Cyber-Risks and Liabilities

January/February 2020

How to Improve Your Cyber-incident Response Plan in 2020

In an era of constantly evolving cyber-threats and advancing technology, no organisation is immune to the risk of cyber-attack. Just this past year, over 30 per cent of businesses experienced a cyber-attack, according to government data.

That's why having a cyber-incident response plan is a vital element of any organisation's approach to business continuity. At a glance, cyber-incident response plans provide business leaders like you with proactive guidance to prevent cyber-attacks, as well as reactive steps to follow if a breach occurs. In other words, having a cyber-incident response plan can help prevent attacks from happening altogether and limit the damages in the event of a worst-case scenario.

However, simply having a cyber-incident response plan in place won't gaurantee cyber-resilience. Rather, it's important for your organisation to routinely revisit your plan to make necessary updates and improvements when new threats emerge.

Consider the following tips to adequately update and improve your cyber-incident response plan in 2020:

- **Maintain proper documentation**—Make sure your cyber-risks are properly documented as a reference point for improving your incident response plan. Keep in mind that when cyber-risks or threats evolve, your response plan should follow suit. Also, be sure to document any past cyber-incidents that took place. By doing so, you can better analyse what went wrong and adjust your incident response plan to make sure the same concern doesn't happen again.
- **Prepare for different scenarios**—No cyber-incident is exactly the same. With this in mind, be sure your cyber-incident response plan is multi-faceted with tailored steps and preparations based on the type of attack. A common approach is to have varying levels of response based on the severity of the breach. For example, a phishing attack that only infected a single user and led to minimal data loss would call for a different response than a large-scale breach that resulted in significant disruption.
- **Test your plan**—In addition to preparing for different forms of cyber-attack, it's also crucial to routinely test your response plan with sample scenarios. Similar to a fire drill, try to involve every employee in the process of testing your response plan. This way, all staff members will know how they play a role, and you will be able to accurately determine the effectiveness of your plan. From there, you can make adjustments as needed and feel more confident in your plan in the event of a real cyber-attack.

Apart from updating your cyber-incident response plan, don't forget to make sure your organisation possesses adequate levels of cyber-insurance. Contact MacKay Corporate Insurance Brokers today to further discuss cover solutions for your unique cyber-security needs.

MacKay Corporate Insurance Brokers
01292611028
http://www.mackaycorporate-brokers.com

MACKAY
Corporate Insurance Brokers

The Numbers Behind Remote Work Offerings

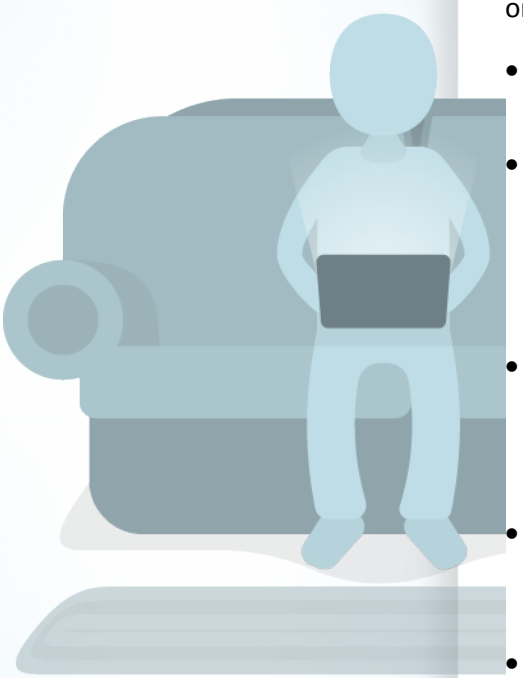
When organisations introduced remote work options:

The number of sick days taken decreased by **10%**

Productivity rates increased by **30%**

Stress-related illnesses decreased by **35%**

Office-related costs decreased by **30%**



Source: IT experts

What You Can Do to Implement Remote Working Options in Your Organisation

While you might visualise the average workday for your employees as a 9 a.m. to 5 p.m. schedule in the confines of your organisation's office space, recent research revealed that UK workers are calling for a new norm. Indeed, employees across industry lines are pushing for more flexible working options, such as non-traditional hours and remote work capabilities. A global survey conducted by IT experts found that **over half of UK employees want more flexible working options**, with over 40 per cent of respondents confirming that they would have more job satisfaction from remote work (eg working from home).

What's more, offering flexible work options can benefit more than just your employees. Implementing features such as remote work capabilities can have a variety of positive impacts on your organisation as a whole. Since many employees are able to work better from the comfort of their own home rather than an office, remote work can contribute to boosted productivity rates. Such flexible work options can also save your organisation money in the realm of office-related costs, seeing as you will have the ability to rent a smaller (and more cost-effective) office space or engage in practices like hot-desking. Lastly, remote work offerings are well-known as a solution to help boost employee morale, reduce absenteeism and improve staff retention levels.

Although remote work capabilities come with a wide range of potential business advantages, this flexible work offering can also cause significant consequences without the proper controls in place. Specifically, maintaining adequate cyber-security is a primary concern when allowing employees to work from home. Be sure to utilise this guidance when implementing your organisation's remote work programme:

- Only allow trusted and competent employees to take part in your remote work programme.
- Make sure you have the proper remote work equipment for your organisational needs. This could entail providing a laptop for all employees, offering a technology stipend for staff to purchase their own equipment or allowing employees to utilise their own devices (eg a personal laptop, tablet or mobile phone).
- Ensure all remote working equipment contains updated antivirus and malware protection. Make sure employees use strong passwords and data encryption on company devices. Conduct routine software updates on all remote work equipment.
- Require all remote workers to use a secure wireless connection and prohibit the use of public networks. Consider setting up a virtual private network as an added layer of security.
- Create and enforce a remote working policy, internet usage policy and bring your own device policy (if applicable). Ensure that these policies are compliant with the GDPR.