RISKADVISORY

BUSINESS RECOVERY TOOLKIT

Cyber Protection and Preparedness

COVID-19 fundamentally changed the way that many businesses operate, and nowhere is that more obvious than in cyber security. In the rush to enable remote working, many organisations threw away the rulebook and rapidly found ways to allow staff to access the corporate environment in ways never previously envisaged. The overriding driver was to keep the business functioning, possibly at the expense of security.

Now is an ideal time to take stock of your organisational security posture and incident preparedness. The sections below are designed to allow you to capture your thoughts and findings in a structured way:

Technology

Flexible working may well become the norm. Are your remote access solutions manageable and scalable in the long run? Can you provide the same levels of protection to corporate data when it is outside of the traditional work environment? Has your security team got control over the environment in which your users are working? Are you able to audit and log remote access activities? Do you need to alter your technology stack in order to more easily cope with future lockdowns?

Comments:

Preparedness

With Covid-19 related attacks on the increase, how well prepared is your organisation to respond to a cyber incident? Do your existing plans and structures still work when the team may be geographically dispersed? Are your outsourced IT and security providers able to support you remotely if required? Is there an up-to-date picture of your network? Are you confident that you know where all your corporate data now exists? Have you rehearsed and tested your response plans?

Comments:

Process

Did your organisation already have a Working At Home policy? Does it need revisiting in light of recent changes? Are you able to identify, remediate and quantify the impact of a breach when the source may be on an employee's personal device, located at their home? What is the process for updating the corporate risk register in light of the rapid changes to architecture and working practices? How are you keeping abreast of the cyber threat landscape?

Comments:

Communications

What mechanisms do you have to communicate effectively with all staff, regardless of their physical location? Will these communication channels still work in the event of a cyber attack against corporate IT systems such as email and VoIP? How can you keep stakeholders, clients, suppliers and investors updated during an incident? Do you have a tried-and-tested communications plan for common cyber incidents?

Comments:

Obligations

Do you know your legal obligations in the aftermath of a cyber incident? What will your cyber insurers expect of you? Are there regulatory bodies who you need to report to? What are the thresholds for engaging law enforcement, the National Cyber Security Centre or the Information Commissioner's Office?

Comments: