Keeping your Cyber Insurer Happy

TOP 5 TIPS

Risk mitigation is a key compliment to any quality insurance solution, and cyber is no different. A combination of a rise in the severity of claims (particularly ransomware) and hardening market conditions has focussed attention on simple yet effective measures that insurers will look for as minimum requirements:

1. MFA/2FA

Multifactor Authentication or Two-Factor Authentication is where the user is prompted for an additional form of identification as part of the sign-in process.

Trusted devices are considered one form of authentication (as they are not easily duplicated) and a 2nd method is as simple as a password/PIN or biometric.

MFA and 2FA are essentially the same thing – although MFA allows additional layers of authentication if required.

2. Back-ups

A basic method to minimise ransomware attacks is to back up systems and data regularly.

However, it is not much use if they are on the same system, so they need to be separate and isolated from the network.

Preferably, the back-ups should also be protected with encryption.

It is even better if organisations can demonstrate that there has also been a test for full restoration and recovery (of systems and data) within the previous year.

3. Remote Access

Even before Covid-19, many organisations allowed employees to access their network remotely. That trend has clearly risen sharply (along with the exposures) and looks set to remain, which is a concern for insurers.

Basic controls would include MFA/2FA for remote access as well as restricting access to sensitive data.

A VPN (Virtual Private Network) is also a highly recommended method of protection against publicly exposed remote access services.

4. Email Protection

Email is one of the main vulnerabilities of any organisation. Again, simple solutions can offer additional protection.

Utilising SPF (Sender Policy Framework) on inbound emails ensures the validity of the sender has been verified. Pre-scanning emails for malicious attachments is another basic tool.

Incorporating MFA/2FA on email systems ensures the organisation has increased protection against BEC (Business Email Compromise), which is a dominant feature of many successful access attempts.

5. Training

Education remains a key component in risk mitigation as 'bad-actors' continue to rely on employees making mistakes. Staff can often be the biggest vulnerability.

In a busy (and more remote) workforce these mistakes can easily happen, but the implications can be devastating.

A fully implemented training program for all employees (including identifying phishing scams) is ideal. But even basic training (such as free modules available from the National Cyber Security Centre) is useful and very easy to implement - NCSC Staff Training

MPR MANAGEMENT & PROFESSIONAL RISKS

To be solid, insurance must be flexible