MILLS & REEVE

Managing General Agents' Association

MGAA

MGAA – ten tips for reducing your cyber risk

Leadership and strong direction are the key to building cyber resilience, with the boardroom the command centre for any effective cyber strategy. We set out below ten ways corporate leaders can pre-empt and manage the ever-increasing scale and complexity of cyber risks.

1. Know your network

The essential starting point for strong cyber security: ensure you understand and map the parameters of your network, work out where and how resources are shared and connections occur. Is it designed for reliability and business continuity? Are your mobile/home working and partner networks secure? Where are the risk areas?

A useful step is to make an inventory of all connected devices that are linked to your internal systems and outwardly to the internet – these are higher risk and often poorly protected – a common way for attackers to access or disrupt a system. These include 'things' such as CCTV cameras, removable media and mobile and wearable devices.

2. Identify your data flows

Look beyond physical connections and focus on your data flows – work out where data is stored and processed and check the security conditions under which those operations occur. Where is your highest risk commercial data and staff and customer data stored – and how might someone interfere with that? Bear in mind that whilst high risk commercial data will carry a high monetary value, the risk in personal data must be assessed by considering the impact on the data subject if their data is lost or interfered with.

3. Improve your security culture

Where there is a breach there is almost always some element of human error. Embedding a strong security culture in your organisation is a vital component to managing cyber risks. Consider establishing a senior management group to prioritise key risk areas and prepare policies and procedures. Ensure staff training programmes clearly communicate security awareness, and allocate a point of contact for information security. Establish a culture where staff are empowered to report breaches, not afraid of it, plus a bedrock of policies so that disciplinary processes can be applied where appropriate.

4. Monitor key threats

Know the threat landscape. Cyber risks are constantly evolving and new threats emerge to take unsuspecting businesses by surprise – ransomware being the obvious (and headline-grabbing) example. Which are the key threats that target your data? Which are going to target your business operations? Regular re-evaluation of your cyber risk management strategy will help respond to new threats. Draw on external intelligence, including competitors within your own sector as well as from regulators and from suppliers who specialise in cyber security, to feed into your evaluation.

5. Secure your technology

It's not just about tracking threats; track the solutions. You should start with the basics. Fix known vulnerabilities and ensure that your systems get the updates and patches they need. Remove or disable unnecessary, outdated, or unsupported functionality from your systems and consider encryption, backups and/or replication to mitigate the impact of a cyber-attack. Importantly, change default usernames and passwords on connected devices. Ensure user privileges are appropriately managed to safeguard against malicious or negligent insiders, or social engineering attacks. So far as practically possible and lawful, maintain logs of permitted users' activities on your networks and systems to help address internal misuse.

6. Understand your legal obligations

Under current UK data protection law, and the forthcoming EU General Data Protection Regulation, organisations are required to adhere to strict standards of information security, with severe penalties. Fines of €20m may be issued under the new legislation. Keep in mind your contractual obligations, as companies increasingly seek to ensure their business partners are complying with best security practices. Remember company directors are required to exercise reasonable skill, care and diligence in the performance of their duties. Businesses that provide essential infrastructure may have enhanced cyber security obligations. Make sure knowledge of cyber risks is a boardroom priority.

7. Incident management

A cyber-attack can harm a company's finances and reputation, disrupt a business and cause damage to customers. With the number of reported incidents worldwide rising steeply in some sectors, review how well your organisation is set up to identify and respond to a breach. Ensure your risk register is updated and your internal solutions are clearly mapped. Consider your reporting set-up – new mandatory requirements coming in May 2018 require businesses to be able to notify incidents to supervising authorities within strict timescales.

8. Work with third parties

Consider what assistance can be drawn from experience outside your organisation. Cyber liability protection, for example, will cover your business in the event of an incident. Draw on PR, legal and advisory expertise to assist further. Consider using data mapping technology and network immunisation technologies to assess and protect your systems well in advance of any incidents. Seek reporting from your inward and outward supply chains to provide lines of intelligence to help you identify potential vulnerabilities or threats, and to help you ensure that they are providing appropriate cyber security assurance for you, your customers and staff. Even consider sharing intelligence with competitors.

9. Prepare for accountability

Accountability is the watchword for digital businesses. Consider gaining independent compliance accreditation (eg ISO27001) to demonstrate your organisation's cyber effectiveness and to build user trust. Ensure you document everything, from staff training programs and internal policies, to records of key decisions, and names of key compliance personnel. In the event of an incident, any outside investigators will be seeking assurances that you are complying with best practice.

10. Test your systems

It can be a wake-up call for many organisations to test systems for weaknesses and improve responsiveness. Initiating a fake phishing scam, for example, can help you assess your workforce's propensity to click links or download files. For large organisations and complex systems consider carrying out a penetration testing exercise or offering financial compensation – a 'bug bounty' – to individuals who can locate any weaknesses of your network. Under new data protection laws, from May 2018, this kind of testing (and your ability to recover your systems and data following a major attack or incident) is explicitly on the radar of measures that regulators will be looking at.

contact us

Peter Wainman
Partner
T +44(0)1223 222408
peter.wainman@mills-reeve.com

Edward Hadcock
Associate
T +44(0)1223 222205
edward.hadcock@mills-reeve.com