BEAZLEY CYBER RISK MITIGATION STRATEGIES

1 Regularly back-up critical data to a separate location that would be unaffected by an issue with your live environment, and test to ensure those backups are recoverable.

All organizations should perform regular back-ups of their critical/important data and should ensure these back-ups are recent and restorable. By doing so, you can guarantee your organization will still function following the impact of a cyber attack, accidental deletion, physical damage, or theft of data. Furthermore, if you have back-ups of your data that you can quickly recover, ransomware attackers are much less likely to successfully blackmail you.

The more often you update your files and data that are critical to your business, the more often you need to back-up. You should consider daily back-ups if you make changes every day, or monthly back-ups if your updates are less frequent, for example.

Many platforms have built-in back-up functionality, so you may already have available options. Alternatively, you can explore either a third-party back-up solution (like cloud backup platforms) or perform your own back-ups to external drives that you keep secure and disconnected from your live environment.

2 Use multi-factor authentication (MFA) for cloud-based services and for all remote access to your network.

Passwords no longer provide sufficient security, especially for services available via the cloud (Microsoft 365, Google Workspace, etc). Users might create passwords that can be easily guessed, and humans are vulnerable to accidentally sharing their password via social engineering.

MFA is important as it makes stealing your organization's information much harder for the average criminal. MFA doesn't eliminate the necessity for usernames or passwords, but it adds a layer of protection to the sign-in process. When accessing accounts or apps, users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone or mobile app. MFA is built-in to most cloud/internet-based services, so please ensure you enable it. Alternatively, there are third-party suppliers that offer MFA utility using SMS codes, unique codes, and even hardware tokens. Please note, MFA is not required if you/your business uses Jane, Clinicmaster, owl practice, or Practiceperfect.

3 Do not allow remote access into your environment without a virtual private network (VPN).

Attackers are regularly "port scanning" the entire internet for visible remote-access services, such as Microsoft's Remote Desktop Protocol (RDP). Any open RDP services will be constantly probed for weaknesses, so hiding your remote-access services behind a VPN will provide a good level of protection against these attacks.

Like MFA, there are many third-party providers that offer VPN services and your own networking infrastructure (e.g. routers) may also have this functionality built in that needs to be enabled. This requirement is only for remote access to on-premises services.

4 Regularly (at least annually) provide cyber security training, including anti-phishing, to all individuals who have access to your organization's network or confidential / personal data.

Your staff are at the front line of your organization. They are constantly exposed to electronic communications with third parties that may leave them open to attack. Even though technical security measures may afford some level of protection – think of email gateways, endpoint detection, and response (EDR) software – it is still essential for staff to be aware of the risks. Training will help employees identify cyber risks, and in turn, will hopefully prevent them from impacting your organization in the first place. The National Cyber Security Centre (NCSC) offers free cyber security training for staff, which has an anti-phishing module within it. You can visit getcybersafe.gc.ca for information and free resources.

For more information, or if you have more questions about professional liability and business insurance solutions, contact a broker at BMS – we're here to help.

1-855-318-6558

info.canada@bmsgroup.com

bms. beazley