COMPLEX INVESTIGATIONS: ARE YOU PREPARED TO MEET THE RISING BAR?

As organisations improve their ability to respond to incidents, the expectations of regulators and clients have increased

Increased data regulation has led to significant improvements in organisations' preparation for cybersecurity incidents. We have seen this additional preparation result in a vastly improved experience for organisations suffering from ever-increasing cyber threats. As the average effectiveness of response improves, it raises the bar across the board, forcing underprepared organisations to make changes in order to keep pace.

Even 12 months ago, the incident response focus may have been simply ensuring that an organisation was able to meet the GDPR's 72-hour notification window by having a judiciously chosen list of outside help they could contact in short notice. Today, however, we are seeing the questions that organisations are being expected to answer are increasingly complex.

While an organisation might have a good handle on how to rebuild their systems in a secure manner after a ransomware attack, they could struggle when faced with questions from their external auditor about whether their financial data is still accurate and intact.

For organisations that possess intellectual property, can they demonstrate it has not been stolen in order to confirm it still holds its value? These types of questions are not trivial, yet are frequently left out of incident response plans, many of which are solely focused on getting the business back up and running, while answering high-level questions about the impact to personal data. Having a clear and defensible investigative methodology is critical when trying to properly answer these questions.

An indicator of this higher level of scrutiny is the increase in the incidence and severity of litigation that organisations face following cybersecurity incidents. While fines from regulators can be significant, they pale in comparison with the figures sought during group litigation orders. We are also seeing that directors and officers are becoming the focus of this litigation as they struggle to demonstrate they have effectively exercised their duty to ensure value has been protected appropriately[1].

Demonstrating required protection has become a key battleground, as organisations seek to show that the technical and organisational measures implemented were appropriate to address the threats they were likely to face. Claiming an incident was the result of a sustained assault by a sophisticated nation-state actor is no longer an adequate defence. The ability to evidence the attack sophistication alongside the strength of controls in place prior to the incident can be the difference between intervention from the regulator and a devastating lawsuit.

What can organisations do to keep up with expectations?

Thankfully, cybersecurity incidents continue to be largely preventable. Most are the result of systems not having security patches applied promptly, user credentials being stolen through phishing attacks, or some combination of the two. Ensuring basic controls are implemented, audited, and approved by a third party on a regular basis can go a long way in providing assurance that the organisation has established appropriate controls.

Further, organisations should ensure their crisis management exercises include testing responses to complex questions we are starting to see. Is the organisation's CFO able to ask the right questions of the incident response team, and is that team able to answer those questions with sufficient detail to satisfy an auditor?

Unfortunately, this is an adversarial problem. Threat actors learn where organisations' pressure points are and have shown their ability to exploit them and increase their leverage. While organisations are improving their cyber risk mitigation techniques, we should expect threat actors to continue to adjust their attacks accordingly.

As the bar is raised for effective incident response, the impact of not meeting that bar will inevitably increase. This is an upward trend that will continue for years to come. Is your organisation or client able to adequately perform complex investigations and answer difficult questions?

[1] https://boardagenda.com/2020/11/20/do-litigation-on-the-rise-amid-host-emerging-risks/

Oliver Price, senior director

FTI CONSULTING | CYBERSECURITY

FTI Consulting, Cybersecurity, 200 Aldersgate St, London, EC1A 4HD
E-mail: Oliver.Price@fticonsulting.com
Tel:+44 (0)20 7632 5141 **Web:** fticybersecurity.com/thelawyer