Cyber Pulse: The State of Cybersecurity in Healthcare – Part Two

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

kaspersky

Introduction

As healthcare organizations continue to evolve and offer innovative information sharing systems for healthcare professionals and patients, it is more important than ever to be certain that sensitive patient information is processed and stored in the utmost secure electronic environments.

As of January 1, 2019, there have been over 200 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], and the number of incidents continues to grow every day.

On average, a breached healthcare provider will spend up to $408 per patient to recover their personal healthcare records and up to $1.75 million in advertising to help reverse reputational damages.[2] Not only will medical facilities endure financial losses and reputational damages when a cyberattack arises, they also face a more important issue: patient breach of privacy.

To have a better understanding of where the healthcare industry stands in their knowledge of cybersecurity, Kaspersky commissioned a survey to gauge the perceptions of healthcare employees in North America with regard to cybersecurity in the workplace. The survey offered several valuable insights, so many in fact that the findings were too vast to fit in one report.

In December 2018, Kaspersky revealed its first report, Cyber Pulse: The State of Cybersecurity in Healthcare, which focused on ransomware attacks in healthcare, how patient information is being protected, why it is important to consider cybersecurity in the workplace and cybersecurity confidence in the work place. Kaspersky is now issuing a second report which offers additional insights specific to healthcare industry perceptions on cybersecurity regulations, policy awareness and training.

In sharing the results of the complete survey data, Kaspersky aims to create an open dialogue among businesses and IT staff in healthcare about the current state of cybersecurity awareness among their employees. Additionally, the report will offer suggested proactive tips to prioritize cybersecurity awareness through trainings and consistent education, aiming to prevent or minimize future cybersecurity issues.

Key findings from the study include:

- **Nearly a third of all respondents (32%) said that they had never received cybersecurity training from their workplace but should have.**
- **Nearly 1 in 5 respondents (19%) said there needed to be more cybersecurity training by their organization.**
- **Almost a third of healthcare IT respondents (32%) said that they are aware of their organization's cybersecurity policy and have read it only once.**
- **2 in 5 respondents (40%) of healthcare workers in North America are not aware of cybersecurity measures in place at their organization to protect IT devices.**
- **Nearly half of respondents (49%) said they didn't know if Canadian patient healthcare information needed to stay in Canada.**

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 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

Cybersecurity Regulations in Healthcare

Due to the rise in healthcare industry cyberattacks, healthcare providers in the U.S. and Canada are lawfully bound to protect sensitive patient healthcare information (PHI). In the U.S., the Healthcare Insurance Portability and Accountability Act (HIPAA) requires measures that protect the PHI of patients, while its Canadian counterpart is the Personal Information Protection and Electronic Documents Act (PIPEDA).

With support from the government, Kaspersky was interested in learning more about how knowledgeable healthcare industry workers in North America are in regards to cybersecurity regulations.

According to the survey, nearly a fifth of U.S. respondents (18%) reported they didn't know what the HIPAA security rule meant. Additionally, less than a third of respondents (29%) were able to identify the correct meaning of the HIPAA Security Rule .

In Canada, nearly half of respondents (49%) said they didn't know if Canadian PHI needed to stay in Canada and only 1% of respondents correctly identified that all Canadian PHI data can reside in the U.S. with the exception of British Columbia and Nova Scotia.

These results bring to light the alarming amount of healthcare industry employees that do not understand the PHI laws their government puts in place to protect patient confidentiality. With a clear lack of knowledge about the regulations meant to keep PHI safe, healthcare workers are widening the gap for cyber attackers to breach their IT systems and exploit sensitive patient information.

"The results of the survey show that knowledge of regulatory requirements is missing or too low. In working with many clients and talking with others across the healthcare industry, the results are not surprising given the number of erroneous statements made about regulatory requirements and the misuse of regulations as the reason not to engage in an action that is actually permissible. The lack of awareness creates unnecessary risks."

Matthew Fisher,
Chair of Health Law Group
and Partner, Mirick O'Connell

Cybersecurity Awareness in Healthcare

For healthcare professionals, their top priority is to provide quality healthcare services to patients, and this includes maintaining the safety of the personal health information entrusted to them. However, research has found that just over half of businesses (52%) believe they are at cybersecurity risk from within their organization due to several factors including lack of employee awareness.[3] Furthermore, employee negligence in security breaches can even result in employee termination, as was the case in SingHealth's data breach which compromised the personal data of 1.5 million patients in Singapore due to poor system management and a lack of employee training among several other factors.[4]

1 in 10

employees in management positions saying they were not aware of a cybersecurity policy in their organization, but should be if there is one.

