Author

Richard Bergman
Partner – Tech Consulting
richard.bergman@pwc.com
+61 (2) 8266 0053

Why your cyber incident response plan matters now

Taking your cyber incident response plan seriously can help you bounce back from attacks faster and recalibrate your customer relationships in the process

When it comes to the problems that plague modern-day businesses, it's hard to overestimate the magnitude of cybercrime. Over the last few years, one-off threats involving Trojan viruses and instantly detectable phishing scams have morphed into full-blown attacks mounted by professional cybercriminals—often, with worldwide teams at their disposal. In March 2019, *the World Economic Forum reported* that more than 4.5 billion records were breached in the first half of 2018 and that cybercriminals were employing tactics that are more sophisticated and globally scalable, using advanced phishing kits and conducting more attacks via smartphone.

A 2017 report by Cybersecurity Ventures predicted that cybercrime will cost the world nearly 6 trillion dollars each year by 2021, the biggest economic wealth transfer in history while **Cisco reports** that ransomware attacks were jumping 350 percent annually.

And according to PwC's 2018 ***Digital Trust Insights*** report, seismic shifts in the way we use technology—such as the growing network of connected devices and the rise of artificial intelligence—will continue to add extra layers of complexity to our ability to prepare for incidents that could arise.

It's essential to acknowledge that organisations are wising up to the importance of cybersecurity. But for too long, cyber incident response has been relegated to IT departments rather than understood as a critical responsibility that affects everything from marketing and infrastructure to customer relationships and bottom lines. *The Digital Trust Insights* report found that only 39 percent of companies are "very confident" that they are building sufficient digital trust controls. Here are some critical reasons why we need to evolve our perceptions around cybersecurity and make a holistic and actionable incident response plan a high priority.

Cyber incident response is a whole-of-business matter

The fallout from cyber threats have been well-documented by the media. In December 2018, ***The Australian Financial Review*** reported that the Lowy Institute had attracted two cyber attacks from China potentially seeking information on foreign policy. And in February 2019, major Australian banks compromised property valuations and personal contact information belonging to nearly 1000,000 customers when **a data breach** affected property valuation firm LandMark White.

Unfortunately, many board members and senior executives still view cyber incident response as a technical risk rather than a potential event with implications for the entire business. They also fail to understand how reputational factors, legal expectations and changing regulatory requirements can make cyber incident response complicated and ever-shifting or the ways which miscommunicating an incident response to stakeholders—both internal and external—can exacerbate the damage.

But conversely, executing a strong cyber incident response plan and communicating your actions clearly and calmly can create new levels of transparency with your customers and improve loyalty and trust.

Response speed plays a starring role in modern-day cyber security strategy

In the age of sophisticated, highly targeted security incidents, a speedy response speed is crucial. The time your business takes to identify a potential data breach, contain and eradicate the damage and communicate your message to the organisation and the public can make or break your brand. But this doesn't mean that incident response should revolve around being *reactive*. In fact, it's quite the opposite. Given that the threat of cyber attack is escalating, companies need to spend more time investing in the operational readiness that will enable them to deal with the incident. Rehearsing and fine-tuning your incident response plan when you have the time and space to do so will ensure that it is much more effective when you're called to rapidly put it into action.

Modern-day incident response demands preparation and investment

During a moment often shaped by social media and the 24-hour news cycle, cyber incidents can fast become matters for public consumption. In the worst cases, this can shut down infrastructures and entire cities—such as **the 2018 ransomware attack against Atlanta that paralysed the metropolis's municipal operations.** But a cyber threat only becomes an incident once it becomes public, causes irrevocable damage or adversely impacts your brand. The more strategically a company invests time and resources in incident response and makes a habit of 'battle-testing' security incidents before they happen, the greater the chance that dealing with cyber threat becomes muscle memory that can be called upon again and again—rather than a knee-jerk reaction to a crisis.

Conclusion

Cyber attacks are part of our modern-day landscape. They're also a form of threat with parameters that are increasingly nebulous. But that doesn't mean that organisations should leave their game plans up to chance. In fact, preparing and investing in incident response and reframing cybercrime as an issue that affects every aspect of an organisation is the first step towards cultivating a deep resilience while managing uncertainty both now and into the future. It can also strengthen customers' confidence in your ability to put their best interests at heart—and build relationships that are stronger and ultimately more valuable for it.

References

https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/

https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

https://www.digitalpulse.pwc.com.au/report-digital-trust-insights-journey-trust/

https://www.afr.com/news/special-reports/cyber-security/the-lowy-institute-hit-by-chinese-hackers-20181203-h18nn3

https://www.smh.com.au/business/companies/home-loan-details-in-major-data-breach-20190212-p50xas.html

https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

127068131