Cyber Pulse: The State of Cybersecurity in Healthcare

A study on cybersecurity amongst Americans and Canadians working in the healthcare industry.

Introduction

In today's healthcare system, it has become increasingly critical for patient information to be properly processed and stored electronically. With the industry progressing toward a more tech savvy routine to improve patient care and accelerate communication of health records, the potential that information can be lost or stolen – ending up in the wrong hands of a cybercriminal – is increasing in turn.

As of January 1, 2018, there have been over 110 hacking/IT-related healthcare organization incidents affecting 500 or more individuals in the U.S. alone according to the U.S. Department of Health and Human Services[1]. New risks arise daily that don't only disrupt businesses continuity, but also put patient privacy at stake. As healthcare providers strive to protect patients from threats to their well-being, the importance of safeguarding the infrastructure of the organization – from electronic medical records to medical devices – is more important now than ever given the success cybercriminals experience today breaching healthcare organizations and gaining access or control of this information.

Underestimating the dangers associated with cybersecurity can disrupt business operations and even permanently damage the reputation of the company. In today's news headlines, a new data breach or some kind of cyberattack is making the news on a weekly, if not, daily, basis. This is even more prevalent for the healthcare industry, but the industry has many complex regulations and security measures to protect the privacy of patients, so why question cybersecurity?

To gain insight into what's happening in the healthcare industry when it comes to cybersecurity, Kaspersky Lab issued a survey. The research provides insight into the perceptions of healthcare employees in North America regarding cybersecurity in their workplace, including awareness of cybersecurity breaches, protection of sensitive information, cybersecurity awareness and training, and more. Kaspersky Lab commissioned the research firm Opinion Matters to conduct a survey of 1,758 employees based in healthcare organizations in the United States and Canada.

Through this research, the company aims to create a dialogue among businesses and IT staff in healthcare about the current state of awareness of cybersecurity among their employees, along with providing suggested proactive steps that can be taken to prioritize cybersecurity awareness through trainings and consistent education, aiming to prevent or minimize the next cybersecurity issue.

Key findings from the study include:

- Of those that experienced a ransomware cybersecurity attack in their organization, **81% of VSB, 83% of SMB, and 81% of enterprise**, employees admit to having had experienced **up to four** ransomware cybersecurity attacks.
- More than **1 in 4 (27%)** healthcare IT employees admit they are aware of ransomware cybersecurity attacks to their employer within the past year.
- Of those that stated they were aware a ransomware cybersecurity attack had taken place in their organization, **a third (33%)** noted that this had happened more than once.
- Of those that stated they were aware a ransomware cybersecurity attack had taken place in their organization, **78% of respondents** in U.S. and **85% of respondents** in Canada stated their company had experienced up to **five attacks**.
- Over half **(57%)** of employees of VSBs said they would report a suspicious email to their employer's IT team, as opposed to almost three quarters of those working at SMBs **(74%)** and **79%** of employees working at enterprises.
- Nearly three quarters of respondents **(71%)** said that they care about having cybersecurity measures in place at their organization to protect patients.

Research Methodology

The quantitative study was conducted by research firm Opinion Matters via an online survey targeting 1,758 employees – in a variety of roles, ranging from doctors and surgeons, to admin and IT staff – working at healthcare organizations in North America in October 2018. The survey allowed Kaspersky Lab to collect market research on employees' opinions in the U.S. (1,004 employees) and Canada (754 employees) on cybersecurity breaches experienced, awareness and preparedness for the future at their healthcare workplace.

Throughout the report, businesses are referred to as either VSBs (very small businesses with 1-49 employees), SMBs (small & medium sized businesses with 50 to 249 employees) and enterprises (businesses with over 250 employees). Not all survey results are included in this report.

Research Findings

The State of Cybersecurity – Ransomware in Healthcare

One of the most notorious cyberattacks to impact the healthcare industry is the four-day WannaCry[2] epidemic, which knocked out more than 200,000 computers in 150 countries last year. In some hospitals, WannaCry encrypted all devices, including medical equipment, and some factories were forced to stop production. With healthcare-related data breaches like WannaCry making headlines in mainstream news outlets, the awareness of the vulnerabilities in the healthcare industry make these organizations an even bigger and easier target for cybercriminals, and a headache for healthcare IT staff to prevent and protect against.

