Are you prepared for the worst case scenario?

"These days, it's not a question of if a company will be breached, but when. Businesses tend to focus on threat mitigation and risk management, but incident response is often overlooked. A cybersecurity incident response plan (CSIRP) has to be in place to allow companies to recover should the worst case scenario happen." says Simon Campbell-Young, MD of Credence Security.

Simon Campbell-Young, MD of Credence Security

Campbell-Young says companies with a CSIRP are in the minority. In 2018, the third annual “Cyber Resilient Organisation” study conducted by the Ponemon Institute found that fewer than one in four respondents had a formal CSIRP.

“That is a scary result. Without a CSIRP, a business risks not only losing the opportunity to minimise the damage in the case of a breach but will likely not have plans in place about how to deal with the other factors that an incident results in, like loss of customer confidence,” he points out.

He adds that research has also found that most companies feel their CSIRP will not achieve the kind of response they would need to deal with an incident effectively.

“A CSIRP should be a work in progress. It should evolve as the threats – and the business – change, and should provide clear guidelines for every person in the organisation.”

The plan should include updated contacts, along with detailed processes and procedures for both employees and third parties, Campbell-Young says.

Breaches affect all areas of business

“While the security incident response team is responsible for making sure the plan is in place and is implemented should the need arise, breaches touch all areas of the business. It makes sense, then, to make sure the plan itself touches all areas of the business.”

This includes human resources, marketing and corporate communications, the risk and compliance team, the financial team, and law enforcement, he explains.

“The plan should define roles and provide guidance based on incident severity and scale, as well as identifying how each department should deal with the incident. In a real-world event, the CSIRP should make it relatively easy for the organisation to get on top of the incident by ensuring that everyone knows what they need to do, and how to do it.”

This means that all of the appropriate people understand the broader perspective of business stakeholders, know how to use the third-party resources available to them, and clearly understand their roles and responsibilities.

“A business should take every opportunity to engage stakeholders before you’re faced with real cyber threats. A good way to stay ahead of the bad actors is to conduct regular exercises that will put the CSIRP through its paces, allowing stakeholders to see how it works, which will also help highlight any gaps,” Campbell-Young says.

“With the ever-increasing threats out there, not to mention a mountain of regulatory and compliance requirements, it’s far too easy to lose track. Companies that don’t have a CSIRP in place, or have only put an outline together as part of a tick-box exercise, will find that they are woefully unprepared should the worst happen. Everyone in the company should be aware of what’s included in the plan, who the appropriate contacts are, and what their roles and responsibilities are in case of a security event or security breach.”

For more, visit: https://www.bizcommunity.com