CHIROPRACTIC ECONOMICS

YOUR PRACTICE PARTNER

Issue 13: August 18, 2024 chiroeco.com

NEW DC TECHNOLOGY

THE IMPACT OF COMPUTING AND THE IMPORTANCE OF CYBERSECURITY MEASURES

How to keep your valuable data secure and your practice safe

By Thiery Gagné

THE IMPACT OF COMPUTING AND THE IMPORTANCE OF CYBERSECURITY MEASURES

How to keep your valuable data secure and your practice safe

BY THIERY GAGNÉ

TIME TO READ: 6-7 MIN.

THE TAKEAWAY

You must take cyberattacks seriously, adopt safe behaviors on the web and recognize signs that could put your clinic in danger and lead to the loss of your valuable data.

COMPUTING HAS REVOLUTIONIZED ALMOST EVERY FIELD OF MODERN SOCIETY. Not a day goes by without us interacting with an electronic device connected to the internet. The advent of artificial intelligence (AI) and the Internet of Things (IoT) has drastically intensified this trend, with previously simple items now brimming with sensors and connected to the internet. You likely have equipment in your clinic using such sensors. Indeed, it's no longer uncommon to update your vacuum cleaner, reset your washing machine or restart your connected lighting system after a power outage.

The key takeaway from this technological revolution is that all devices connected to the internet form a link in a vast network, where actors of all kinds are present. Thus, a robot vacuum may seem like an innocuous device, but it can serve as a gateway to all other devices connected to the same internet network. Therefore, the incredible versatility of the internet

Using a virtual private network ensures data transmission to employees without said data being intercepted by a malicious entity or even the government.

353 MILLION

353,027,892 people were impacted by data breaches in 2023.

Source: Identity Theft Resource Center 2023 Annual Data Breach Report

and the network structure connecting all our devices also constitutes an increased security risk that many people try to exploit daily.

In every business, all employees must be vigilant since all devices, sensitive or not, are interconnected. A fortress with 100-meter-high and 30-meter-wide walls will be useless if a small hole allows free passage. The same principle applies to any institutional computer network, including that of your clinic. This is especially true for all electronic health record (EHR) systems allowing remote connections.

How to effectively protect against cyberattacks

The first measure relates to employee training and awareness. Capsules illustrating the typical profiles of approaches used by web fraudsters and criminals can be implemented. Moreover, many organizations now test their employees by sending fake fraudulent emails they must identify. At the end of a semester, each employee has a score related to the proportion of fake fraudulent requests identified, which is very useful for identifying who in the company is most likely to unintentionally disclose sensitive information to malicious entities.

A second very useful tool is the use of virtual private networks (VPNs) to ensure remote access to the clinic's information technology (IT) resources. Indeed, telework is ubiquitous nowadays, and many employees need to access more or less sensitive information stored on the clinic's computers. Using a VPN ensures data transmission to employees without said data being intercepted by a malicious entity or even the government.

Companies using the cloud must also be very cautious. Even if they outsource their data storage to external entities, such as Amazon (AWS) or Microsoft (Azure), managing access keys to the data remains critical. Moreover, choosing a data architecture that meets business needs and complies with local jurisdiction is essential. For instance, it is not wise to have only one data partition accessible to all employees. Fortunately, all major cloud providers offer comprehensive tools to structure and manage data efficiently and quickly. However, these tools are quite complex, and a cybersecurity expert should ideally be present to set up the initial data environment and preferably manage it.

When choosing a cloud-based EHR system, it is imperative to call upon a serious provider with the necessary infrastructure to support you well. Indeed, prevention is better than a cure! Having an employee tasked with maintaining data integrity can save a company a lot of money by preventing attacks that could potentially paralyze operations for several days, if not lead to data loss.

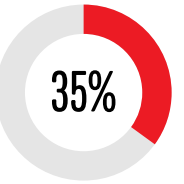
Finally, another way criminals try to access sensitive information is through software containing malicious modules. This aspect is even more critical for clinics with employees

Choosing a data architecture that meets business needs and complies with local jurisdiction is essential.

who need to download modules and tools from the web to do their work. Sometimes, the threat doesn't even come from the software itself but from the platform from which it is downloaded. In any case, the best way to protect against this type of intrusion is to monitor and control which applications are used by employees. To do this, a clinic can set up an internal application "market" where only software and libraries validated and tested by cybersecurity experts are present.

35%

Email is the most common vector for malware, with around 35% of malware delivered via email in 2023.



Source: Verizon 2023 Data Breach Investigation Report

Final thoughts

Realistically, even with the best control, it is possible that a virus will be inadvertently introduced into a company's IT infrastructure. Thus, having excellent antivirus protection and a robust firewall is very important and complements the cybersecurity strategies mentioned so far. Many excellent tools are available on the market, including the Defender for Business software suite offered by Microsoft. Don't hesitate to ask your EHR provider about all the measures they have in place to ensure the protection of your data hosted in the cloud.

THIERY GAGNÉ is a young data scientist, consultant and lecturer holding a bachelor's degree in business administration with a specialization in business intelligence and a Master of Science (MSc) degree in data science and business analytics from HEC Montreal. He is also an ad hoc consultant for Platinum System. For more information on PLATINUM2.0 cloud-based EHR software, contact 888-808-4898, sales@platinumsystem.com or visit platinumsystem.com.