WannaCry: One and a half years after the WannaCry epidemic, it continues to top the list of the most widespread cryptor families. This is especially alarming considering that a patch for the EternalBlue exploit used by WannaCry existed even before the initial epidemic in May 2017.[3]

Surprisingly, more than a year later, WannaCry ransomware continues to be a major threat, continuing to affect almost 75,000 users[4] as of the third quarter of 2018. As ransomware is not a new threat but continues to penetrate the healthcare industry today, Kaspersky Lab took a look into awareness about ransomware among healthcare employees. As a result, more than one-in-six (17%) respondents said that they were aware of a ransomware cybersecurity attack to their organization in the past five years or more and 12% of respondents has stated that an attack had happened in the last two years.

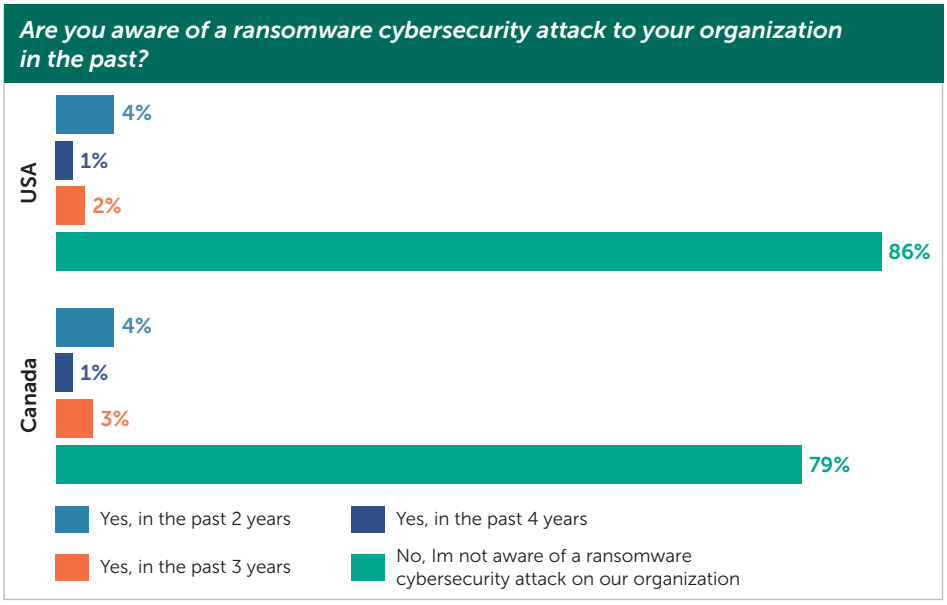
Ransomware

is a type of malware which can systematically encrypt files on a hard drive so it becomes difficult or impossible to decrypt without paying a ransom for an encryption key. This restricts access to an infected computer or mobile system in some way, and demands are made for the user to pay a ransom to the malware operators to remove the restriction.

According to the survey results, organizations are not always learning their lessons on cybersecurity protection the first time around after a breach. Of those that stated they were aware a ransomware cybersecurity attack had taken place in their organization, a third (33%) noted that this had happened more than once.

When it comes to the size of the organization, of those employees that were aware a ransomware cybersecurity attack had taken place in their organization, 81% of VSBs, 83% of SMBs, and 81% of enterprises, claimed that they have experienced up to four ransomware cybersecurity attacks.

According to the research, awareness of attacks has grown over the past couple of years. In the survey, 5% of U.S. and 6% of Canadian respondents said they were aware of a ransomware cybersecurity attack on their organization three or more years ago, however, the figures increased to 10% for U.S., and 15% for Canada over just the past two years. Although ransomware is not a new threat to healthcare, the results show that businesses do not have the right protection and security awareness through employee education to prevent it from happening.



Of those that stated they were aware a ransomware cybersecurity attack had taken place in their organization, 78% of respondents in U.S. and 85% of respondents in Canada stated their company had experienced up to five attacks. This is alarming, given malware attacks, such as ransomware attacks, can cost enterprises an average of $1.24M and SMBs $123K according to a Kaspersky Lab report[5] detailing the types of data breaches and their financial impact. It's hard to believe that a company would want to incur such unexpected, high costs over and over again. At some point, shouldn't they learn a lesson from the costly experience?

With a comprehensive security strategy in place, ransomware is preventable, but as we've found through this research, ransomware is continuing to plague the healthcare industry and disrupt patient care today. We are seeing recent evidence of this in hospitals, such as East Ohio Regional Hospital and Ohio Valley Medical Center, which both had to close part of their operations and turn to paper charts due to a ransomware attack over the course of a weekend that took down their computer systems[6]. It's clear that healthcare organizations need to review their security strategies and take a closer look at how they are protecting information.

