in security features that prevent adversaries from compromising the apps and gaining access to the data and the networks they interact with.

Principal Connected Health Analyst at Frost & Sullivan, Nancy Fabozzi explained to the HIPAA Journal, "Hospitals are transitioning from their traditional reactive and fragmented approach to protecting privacy and security that is highly dependent on HIPAA compliance to a new approach and mindset that is proactive, holistic, and coordinated, anchored by integrated solutions designed to protect multiple endpoints."

Double-Digit Growth

Those kinds of solutions cost money, money that will be driving the healthcare security market over the next five years. "The healthcare market has been undersized by researchers because it's limited mainly to IT security," says Morgan.

IT Analyst forecasts have not kept pace with many of the factors that can impact healthcare IT expenditure, including: the dramatic rise in cybercrime, the ransomware epidemic, the refocusing of malware from PCs and laptops to smartphones and mobile devices, the massive deployment of smart medical IoT devices that require embedded security, growth in computer controlled hospital building physical and electronic security, hackers-for-hire who target hospitals, the more sophisticated cyber-attacks launching at healthcare organizations, and the need to train employees on security awareness.

Cybersecurity Ventures predicts the healthcare industry will spend more than $65 billion cumulatively on cybersecurity products and services over the next five years, from 2017 to 2021. "We anticipate 12-15 percent year-over-year cybersecurity market growth through 2021, commensurate with other industries," says Morgan.

"Healthcare organizations have lagged the market in cyber defense spending, and they've suffered for it," Morgan adds. "They've been hacked into spending. Security has become just as important, if not more so, as digitizing patient records."

"Healthcare is one of our fastest growing verticals," says Robert Herjavec, founder and CEO of Herjavec Group.

"The fundamental difference between healthcare and other industries," he adds, "is that it's not just about money. It's about lives."

According to a report by Grand View Research that looks out to 2022, the largest portion of the healthcare cybersecurity market is in North America. The report highlights that the region's sophisticated healthcare infrastructure and collaboration between the pharmaceutical and medical-device industries and regulators have all contributed to a robust market.

In addition, the United States is a bit of a magnet for healthcare data thieves as it's the home of some very large Fortune 500 healthcare organizations and it makes extensive use of digital patient records and Social Security Numbers for transactions.

Other areas of the world will be making larger contributions over the coming years, however. China, India, and South Korea all have developing healthcare infrastructure. Couple that with growing numbers of online users and you have a target market for information thieves.

> **"Healthcare providers have to prioritize a proactive approach to security — balancing people, process, and technology to improve the protection of their informational assets and patient information."**
>
> –Robert Herjavec, CEO & Founder, Herjavec Group

Priorities Need Realignment

Healthcare security executives appear to have less understanding of the threats facing their organizations than executives in other industries, according to a 2016 White Paper from Cisco.

Because IT spending in the healthcare industry has lagged and cybercrime awareness — until recently — has been largely missing, providers have found themselves vulnerable to attacks. "Healthcare organizations are a prime target for cyberattacks because they're focused on what they do best — providing patient care," explains Herjavec. "In the majority of cases, budgets are spent on research, on advancing treatment, and rightfully so, on patient care."

"Many security systems are entirely antiquated while emerging tech is too expensive and cumbersome to implement or adapt," he says. "But just like a large public enterprise organization, healthcare providers have to prioritize a proactive approach to security — balancing people, process, and technology to improve the protection of their informational assets and patient information."

In the coming years, healthcare organizations will be buying security solutions for identity and access management, risk and compliance management, antivirus and antimalware software and DDoS mitigation services, as well as security information and event management, intrusion detection and intrusion prevention systems.

Herjavec predicts that in the next three years, healthcare providers will be adopting technology at a rate that's on par with other industries.

"They have to," he says.

"Improvements in auditing and monitoring have already taken healthcare security a very long way," he continues. "By leveraging user behavior analytics and improved identity management tools, healthcare providers are better able to determine who has access to what data, when, for how long, and why."

