


Is your cyber resilience shored up?

26 July 2024  Kay Chand

As some of us start to think about heading to the sea shore for our summer holidays, in light of a number of recent high profile cyber attacks, have you shored up the cyber resilience of your digital systems?

“Cyber attacks are increasing in number, scale and sophistication, and pose a threat to all financial services firms. We expect you to be able to protect the sensitive information you hold. **Is your firm capable of defending itself against cyber attacks?**”

The Government published its [cyber security breaches survey](#) on 9 April 2024. It has identified that “Half of businesses (50%) and around a third of charities (32%) report having experienced some form of cyber security breach or attack in the last 12 months. This is much higher for medium businesses (70%), large businesses (74%) and high-income charities with £500,000 or more in annual income (66%).

By far the most common type of breach or attack is phishing (84% of businesses and 83% of charities). This is followed, to a much lesser extent, by others impersonating organisations in emails or online (35% of businesses and 37% of charities) and then viruses or other malware (17% of businesses and 14% of charities).”

As technology becomes more sophisticated, so do the nature of cyber attacks. The level of sophistication is currently such that any legal framework to hold threat actors to account is of little effect in practice as the sophistication of the threat actors makes it extremely difficult to identify them and take and enforcement action and indeed obtain redress for those firms which have been harmed.

One only needs to look at the rise in number and the increased sophistication of deepfakes.

Taking into account the current digital landscape and the pace at which it is evolving, it would be prudent to accept that the number of cyber attacks will rise, the sophistication of them will continue to develop and that it is a matter of “when” and not “if” a firm will be attacked.

This is a concerning trend especially at a time when firms are implementing digital security processes and procedures precisely to mitigate against data breaches and cyber attacks. For example, voice recognition is becoming common place across firms in numerous use cases, for example customer verification and to analyse whether perhaps a customer is under duress when making withdrawals from banks or claims with insurers.

Deepfakes use two neural networks, a “generator” and a “discriminator”. These are not rules based and use advanced algorithmic training across a vast number of data sets such that the deepfake improves itself as it goes along. The generator creates the fake content and the discriminator evaluates the authenticity (acting almost as a judge of the generator). The more advanced the algorithmic training, the more authentic the deepfake.

In light of this increased risk exposure from potential cyber attacks, it has never been more important for firms to shore up their cyber resilience. “Cyber resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources” (NIST SP 800-160).

The regulatory obligations around mitigating the risk of cyber attacks are already wrapped into various regulatory requirements laid down by the Financial Conduct Authority and the Information Commissioner’s Office.

From an insurance sector perspective the risk is two fold a) ensuring the firm’s own cyber resilience and b) the risk of increased claims due to cyber attacks.

Some key questions to get you started are:

- do you know what level you are at on the cyber security maturity model?
- when did you last conduct penetration testing and was it deep enough?
- what pre-emptive or preventative cyber security measures is your firm taking?
- how ready are you to respond to a cyber attack based on 4 key cornerstones:
 1. Anticipate
 2. Withstand
 3. Recover
 4. Adapt/Evolve
- do your data processing procedures and impact assessments take into account cyber security risks?

The risk of cyber attacks is here to stay. For firms to survive in this digital era, it is crucial for them to be able to weather the inevitable storm of a cyber attack. A firm's approach to cyber resilience and their cyber resilience strategy will be a key factor in mitigating against the risk of cyber attacks. Any digital strategy must now include cyber by design.

Key contact

Kay Chand

Partner

Kay.Chand@brownejacobson.com

+44 (0)330 045 2498

Related expertise

Services

Criminal compliance and
regulatory

Cyber liability and data security
insurance

Data protection and privacy

Insurance claims defence