With these staggering statistics in mind, Kaspersky took a deeper look into healthcare professionals' cybersecurity policy awareness as well as their knowledge of the protection of internal IT devices.

Awareness as it applies to policy

Cybersecurity policy is a carefully researched statement written by IT decision makers about the protection of a company's crucial physical and information assets. Its purpose is to offer guidance on how employees can preserve the security of company data and technology infrastructure as well as how to properly report any suspicious activities.

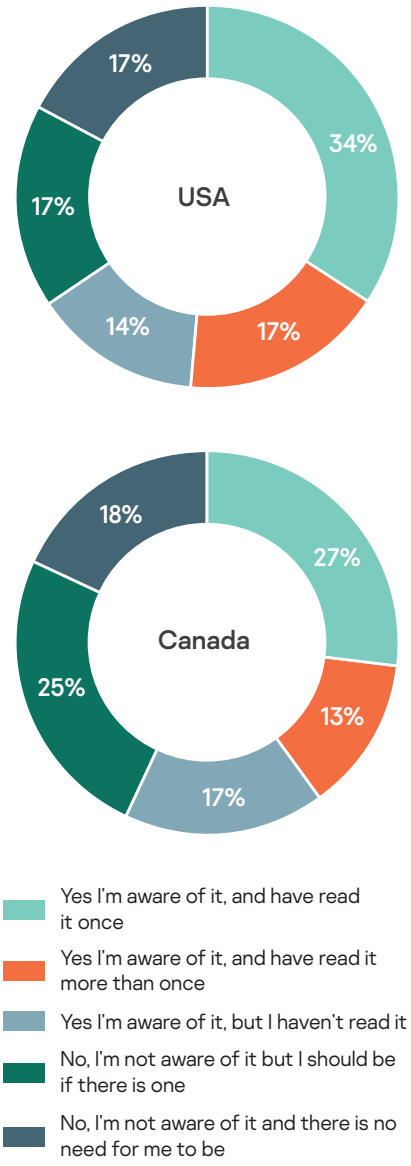
Over a fifth of respondents (21%) in North America admitted that they were not aware of the cybersecurity policy at their workplace, but felt as though they should be if there is a policy in place. Alternatively, nearly a third of respondents (31%) said they were aware of the cybersecurity policy at their workplace, but had only reviewed it once. Of the respondents that were aware of their organization's cybersecurity policy, 15% said they had never read it.

When breaking down the results by region, just over a third (34%) of respondents in the U.S. and just over a quarter (27%) of respondents Canada said they were aware of the cybersecurity policy at their workplace, but have only reviewed it once. Similarly, when looking at whether or not the size of the organization effected cybersecurity policy awareness, enterprise and medium organizations reported 17% of respondents who said they had read the cybersecurity policy at their workplace more than once, as opposed to only 10% of respondents from small businesses.

Individual roles within the organization were also surveyed, with 1 in 10 employees in management positions saying they were not aware of a cybersecurity policy in their organization, but should be if there is one.

In addition to policy awareness, Kaspersky's survey also measured cybersecurity protection of IT devices within healthcare organizations.

Are you aware of the cybersecurity policy at your workplace and have you read it?



Awareness of IT device protection

When looking at North America as a whole, 40% of respondents were not at all aware of cybersecurity measures in place at their organization to protect IT devices. When breaking the findings down by region, just under two thirds of U.S. respondents (64%) said they were aware of their organization's cyber security measures in place compared to just over half of Canadians (54%).

Small organizations had the highest percentage of respondents with a reported 53% who were not aware of cybersecurity measures their organization had in place, as opposed to 39% of respondents in medium and 36% of enterprise companies.

While human error is an honest mistake, it is clear there is a lack of cybersecurity awareness present in the healthcare profession. Consider the employee who cannot tell the difference between a phishing email scam and a real email from a bank, so they click on a questionable hyperlink. Employees are just one click away from unknowingly infecting their entire organization's IT systems with malware and other viruses. By being more cognizant of their employer's cybersecurity policies and security protections in place, employees can minimize the risk of costly and compromising mistakes as well as keep their job security intact.