"Continued adoption of technologies being adopted by the general market, including SIEM, IPS, Next Gen Firewalls, and endpoint securities will only continue to benefit the healthcare industry," he adds.

Lack Of Staff

"The Black Hats are still multiple car lengths ahead in the grand prix of the cybersecurity race," says Atif Ghauri. "The few organizations that have mature tools and processes to detect attacks, are still doing just that – detection. Few and far between actually know what data was compromised and when."

Ghauri subscribes to the notion that black-hat hackers are more daring and experienced than white-hat hackers. In the healthcare space, the black-hats face limited competition.

"Healthcare organizations are often the worst places to work for cybersecurity engineers," says Ghauri. The industry traditionally doesn't pay well. Hospitals have some of the least innovative and most antiquated platforms. There's more off-the-shelf software than other markets. Security engineers may not find their work as challenging as other verticals which generally have more custom code."

The cybersecurity workforce shortage, which has 1 million job openings in 2017, and is projected to reach at least 1.5 million by 2019, is especially acute at hospitals and healthcare providers, according to a recent CSO story.

The most sophisticated and high-paying industries, including financial services, are competing for talent against the hottest pure-play cybersecurity vendors and MSSPs (managed security service providers), the tech giants — including IBM, Cisco, Microsoft, Google, Amazon and others who are aggressively pushing into cyber and defending their own massive cloud infrastructures — and governments who promise to train the next generation of cyber warriors.

"Healthcare organizations are severely challenged when it comes to recruiting and retaining security personnel," says Ghauri. "Many healthcare providers have tried to manage security internally, and failed. Unfortunately, too many of them wait until they've suffered a hack or data breach before turning to outside firms for help."

Not All Doom and Gloom

"Ransomware is exploding and it will continue to plague the healthcare organizations who fail to train their employees on how to spot and react to phishing attacks and other detectable cyber threats," says Kevin Mitnick, the world's most famous hacker and Chief Hacking Officer at KnowBe4, a security awareness training company.

Mitnick informs that a surprising number of enterprises – including healthcare companies – still don't have the backups they need in order to avoid paying ransoms. His best piece of advice: backup. Sounds simple, but the ransom payouts are proof that the backups are not in place. HR chiefs may want to take Mitnick's advice to heart and mandate all employees to backup their business and BYOD data.

Despite the rise in cybercriminal activity committed against healthcare organizations, there is a bright side.

"IT and security leaders at healthcare organizations have been very vocal about getting more budgetary support to combat cybercrime," says Morgan. "IT budgets have historically allocated much less to security compared with other industries. 2017 marks the turning point. The continuation of hacks on hospitals — and especially the growth of ransomware attacks — has heightened awareness at the C-suite and the board level, where it needs to be. As a result, we expect a major uptick in cybersecurity spending from this vertical."

With more budget at their disposal, healthcare organizations may not be such a bad place for cybersecurity engineers to work at after all.

Although ransomware attacks on healthcare organizations are expected to quadruple by 2020, training employees on security awareness and backup practices should reduce the number of ransoms that are paid out by hospitals — and minimize the post-hack disruption to the normal course of business and patient care.

A future with no more ransomware? Doubtful. But, the pain can be minimized. A new project holds out hope in the war against ransomware attacks. Read about it here.

About the Author

John P. Mello, Jr. is a freelance writer specializing in business and technology subjects, including consumer electronics, business computing and cyber security.

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

At Herjavec Group, we take our role as your trusted advisor in information security very seriously.

Information Security Is What We Do. Full Stop.

We are laser-focused on protecting the infrastructures of our customers globally and will take every measure possible to learn and engage with security experts worldwide to ensure we remain on the cutting edge of this rising threat landscape.

Dynamic IT 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 players, and excel in complex, multi-technology environments. Our service expertise includes Consulting, Installation & Architecture, Identity & Access Management, Managed Security Services and Incident Response. Herjavec Group has offices globally including across the United States, the United Kingdom and Canada.

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

Follow Us
Herjavec Group
@HerjavecGroup