"I believe ransomware attacks are probably the largest immediate threat since, if we're talking about hospitals or patient care facilities for instance, availability of equipment is critical to their function. Having machines rendered useless can severely impact a facility's ability to care for patients."

Brian Bartholomew
Senior Security Researcher,
GReAT, Kaspersky Lab

"Healthcare is a profitable target. Medical record data sells for far more on the dark web than financial data. Medical records can be used to support insurance and tax fraud, which can go undetected longer and generate more revenue for cybercriminals."

Jeff Becker
Senior Analyst, Forrester

Arm Yourselves For Healthcare's Cybersecurity War, Forrester blogs, November 9, 2018

Is Healthcare Information Really Protected?

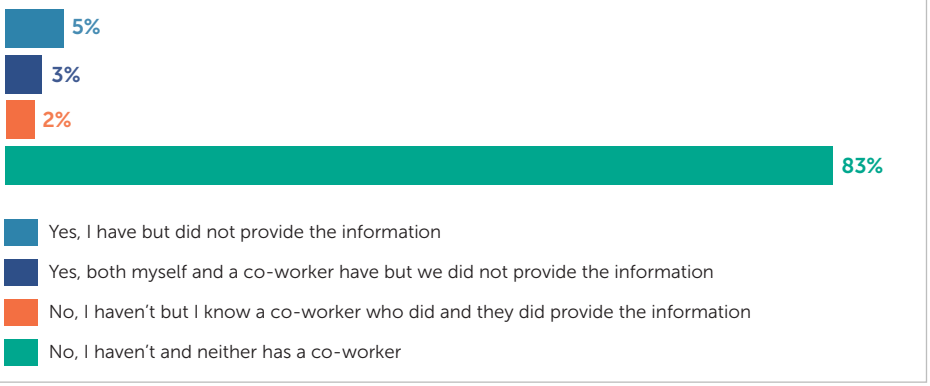
If financial information is stolen, banks will typically let customers know right away through an alert, but in the healthcare industry if patient medical records are compromised, it can take months[7] to find out about a breach, making it difficult for patients to manage and protect their own health information, or PHI.

Although many healthcare organizations allow patients to independently track and manage health information, are they securing, alerting and managing this information safely if a cyberattack occurs? According to a Kaspersky Lab study[8], 88% of businesses collect and store their customers' PII, and 86% collect and store employee PII. In order to understand how patient PII or e-PHI is being breached, Kaspersky Lab asked employees of healthcare organizations what they typically do when asked to provide PHI or access to information through system credentials.

Seventy-three percent of respondents said if they received an email at work from someone who they weren't familiar with asking for PHI or system credentials (passwords / logins) they would report it to their IT team. It is a good sign that employees are informed to report suspicious emails requesting data; however a sixth of respondents (17%) said they would not do anything in this situation. This proves that there is still some confusion when it comes to what to do in this type of situation. When analyzing the size of the companies these employees work for, the larger the company, the more informed and skeptical employees are of handing over information. Over half (57%) of employees of VSBs said they would report the email to their employer's IT team, as opposed to almost three quarters of those working at SMBs (74%) and 79% of employees working at enterprises.

Although employees claim they are very willing to report requests for PHI or system credentials, 17% of respondents admit they or their co-worker have responded to a third-party vendor email request at work to share patient information providing the requested e-PHI.

Have you or a co-worker ever responded to a third party vendor email request at work to share patient information providing the requested e-PHI?