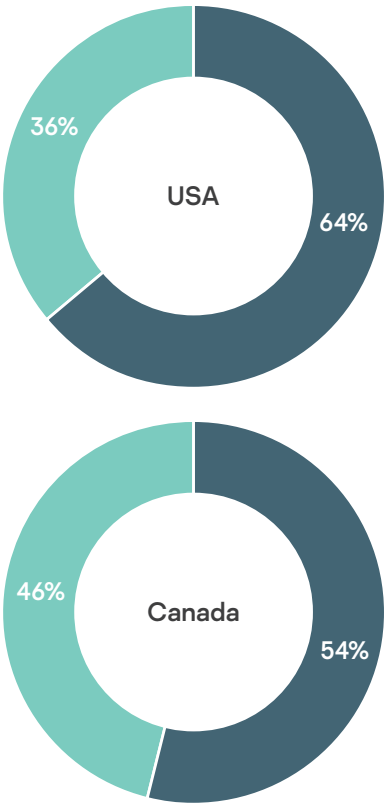
According to Brian Bartholomew, principal senior security researcher at Kaspersky:

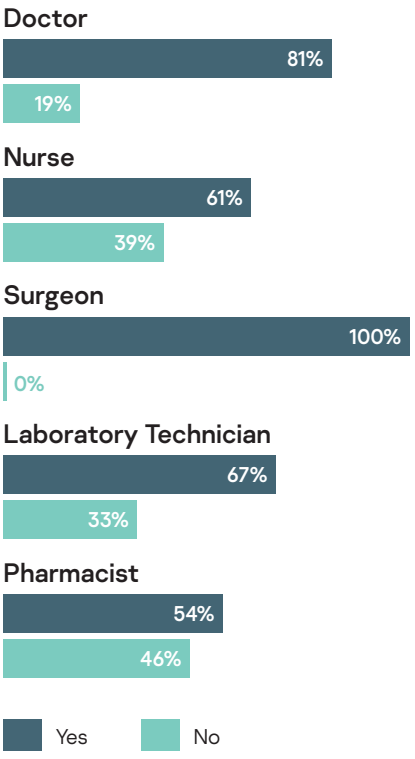
"Understanding your company's security policies, procedures and incident reporting channels is crucial to protecting not only the company's infrastructure, but also patient data. In addition, security awareness training aids an employee in understanding how an attacker thinks, what they're targeting, how to recognize attacks and what to do in the event one may occur.

Time is also an important factor in preventing the spread of some attacks. For example, if an employee is not aware of what a ransomware attack may look like and doesn't take necessary measures to stop the spread of such an attack, the entire network could be infected in a matter of minutes.

Employees should also have a general understanding of how a company's networks are segregated, especially in the healthcare industry. Knowing what network houses sensitive data and maintaining proper cyber-hygiene when on those networks can greatly reduce the exposure to that network, Just one employee browsing the internet mistakenly on a sensitive wireless network can inadvertently expose that sensitive data to the outside world."

Are you aware of cybersecurity measures in place at your organization to protect IT devices (ex: computers, laptops, tablets, iPads, mobile phones)?





Cybersecurity Training in Healthcare

The type of organization and amount of available resources where healthcare employees work will largely impact the scale of cybersecurity training; however, a lack of training should not diminish cybersecurity's importance. With attacks on personal data via healthcare IT systems on the rise, cybersecurity training, including an understanding of what to look for and actions to take, is vital for healthcare employees to regularly participate in and keep a pulse on.

To gain a better understanding of the scale of cybersecurity training healthcare professionals are provided, Kaspersky surveyed respondents for insight.

Nearly a third of respondents in North America (32%) said that they had never received cybersecurity training from their workplace, but think they should have.

