MARCH NEWSLETTER

RWK IT Services

Vol. 3 Ed. 7 | March 2023

Cyber Insurance: Why you need it now more than ever

The COVID-19 pandemic has brought about significant changes in the cyber risk profiles of companies. With the majority of their staff working from home, businesses are much more vulnerable and easy targets for cybercriminals.

Some of the reasons include the abrupt switch to the WFH model, which resulted in:

- A lot of people accessing their work data from home networks, which lacks high-level security
- The inability of businesses to monitor the work-related IT activities of their staff and,
- The use of personal devices by employees for work purposes

Businesses can overcome this challenge through a combination of tools and actions such as:

- Installing anti-malware software
- Putting in firewalls to safeguard their work network
- Having clear and effective IT policies in place when operations are remote
- Providing staff with laptops or desktops to use for work purposes during the WFH phase
- Training employees to identify cyber threats and steer clear of them
- Educating employees on password hygiene and cybersecurity best practices

However, these measures are no guarantee that nothing will ever go wrong! One malicious attachment could bring the whole IT infrastructure crashing down. And, if there's a data breach where confidential information has been compromised, then you'd be looking at hefty compensation payouts.

That is why you need cyber insurance. Cyber insurance is not something new, but it has never been so important as it is now.

Cyber insurance typically covers direct and indirect costs arising from cybersecurity incidents. When you lose data accidentally or, when your data is compromised or held ransom, your first thought would be to get access to your data and get your business back on its feet. Yes, you will want to call in for a trusted IT services provider to put your business back on track quickly. But, it is not that simple. If you don't have a service level agreement with an IT service provider, it may be difficult to find one instantly and also, challenging to find someone who you can trust with your situation. Even if you do find someone, chances are, they will charge you exorbitant rates by the hour.

But, apart from this direct expense, there are several factors involved in such situations, and all of them can deeply compromise your bottom line. They include-

- **Forensic analysis -** After a cybersecurity attack, you need to conduct a root cause analysis to identify what went wrong and where, so you can take corrective action to prevent the possibility of it repeating.
- **Notification expenses, penalties & lawsuits** Along with data breaches come a lot of liabilities including timely notification, fines, penalties, and perhaps even lawsuits for which you will need legal representation.
- **Revenue loss--direct and indirect** - If your business is a victim of cybercrime, you will likely have to shut down your IT infrastructure for some time even as the issue is being resolved or contained. This downtime can cost you quite a bit in terms of lost sales and also employee productivity. Not to mention the damage to your business's brand name which will have some effect on your sales revenue for at least a few months to come--and add to that the costs of employing a good PR agency to create some positive buzz around your brand to overcome the bitter taste left by the data breach incident.

continued on page 2

continued from page 1

Apart from the items covered above, which is more like a consequence of data loss, there are two big risks that cyber insurance policy can protect you against--cyber extortion and fund diversion.

- **Cyber extortion -** Remember the WannaCry Ransomware incident that happened in 2017? Cybercriminals used a worm, a form of malware to infiltrate more than 200,000 target computers and freeze user's access to the data therein. The losses caused by WannaCry are estimated to be in the range of billions of dollars. What would you do if someone held your data hostage or worse still threatened to leak it online? As a business owner, you have no choice but to pay up the ransom amount.
- **Fund diversion** - This is another form of cyber attack, though not as obvious as cyber extortion. Fund diversion is when you or your staff accidentally end up diverting your business funds to a fraudster. For example, your accountant clicked on a phishing link that took them to a clone site of the bank where your company has its account, or they made a payment by clicking on a fraudulent email sent by a cybercriminal posing to be your vendor.

As you can see, pandemic or no pandemic--cyber insurance is a must-have. And, not just that, some of your clients may insist that you have cyber insurance coverage before they trust you with their data--especially if you are operating in the B2B market. So, while cyber insurance can break the fall in case you become the victim of a cyber attack or some gross malfunction that causes data loss, it is important to remember that cyber insurance is still NOT a replacement for cybersecurity. You cannot invest in a cyber insurance policy and not bother about putting data security measures in place. In fact, like any other insurance, cyber insurance will also have exclusions and any laxity on your part in terms of data security can cause your coverage to become null and void. This is where a trusted managed services provider can be of help. An experienced MSP, such as RWK IT Services, can help you pick the right cyber insurance policy based on your needs. We will be able to explain the exclusions clearly to you--in your terms and help you design and maintain the security mechanisms and processes necessitated by the cyber insurance policy.

Team Birthday Celebrations

Jesus - March 19

Rob - March 20

Mohammad - March 29

Other RWK News

Existing Partners: Want to earn a credit on your monthly service? **Ask us about our referral program!**

Are you in need of a laptop for home or secondary use? We have good, refurbished laptops in stock for purchase.

Do you have 2 monitors and want more desk space? We have pre-owned monitor mounts that just may be the ticket for you.

Contact Kelly Paroubek or Jeff Reiter for details!