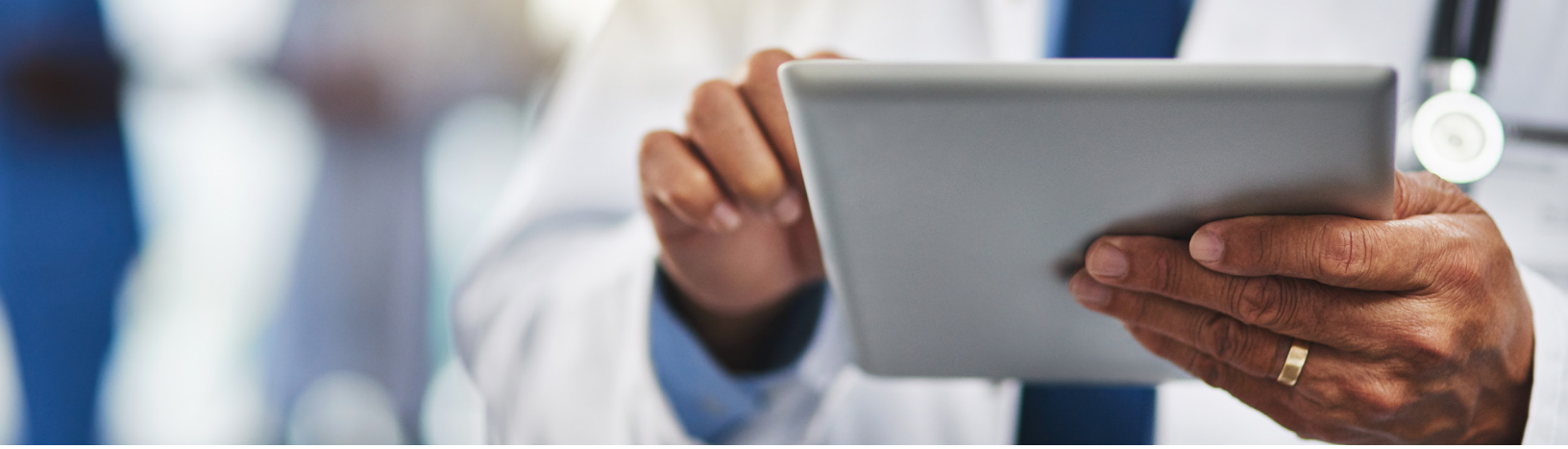
Protected health information (PHI)

under the U.S. law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked back to a specific individual. For example, a medical record, laboratory report, or hospital bill would be PHI because each document would contain a patient's name and/or other identifying information associated with the health data content.

Electronic protected health information (e-PHI)

refers to any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form.

Covered Entities recognized and regulated under HIPAA are 1) health plans 2) health care clearinghouses and 3) health care providers who electronically transmit any health information.



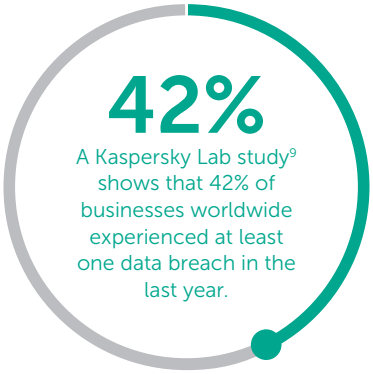
So who is most aware and what organizations are most likely to provide information?

- The findings show that medium sized organizations are more likely than VSBs and enterprise organizations to have employees who have responded to a third-party vendor email request at work to share patient information providing the requested e-PHI.
- When taking a deeper look at regional differences, employees in the U.S. (76%) are more likely to report an email to their employers IT team compared to those working in Canada (69%).
- A fifth of Canadian respondents (20%) said they or a co-worker they knew have responded to a third-party vendor email request at work to share patient information providing the request to e-PHI.

Over a third of doctors said they had, or knew a co-worker that had, responded to a third-party vendor email request at work to share patient information providing the requested e-PHI.

Why Care About Cybersecurity at Work?

When a data breach occurs, it not only results in a costly recovery burden, now at $1.23M on average for enterprises, but it can also impact the company's reputation, customer privacy, and even severely impact employees' careers. Of businesses globally that experienced a data breach in the past year, nearly one-in-three (31%) have led to employees being laid off from their jobs.



After analyzing employee awareness of sharing PHI and system credentials, Kaspersky Lab took a deeper look into why employees care about strong cybersecurity strategies at their workplace. As a result, nearly three quarters of respondents (71%) said that they cared about having cybersecurity measures in place at their organization to protect patients.

Respondents also expressed other reasons as to why they care about having cybersecurity measures in place at their organization. For example, three out of five people (60%) claim they care because they want to protect people and organizations they work with. In addition, nearly a third of respondents (31%) said they cared about having cybersecurity measures in place at their organization as they didn't want to lose their job as a result of not having appropriate cybersecurity measures.

