Cyber-Risks and Liabilities

September/October 2020

Key Elements of Cyber-security for Educational Institutions

Although the UK has made reopening schools a priority in advance of the upcoming academic year, a large portion of teachers and senior leaders believe that remote or blended education will continue to be a part of the teaching and learning process—even with reduced lockdown measures.

With this in mind, strong cyber-security practices and procedures may be an even more important priority for educational institutions in the future. When planning for the upcoming school year, educational institutions should consider addressing the following cyber-security risks.

Phishing Emails

Both in the years prior to the coronavirus pandemic and during it, the frequency and threat of phishing emails has been on the rise. As they pertain specifically to schools, these cyber-attacks may have been attempting to impersonate school payment systems, such as ParentPay, +Pay and SchoolMoney. Parents and schools alike must be aware of these cyber-criminals and their methods, which may include directing victims to fraudulent websites.

Institutions should be sure to conduct cyber-security training for all school staff and encourage them to always think twice before opening a link or downloading an attachment. Schools should also take the time to inform parents about what kinds of communication and information they can expect to receive and how it will appear.

Internal Device Checks

Not all cyber-security threats are external. It is possible that a computer or other piece of equipment connected to a school's network may already be compromised. Institutions should conduct audits of all equipment that will have access to their network. IT employees or contractors should also be tasked with checking all user accounts to make sure that they do not have unnecessary access to certain data or systems. In the event of a device or account being compromised, this type of limited access can minimise the amount of data or information available to the perpetrator.

The Cloud

While cloud servers allow teachers and other employees to work remotely and have access to necessary files from various locations, they also can help reduce the danger or consequences of a cyber-attack. Moving servers and file storage off-site can provide a safer environment, while also ensuring that important and sensitive data and information is regularly backed up.

Conclusion

Even for schools that are able to welcome back students in a traditional learning environment, it is important to be prepared in the event of a second wave of COVID-19 cases forcing additional closures.

For more information and insurance solutions related to cyber-security, contact us today.

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

MACKAY
Corporate Insurance Brokers

The Importance of Using a VPN to Protect Your Data

Despite the UK's ongoing efforts to reduce lockdown measures and allow more employers and organisations to bring employees back to their physical workplaces, a large portion of the workforce continues to work remotely.

Given the threat that cyber-criminals continue to pose to organisations of all types and sizes, it is important to implement and deploy a number of general cyber-security measures. The use of a virtual private network (VPN) can be a particularly valuable security investment.

VPN servers can help prevent criminals from being able to access information, such as web traffic. These virtual conduits provide encrypted pathways through which data and internet traffic travel. As such, the eyes of potential cyber-criminals are kept blind.

In addition, VPN servers also cause employees' devices to appear to have the VPN's IP address, rather than that of the network an organisation is actually using. As such, cyber-criminals will not be able to track employees' identities or locations.

For employees who may utilise public Wi-Fi networks, VPNs are of even greater importance. Public Wi-Fi, such as those available at coffee shops or airports, may not only leave users vulnerable to cyber-criminals monitoring the network, but also can be impersonated in an attempt to lure users into exposing information. Fortunately, VPNs will keep not only third-parties, but even the operators of the network from being able to access users' data.

With so many employees working remotely, there is a far greater amount of potentially sensitive information or classified data travelling back-and-forth online. VPNs present a key element of cyber-security that should be highly considered by all organisations.

INTERPOL Report Shows Cyber-criminals Attacking More During COVID-19

With so many employers conducting operations remotely due to the coronavirus pandemic, cyber-security may have never been as important for organisations to prioritise as it is now.

In addition to the increased amount of work, data, meetings and potentially sensitive information being communicated or conducted online, it is now known that cyber-criminals have indeed been attempting to take full advantage of the situation. According to an August report from INTERPOL, cyber-crime has seen a stark rise in frequency, as well as shifts in targets, since the beginning of the pandemic.

In recent months, cyber-criminals have made a noticeable change from targeting small businesses and individuals to large corporations, government bodies and critical infrastructure. As these organisations have implemented remote work systems and networks to assist employees working from home, cyber-criminals have been attempting to take advantage of new gaps in cyber-security systems.

INTERPOL's report noted that since the start of the pandemic, the following cyber-crime patterns have been related specifically to COVID-19:

- **Scams and phishing**—Cyber-criminals have specifically preyed upon fear of the pandemic by utilising coronavirus-themed phishing emails and impersonating government or public health officials in order to coerce victims into revealing personal information.

- **Ransomware**—Cyber-attacks have also targeted critical infrastructure and health care providers. Criminals understand that these types of attacks can garner large ransoms due to the importance, impact and need for such targets to be able to operate efficiently.

- **Data harvesting**—Malware can be used by cyber-criminals to harvest data. This type of cyber-crime is also on the rise, with perpetrators using information related to COVID-19 to gain access to systems, networks and sensitive data.

- **Malicious domains**—Cyber-criminals have also been registering a large amount of fraudulent and malicious website domains, often including words likely to gain the attention of victims, like 'coronavirus' or 'COVID.' According to an INTERPOL private sector partner, there was a 569 per cent increase in malicious domain name registrations between February and March this year.