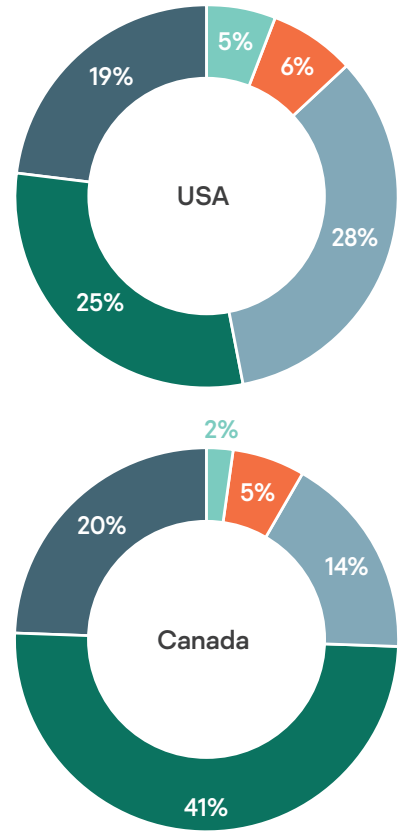
Of the respondents who did receive cybersecurity training, over one in ten (11%) said they have only received cybersecurity training from their workplace when they were hired and on boarded, with no additional or ongoing trainings. When looking further into the frequency of trainings, just over a third of respondents (38%) said they receive regular (at least once a year) cybersecurity training from their workplace and nearly 1 in 5 respondents (19%) said there needed to be more cybersecurity training by their organization.

When determining whether or not the size of the organization effected cybersecurity training, the survey results found that 35% of respondents working for small businesses and 36% of medium sized businesses said they had not received cybersecurity training but should have, compared to only 29% of respondents working for enterprise sized companies.

In comparing respondents by region, it is clear to see that Canada is behind on cybersecurity training in healthcare when compared to the U.S. Over 24% of respondents in the U.S. noted they had never received cybersecurity training but should have, compared to 41% of respondents in Canada when asked the same question.

If healthcare employees are not effectively trained on cybersecurity regulations and procedures for their organization, how are they expected to spot a cyberattack or communicate to their internal IT department if an attack strikes? Organizations of all sizes and resources must ensure that their staff can adequately recognize malicious attacks and who to report them to. It is also imperative that healthcare enterprises employ IT leaders who prioritize cybersecurity trainings and regularly update employees with new strategies and policies to minimize the potential impact of a breach.

Have you received cybersecurity training from your workplace?



"There is clearly an opportunity to develop cost-effective cybersecurity training to engage all employees in relevant trainings to identify, interpret and plan for cyberattacks, including providing consistent and standard processes and procedures."

Sandy Becker, Professor,
Rutgers School of Management
and Labor Relations

Conclusion

As we look towards the future of improving cybersecurity in the healthcare industry in North America, it is imperative that healthcare IT leaders keep pace with the increasing number and sophistication of cyber threats that could target their organizations. In order to do so, several measures must be in place to ensure sensitive patient information is protected and that IT systems are able to defend against potential future data breaches.

First, it is essential to establish a skilled IT security team who understand your organization's unique security risks as well as the proper security tools required to keep your IT environment safe and secure. With a growing number of private patient information files being electronically transferred daily, it is more important than ever to be sure that patient information is being safely processed and stored.

As the data highlights, there is a severe lack of cyber security training for healthcare employees which leaves a significant opening for cyberattacks as well as missteps in human error. To combat this, IT security leaders must implement ongoing cybersecurity trainings for employees of all levels, specializing the trainings based on role and the most common threats employees might be challenged with. IT security leaders should also be privy to the variety of training options that they can offer employees from bringing in a consultant, to webinar services, one-day trainings and more.

Finally, having a clear, company-wide cybersecurity policy in place is vital in order to have employees across an entire organization following the same guiding principles. Once a policy is established, it will remain important to proactively communicate the policy to employees on a regular basis to increase awareness in order to minimize future threats. As with any company policy, annual reviews and updates should be made to a cybersecurity policy in order for the guidelines and recommended actions to remain current.

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 is committed to helping people and organizations understand the risks of cybersecurity and what is necessary to empower employees and protect businesses. Kaspersky will continue to research and investigate this industry issue to keep the healthcare community informed.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative 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 technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at **www.usa.kaspersky.com**.

1. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=2CA5B9BCF15730B92E03D1F7148AE689
2. https://healthitsecurity.com/news/hospitals-spend-64-more-on-advertising-after-a-data-breach
3. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
4. https://www.zdnet.com/article/employees-sacked-ceo-fined-in-singhealth-security-breach/

www.kaspersky.com