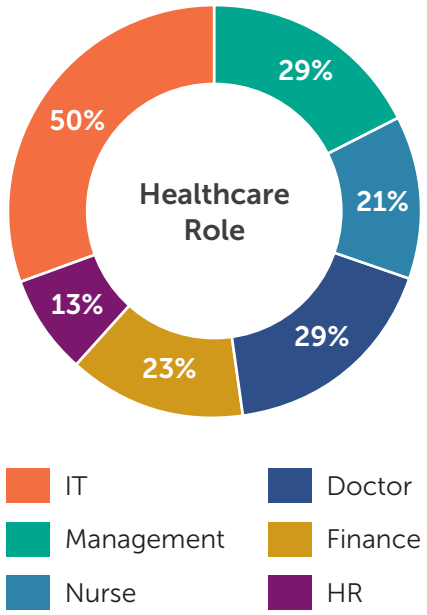
Confidence in Cybersecurity

The consequences of a weak cybersecurity program in the healthcare industry are crippling. From phishing[10] to distributed denial of service (DDoS) attacks and even more complex targeted malicious attacks, the study shows that healthcare organizations need to improve cybersecurity effectiveness and awareness among their staff.

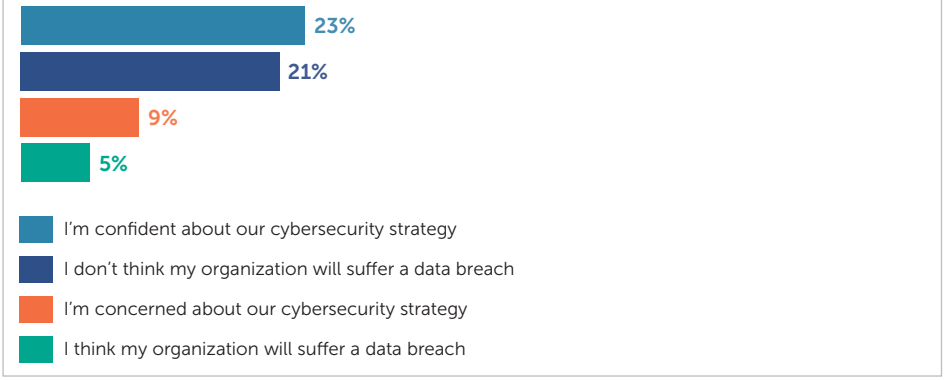
With cyber threats continuing to penetrate healthcare organizations on a regular basis, employees seem to have a false sense of security when it comes to what the future will hold, with just over a fifth of respondents (21%) who said they didn't think their organization would suffer a data breach in the forthcoming year. According to the findings, the larger the company size, the more confident respondents were about their organization cybersecurity strategy (VSBs – 16%, SMBs - 20%, enterprises – 27%).

Although some employees are confident, others can't say the same. In Canada, confidence about cybersecurity strategies is lower than in America – with 18% of Canadians saying they were confident about their organization cybersecurity strategy, as opposed to over a quarter of respondents (26%) in the U.S. Looking deeper into what employees are not confident about being secured, only 14% of respondents said their organization has enough cybersecurity protection for connected medical devices, while one in ten respondents (11%) said they needed better protection for employees to safely work remotely.

Employees who are confident in their organization's cybersecurity strategy for 2019



Which of the following, if any, reflect your thoughts about your organization in the forthcoming year?



"A 2018 national audit of healthcare preparedness found that only 45 percent of businesses followed the NIST Cybersecurity Framework. Furthermore, over half of all connected medical devices are considered "at risk" of security compromise."

Jeff Becker
Senior Analyst, Forrester

Arm Yourselves For Healthcare's Cybersecurity War, Forrester blogs, November 9, 2018

So what do healthcare organizations need to do to improve their security strategies?

"Segregation of networks is a first step. Anything critical should not be directly connected to the internet," said Bartholomew. "Secondly, having a complete backup / recovery plan in place is crucial. If something were to happen, recovering from the attack should be possible. Thirdly, user awareness and a good antivirus product would also be key. Teaching the users what ransomware looks like, what it does, and how to handle an incident can mean the difference between one system going down or all of them."

As businesses look to boost confidence in cybersecurity, it's important to understand what type of strategy is in place. For example, a compliance-driven program – one meeting the requirements of IT regulations – and a security-driven program are two different strategies. Security is risk based and compliance is meeting the requirements of the organization. A strategy led by compliance will not always include protection against the variety of cyber threats that exist today. Having antivirus software installed is good, but a multilayered approach to security is often necessary to fully protect an organization's environment. A security driven, multilayered approach would include endpoint security, but add proactive risk assessments and response, active monitoring and analysis of a network in a security operations center (SOC), threat intelligence, and more.

As a result, business leaders and IT security staff need to work together to prioritize cybersecurity in the workplace to properly manage the risk. This means investing in the design of a program that includes solutions and services that best fit the organization's needs, meets compliance guidelines as well as teaches employees about cybersecurity so that it is strong enough to fight off potential attackers.

