www.solidtech.ca
780-451-2060
9470 51 Ave NW #201
Edmonton, Alberta T6E5A6

Health Care & CYBERSECURITY

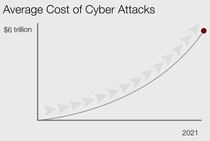
Presented By:

SOLID technology.solutions.inc

A longstanding assumption in the cybersecurity world is that it is not whether an organization is the target of an attempted breach or attack but when such an attack will happen. One of the many unfortunate side effects of the global pandemic is a disturbing increase in hacked and breached data that has been exposed to cyber thieves due to weak work-from-home protocols and data protection measures that are out of date or simply underpowered. Some clear trends that are emerging as we move into 2021:

- **Remote workers are primary targets of cybercriminals**
- **Cloud breaches will continue to rise**
- **The increased presence of 5G will create new issues that will challenge cybersecurity systems by creating new footholds that cybercriminals can exploit.**

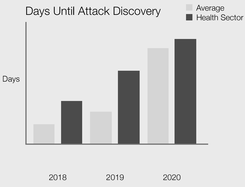
Some interesting facts that underlie these global trends:



The cost of cyberattacks is projected to hit $6 trillion in 2021, double what it reached in 2015

Healthcare is the sector that suffers the highest industry cost from data breaches

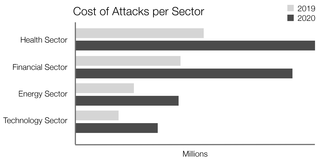
$7.13 million was the average cost of a data breach in the healthcare industry, an increase of 10 percent over 2019; this is more than breaches in the energy sector, financial services sector, and technology sector, and almost twice the global average



68 percent of business leaders report that their cybersecurity risks are increasing in 2019 before the pandemic and work-from-home created even more loophole for cybercriminals to attack

In 2020 alone, data breaches exposed over 36 billion records to malicious intent

73 days was the average time in 2020 from discovery to full containment, though both numbers are significantly higher in the healthcare sector.

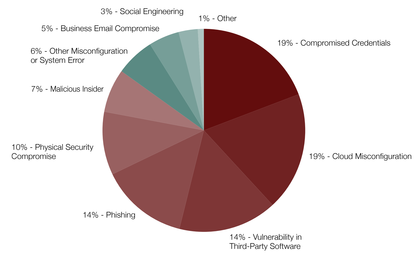


It is time to evolve your organizational defences. Gone are the days when a robust firewall and virus scan are all that is needed to sleep soundly at night. Today's cybercriminals are patient. They probe, explore, looking for a weak spot in your network. Then they watch, collecting data, gaining knowledge into workflows, and learning more and more about your business every day. This criminal monitoring can go on for months or even years without your system ever alerting you of the presence of an intruder.

Until one day, when it is too late, and your organization finds itself confronting a ransomware attack or devastating breach of personal data. In 2020, client personally identifiable information (PII) was the target of a full 80 percent of data breaches, following by intellectual property (32 percent), anonymized client data (24 percent), other organizational data (23 percent), and employee PII (21 percent).

How do cybercriminals attack your system?

The unfortunate answer is by more and more methods every year. As IBM showed through its 2020 "Cost of a Data Breach Report," your system is vulnerable to a plethora of breach points:



The bottom line is clear: Today's IT security must be designed to keep up with the cybercriminals, which means that it should provide 24/7 active application-level monitoring (including document scans) reinforced by a virtual PC that allows your security provider to isolate, open, and execute any suspicious files that are identified as potential threats. It should provide 24/7 monitoring of suspicious probes or enquires, which are often the first signs that your network has caught the attention of cybercriminals. And it should be maintained at the highest level of security upgrade; allowing your defences to become out-of-date for even a short time allows cybercriminals to breach your system and lay in wait.

Given that human error is still at the root of most cybersecurity breaches, your security plan must also include ongoing training for all your employees. Regular and detailed updates ensure that everyone with your organization is familiar with the signs that something unusual is happening. With cybercriminals moving more and more to sophisticated phishing schemes and malicious hyperlinks, have your staff fully aware of possible threats and response protocols is a critical first line of defence in any cybersecurity plan. As the 2020 Gartner report on "The Urgency to Treat Cybersecurity as a Business Decision" stated clearly: "Money alone does not solve the problem, and a major component of future cybersecurity success is the engagement of executives" and staff from all levels of an organization.

Make your IT security a core business decision in 2021. Contact SolidTech today to discuss your current cybersecurity readiness level and explore options that make sense for your business outcomes and budget.

SOLID technology.solutions.inc

www.solidtech.ca
780-451-2060
9470 51 Ave NW #201
Edmonton, Alberta T6E5A6