Warner McCall Resilience

SRA Covid-19 cyber security warning

SRA warning

On April 9th 2020, the SRA advised:

> "criminals have taken advantage of concern over the Covid-19 outbreak."

noting that:

> "The National Cyber Security Centre (NCSC) has reported a 400 percent increase in coronavirus related fraud reports in March.."

and warning that remote working as a result of coronavirus:

> "will present many with new cyber security **challenges**"

The new normal

The way that the majority of us now work has changed beyond recognition in a few short weeks. IT departments have worked tirelessly to enable us to continue to do business, irrespective of our location. This has often meant the introduction of new online tools for both communication and the delivery of work. As we have seen with security concerns over some remote meeting tools, these new ways of working have sadly often brought new opportunities for cybercriminals to exploit. Couple this with a widely reported increase in phishing emails of over 600% since Covid-19, and there is clearly a need to not only review and strengthen our cyber security, but to ensure that we are prepared for a successful cyber attack.

What do the SRA advise?

In October 2019, the SRA posed the question:

> "It may be better to ask when, not if, you will be targeted by online criminals"

advising that firms need to:

> "make sure... that you know what to do in the event of an incident."

and:

> "Use exercises to test your preparedness, resilience and responses."

With an increased cyber threat, this advice has never been more pertinent.

What is incident management?

Incident Management refers to the development of a framework that enables you to prepare for, respond to and learn from a cyber incident. Incident management planning should cover:

1. Defined processes for incident detection.
2. Detailed incident response plan.
3. Clear definition of roles and responsibilities.
4. Resources to contain and resolve any incident.
5. Secure back-up procedures to ensure efficient data recovery.
6. Communication and reporting process.
7. Test scenarios which can be rehearsed.

Why is incident management important?

For those of you with incident management plans already in place, you'll know that the purpose of such a plan is to enable a quick and relatively painless return to business as usual, with limited financial and reputational damage.

The Travelex ransomware incident on New Year's Eve 2019, highlights the reason why effective incident management plans are key to achieving this goal. Initially reporting that systems were down due to 'planned maintenance', Travelex were forced to resort to pen and paper to operate for a number of weeks, impacting more than a dozen UK banks in the process. Damage to brand and reputation, irrespective of the financial cost to the company cannot be understated. As Mark Sangster of infosecurity magazine concludes, in this excellent article on the incident:

> "this event reinforces corporate need for tested incident response plans"

What if I already have a plan?

If you already have a plan in place, it's worth asking not only how well the plan would work with a distributed workforce and key staff potentially unavailable, but also if the plan covers recently adopted tools, processes and procedures.

In the Covid-19 world, there is actually a very strong argument for development of multiple plans based on different scenarios. As we move forward through 2020, it's important that we prepare for a range of options, from fully office-based through to complete remote working and stages in between.

How do I know if my plan is fit for purpose?

In our experience, the only way to check if your plan is fit for purpose is through, as the SRA advises, "preparedness, resilience and responses". Only with regular testing and rehearsing can you be sure that your plan(s) give you the best chance of limiting the brand, financial and reputational damage that a successful cyber attack can bring.

Learn more

If you would like to learn more about Incident Management, then please contact Al Sweet, CCO at Warner McCall Resilience. Al can be contacted at Al.Sweet@wmr.co.uk or on 07778 322230.

hello@wmr.co.uk
+44 (0)800 002 5730
Warner McCall Resilience
WMR_Cyber
wmr.co.uk