Healthcare organizations don't have to continue to suffer from cyberattacks. Below are best practices for IT security teams:

- *Regularly update the operating systems on all computers on your network to the latest version.*
- *Use security solutions with dedicated anti-ransomware technologies.*
- *Make regular backups of important information and keep several copies in different places.*
- *Maintain control over the network by restricting access to information for employees that do not need it.*
- *Don't pay the ransom. It doesn't guarantee you will get your data back and it encourages this criminal business model.*
- *Continuously raise awareness about modern cyber threats through trainings and reminders of security protocols.*

Conclusion

As cybersecurity attacks continue to impact and influence businesses in the healthcare industry, the study clearly shows that more works needs to be done in security strategy awareness amongst employees and protection against existing threats.

In addition, organization leaders and IT staff must inform employees of cyber breaches –properly and in accordance with their hierarchy and role in the workplace. IT staff and leadership teams need to also work together to ensure employees are aware of the protocols for security at their organization to avoid cyberattacks that are preventable, such as social engineering with phishing emails. This can be accomplished through regular trainings for employees and communicating the latest cyber threats – along with best practices and reminders of protocols – so employees are well informed. IT teams should also conduct, on a regular occurrence, security testing/ simulations within the organization to better understand employee strengths and weaknesses when it comes to cybersecurity.

Another element for consideration is that legacy software can present a major threat to healthcare devices and systems. The only way to truly address cybersecurity safety in healthcare is to arm the business with proper cybersecurity solutions in place, ensure leadership is on board with the cyber strategy and supporting it financially, at the same time as making sure employees are educated to avoid the risk of human error.

This research shines a light on the importance of healthcare organizations checking on their "cyber pulse" to ensure they are proactively promoting cybersecurity awareness among employees and are prepared for a potential cyberattack. Kaspersky Lab is committed to helping people and organizations understand the risks of cybersecurity and what is necessary to empower employees and protect businesses. Kaspersky Lab will continue to research and investigate this industry issue to keep the healthcare community informed.

"I think after some of these attacks have happened, awareness of the impact has increased at the top levels and things are finally being done to help mitigate the threats. You're never going to get rid of the threat all together, but having budget / support / mandates to fix certain things can help significantly in the long run."

Brian Bartholomew
Senior Security Researcher, GReAT, Kaspersky Lab

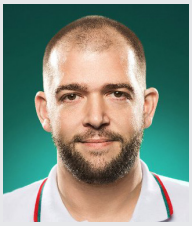
"The outside world moves quicker than healthcare security teams. As external threats continue to barrage healthcare, healthcare security leaders need to also worry about insider threats — both from malicious individuals intentionally accessing or leaking sensitive patient data as well as unwitting employees who accidentally leak data or violate security policy."

Salvatore Schiano and Chris Sherman
Forrester

The US Healthcare Security Benchmark 2017 To 2018

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company, which has been operating in the market for over 20 years. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.



Brian Bartholomew

Senior Security Researcher, GReAT, Kaspersky Lab

As a Senior Security Researcher, Kaspersky Lab North America, Brian is responsible for reverse engineering malware and tracking actors focused on cyber espionage or APT. Brian brings more than 15 years of malware analysis, cyber defense, penetration testing, and cyber operations experience.

1. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=2CA5B9BCF15730B92E03D1F7148AE689
2. https://securelist.com/wannacry-faq-what-you-need-to-know-today/78411/
3. https://securelist.com/kaspersky-security-bulletin-2018-top-security-stories/89118/
4. https://www.infosecurity-magazine.com/news/wannacry-still-alive-hits-75000/
5. https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-report-the-cost-of-a-data-breach-continues-to-grow-worldwide
6. https://healthitsecurity.com/news/weekend-ransomware-attack-interrupts-care-at-2-ohio-hospitals
7. https://www.fiercehealthcare.com/hospitals-health-systems/hackers-access-more-than-2-6-million-billing-records-atrium-health
8. https://www.kaspersky.com/blog/data-protection-report/23824/
9. https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-report-the-cost-of-a-data-breach-continues-to-grow-worldwide
10. https://www.wftv.com/news/local/data-breach-affects-42k-health-first-customers/872235812

Learn more about cybersecurity: **KL USA healthcare landing page**

usa.kaspersky.com
#KLCyberPulse

Kaspersky Lab, Inc.
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: NA-PR@kaspersky.com