Alberta Doctors' Digest

What exactly are cyberattacks?

Technology has revolutionized the world for businesses and individuals alike, and the past twenty years in particular have seen monumental shifts in human behavior directly linked to technological advancements. From the way we shop to the way we access bank accounts and book holidays, everyday life has changed fundamentally.

However, while the technology revolution has brought with it unparalleled convenience and choice to millions across the globe, it has done the same for the criminal underworld. It is now far easier and far more lucrative for criminals to ply their trade digitally rather than physically. Cyberattacks are the modern crime, and cyber insurance is one of the ways to protect against them.

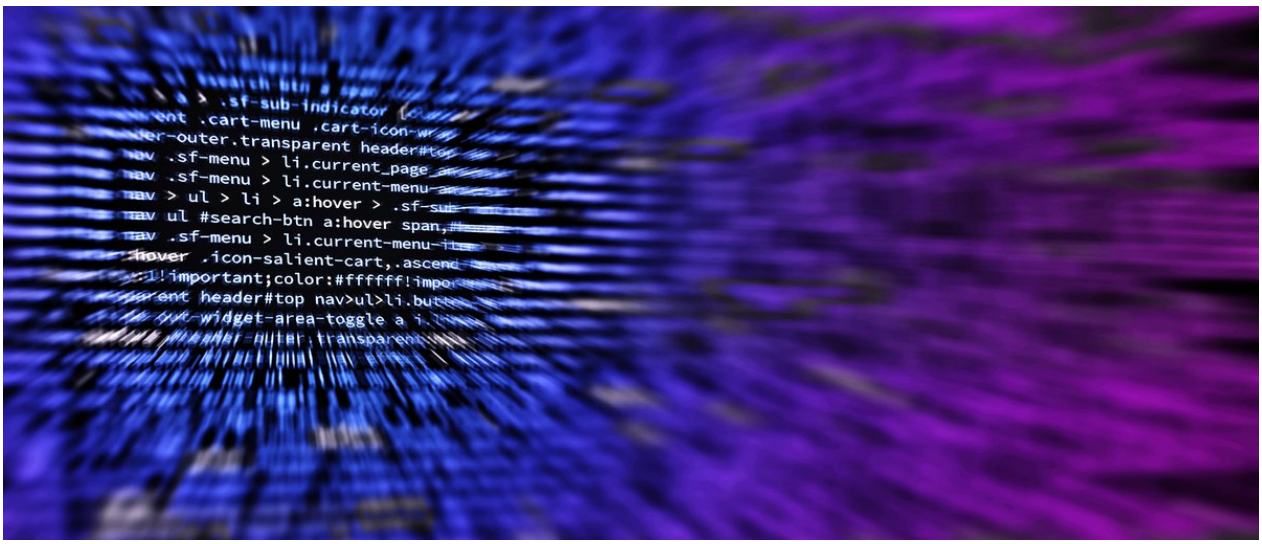
Today it’s clear that the vast majority of cyber events tend to cause financial loss to businesses themselves as opposed to the third parties with which those businesses deal.. These events fall into three broad categories.

Theft of funds

This is straightforward theft of money from a company’s bank account. The fact that nearly every business can now move its money around electronically and remotely means that it is much easier to steal. Criminals no longer target physical banks – they target online accounts. And if a business has somehow been negligent in allowing this to happen, the bank will not reimburse them.

Theft of data

Data is valuable, and if something has value, it is worth stealing. Identity theft has reached record levels around the world, and in order to commit identity theft, criminals need data. Seemingly innocuous information such as names and addresses stored on a computer network can be worth more money than you think.



Businesses have an incredibly high dependency on their systems, and criminals know that (Photo credit: Pexels PixaBay.com)

Damage to digital assets

In order to operate, businesses now have an incredibly high dependency on their systems, and criminals know that. By either damaging or threatening to damage a firm's digital assets, attackers know that they can extort money from the victim who might prefer to pay a ransom rather than see the business grind to a halt. And even after paying up, the victim is often left with systems that are unusable and costly to fix.

In some cases, there may be no financial incentive for the attacker at all. In the same way that criminal damage to property doesn't always have a financial incentive, damage to digital assets doesn't need one either. Claims for theft of funds are actually very easy and quick to quantify, but for theft of data claims, the financial impact can vary depending on the nature of the data compromised and how much of it was stolen.

The costliest part of a cyber event is often responding to the incident. For example, if an attack has compromised a company's computer network, then IT specialists are needed to stop the attack, protect against further immediate threats, and work out what has been stolen. There is then a financial cost associated with limiting reputational damage, notifying clients or customers whose data has been stolen, and offering them identity theft protection solutions if necessary.

Damage to digital assets claims can be easy to determine if there is an extortion demand that the victim has paid (the amount of the claim is the cost of the ransom), but the cost is more difficult to assess if we're talking about the cost of IT specialists to rebuild systems or data – which might only be calculated after the work is completed.

While extortion in the form of ransomware has been one of the fastest growing forms of cybercrime in recent years, social engineering scams have also increased dramatically, and they tend to be more severe. So-called "CEO fraud," where fraudsters impersonate

the CEO of a company (or other senior executives) and email instructions to staff in the accounts department to transfer funds to criminals' bank accounts, has been incredibly successful and a huge source of claims by businesses.

The key point underpinning each of these types of cybercrimes is that there is a direct financial loss to the victim business, which can be transferred with a cyber insurance policy.

For more information on cyber liability insurance, please enquire to Westland Affinity Group Insurance Services (formerly Mardon Group Insurance) at 1.866.846.4467. Be sure to ask about the discounted rates for AMA members. Westland also offers commercial office, directors' and officers' liability, and entity malpractice liability to AMA members.

Banner image credit: Darwin Laganzon, Pixabay.com