HSB

A Munich Re company

Technical bulletin

Cyber-securing your small business

Developing a written programme

If you don't already have a written cybersecurity programme, start by identifying your business objectives and organisational priorities. This will include reviewing the IT systems that your business uses and the types of information processed and stored.

Do you store personal information, financial account information or email addresses? The EU General Data Protection Regulation (GDPR) applies to all companies processing the personal data, by controllers and processors, of subjects residing in the EU; regardless of the company's location. Therefore, knowing what information you have and its location is the first step in expediting and lowering the cost of responding to cyber-attacks and data breaches.

In addition to written policies, your cybersecurity programme will require the selection and implementation of physical and behavioural controls.

Implement physical controls

Patch and update regularly
The most damaging and prolific cyber-attacks exploit known vulnerabilities. Installing patches and software updates is the most effective physical protection you can employ.

Deploy cybersecurity software
Make sure that you are using a firewall and that it's properly configured. Use at least one antivirus program and configure it to scan systems regularly. If you have remote employees or allow remote access, use a VPN (virtual private network) to secure access.

Employ multiple redundancies for backups
Backing your data up to the cloud is good, but backing it up to air-gapped storage (a storage device that is not connected to the Internet or other networks) is better. Recent ransomware attacks have encrypted networks as well as cloud backups. To ensure that your business can recover quickly and reduce remediation costs after an attack, employ multiple backups.

Control physical access to your computers and data
Create individual user profiles so that only authorised users can access your systems and data. Consider multi-factor authentication for sensitive systems and data. Restrict administrative access to only those users who require it. Establish rules that mandate strong passwords that are at least eight characters long and contain a combination of randomly selected letters or phrase and a six-digit PIN[1].

Secure Wi-Fi networks
Set a strong password for your router. Do not use the default password. If you allow guests to access your Wi-Fi, consider setting up a separate router and password for their use.

Employ best practices for payment cards
If your business accepts payment cards, work with your processing provider to ensure that your business is Payment Card Industry Data Security Standard compliant.

Vet vendors' cybersecurity
Employing a vendor, such as a cloud storage or security provider, doesn't eliminate your exposure in the event of a cyber-attack or breach. Ask them to verify their cyber security measures and protocols. Remember, GDPR requires the data owner, not the vendor, to notify affected individuals in the event the vendor suffers a breach of the owner's data.

Implement behavioural controls

Train employees
Cybersecurity professionals routinely warn that employees pose the greatest threat to even the most rigorous cybersecurity programme. Training is the most effective measure you can take to bolster your policies and programme. It's not sufficient to distribute your policies and ask employees to sign off. In addition to formal training, consider posting security posters, encouraging employees to attend free cybersecurity webinars, and regularly educating them about current threats. Consider exercises such as phishing your own employees to reinforce the best security practices.

Address unauthorised devices and shadow IT
Implement a realistic mobile device policy, and reinforce your policy with physical controls and employee training. Control shadow IT - the use of unauthorised devices, software or apps - by employing an approval process for software and hardware purchase and use.

Reproduced with kind permission from The Hartford Steam Boiler Inspection and Insurance Company. For more insights, visit their Equipment Connection blog.

[1]Find the latest National Cyber Security Centre guidance for passwords here.

HSB
A Munich Re company