7 Things Companies Do After A Cyber Breach That You Should Be Doing Now

In a post-pandemic society, our reliance on technology has increased at a rate that no one could have predicted. Unfortunately, the flip side is that the sophistication and frequency of cyber-attacks have also risen considerably due to the increased opportunity. This article will provide an overview of what a cyber-attack is and the ways you can be breached, followed by steps that you should take now to minimise the potential impact of cybercrime on your business.

What is a Cyber-Attack?

A cyber-attack is when a criminal fraudulently accesses your online data and uses it for their own personal gain. The main ways they achieve this are:

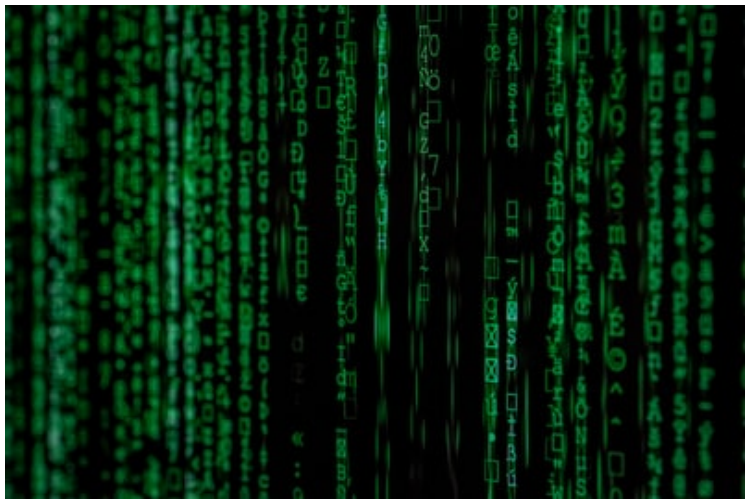
Theft of funds – where attackers steal money directly from the company, many transactions are now done online, so they have seized this opportunity to intercept capital.
Theft of data – data is valuable, and criminals know this! Even if the information is not specifically beneficial to them, e.g., for identity theft, they know that it is valuable to you, so they may attempt to take it hostage and demand that you pay a ransom for its release.

Damage to digital assets – where attackers use ransomware to block a business' systems and then demand that the company pay a ransom. As well as holding data hostage hackers can use ransomware to block your company systems so that unless you pay their ransom business will grind to a halt.
Baiting – where attackers trick you into downloading content such as music that infects your computer with malware.
Phishing – where scammers pose as a trusted entity to trick the user into giving them sensitive information such as credit card details or tricking them into sending money.

The effects of cyber-attacks on a business are usually financial and/or reputational, both of which are hugely detrimental to any SME but even more so in the scale-up community.

The 2021 Hiscox Cyber Readiness Report revealed that compared with last year:

"The average business surveyed now devotes more than a fifth (21%) of its IT budget to cyber security, a jump of 63%."



This demonstrates that businesses are aware of the increased risk, but before you call your insurer in a panic, let's look at some of the things you can do to improve your cyber security. It's essential to do this before taking out a more comprehensive cyber insurance policy because the increase in demand has meant that cyber insurance is getting more and more expensive.

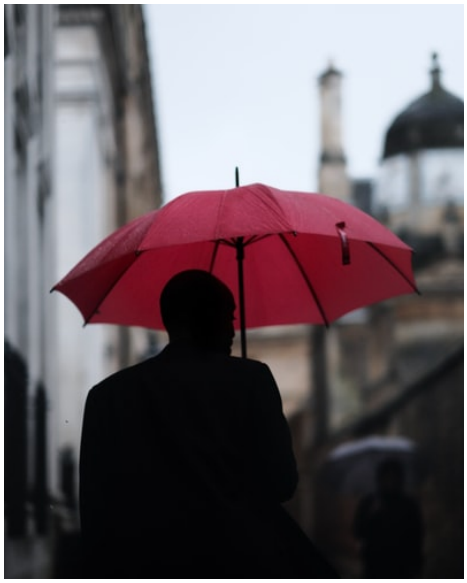
7 Steps to Improve Your Cyber Security

1. **Educate Staff** – this one seems obvious, but because cyber-attacks are constantly evolving, it's essential to keep updating your staff training. Over 60% of cyber incidents directly result from human error, so by educating your staff, you are significantly reducing your risk of a cyber-attack. Attacks such as phishing emails and scam emails are some of the most critical areas that employees may be susceptible

to, so it's fundamental that you continually train them to recognise these sorts of emails.

2. **Secure/ restrict all employee devices** – it's not so easy to limit the use of employees' own devices when working from home; however, this should be done to the best of your ability. It is also essential that any devices staff use for work are end-to-end encrypted.
3. **Back everything up** – in cases where data is stolen/ held hostage or even deleted, it will have considerably less impact if all your data is backed up. Again, this is another point that looks obvious, but it's so easy to forget to back up all your data continually.
4. **Invest in the best antivirus technology** – the better your initial defense against viruses and malware, the less likely you will suffer a cyber-attack.
5. **Use multifactor authentication** – this provides an additional layer of protection besides passwords. It would be best to ensure that all passwords meet a minimum standard of strength, such as utilising lowercase and upper-case letters, numbers, and symbols.
6. **Update your software regularly** – software updates are also referred to as service patches because they essentially patch up holes in the system that leave you vulnerable to attack. If you do not update your software regularly, you are more likely to be breached because there are more holes in your system.
7. **Have an incident response plan** – this will not prevent a cyber-attack, but it will help minimise the impact should you be breached. This would follow the steps of identifying the source of the attack, containing the attack, and then recovering from the attack. A good response plan will significantly impact how damaging a cyber-attack would be to your business.

What Does Cyber Liability Insurance Cover?



After reading that list, you may wonder what you will need cover for once you've taken all those steps! *Unfortunately, you will never be 100% protected against a cyber-attack, so there will always be the necessity for some level of cover; Cyber criminals are continually developing new ways to attack your data, so you will constantly be exposed to some risk.*

As mentioned above, it is harder to prevent cyber-attacks when staff are working from home; in research carried out by YouGov in June 2021, it was found that 17% of businesses experienced more cyber-attacks since staff were working from home. We are not yet out of the covid-19 woods, so cyber security must stay at the forefront of our attention instead of being that thing businesses 'forget' about to save money.

Cyber insurance cannot prevent the attacks themselves, but it does minimise the effects on your business should you fall, victim.

First-Party vs. Third-Party Coverages

Most cyber insurance policies will cover both the first-party and the third-party financial and reputational costs of a cyber breach.

First-party cover in the case of a cyber breach: this covers the cost of investigating a cyber breach, loss of income, cost of restoration of systems, reputation management, etc.
In essence, the first-party cover is the costs faced by your business, i.e., the business that has been breached.

Third-party cover in the case of a cyber breach: this is to cover anything that results from a claim being made against you, e.g., the cost of legally defending yourself and damages and settlements.

Incident Response

Incident response is often the most significant and helpful part of an insurance product because the first few hours after an attack are usually the hardest and the most crucial, as they can have the most significant long-term impact. You should ensure that your cyber insurance policy provides access to an expert response team, who will triage the situation to allow you to gain control of the problem immediately. Moreover, if this is a 24-hour service, you are in the best possible position as you have support regardless of when the breach occurs.

Once you have followed these seven steps and taken out a comprehensive cyber insurance policy, you won't be immune to cybercrime. Still, you are less likely to suffer detrimental effects should you be a victim.