Responding to a cyber-incident

With the coronavirus crisis having exposed many companies to more cyber-threats, senior data protection and cybersecurity lawyer **John Timmons**, and data protection partner **Tim Hickman** at a global law firm White & Case reveal how to respond should a major incident occur.

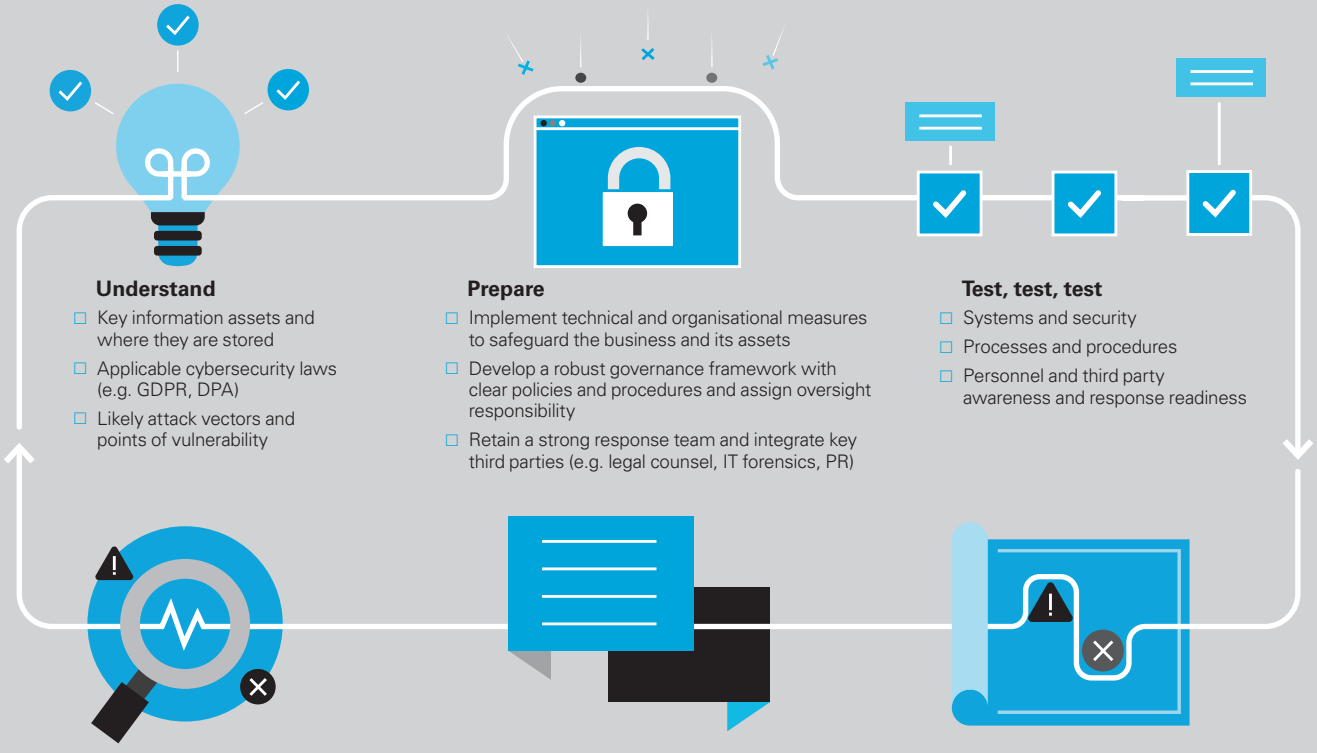
This article was published in a slightly different form in Raconteur's "Business Continuity and Growth" special report, *The Sunday Times*, on 2 August 2020.

The speed of response is vital; as much information as possible must be gathered in the very early moments to understand what information and systems have been compromised

Q: What impact did lockdown have on companies' exposure to cyber-threats?

A: Organisations had to rapidly adopt new systems, processes and procedures to accommodate remote working, and aggressively roll out existing solutions not widely used pre-lockdown. With everybody suddenly operating from home, patterns of work, and therefore network usage, changed too. The attack vectors changed, as did the points of weakness in organisations' information security. All this had a major impact on risk and management of cyber-threats. The sheer speed at which organisations had to adapt meant many did not have the time to do their standard diligence on providers and suppliers, which led to the deployment of solutions based

Responding to a cyber-incident



Understand

- Key information assets and where they are stored
- Applicable cybersecurity laws (e.g. GDPR, DPA)
- Likely attack vectors and points of vulnerability

Prepare

- Implement technical and organisational measures to safeguard the business and its assets
- Develop a robust governance framework with clear policies and procedures and assign oversight responsibility
- Retain a strong response team and integrate key third parties (e.g. legal counsel, IT forensics, PR)

Test, test, test

- Systems and security
- Processes and procedures
- Personnel and third party awareness and response readiness

Audit and improve

- Investigate incidents and conduct root cause analysis
- Review incident response and identify potential weaknesses
- Implement technical and organisational improvements
- Regularly ensure systems, policies and procedures are fit for purpose and audit for compliance

Communicate

- Agree and execute appropriate strategy with incident response team
- Assess whether to notify regulators, law enforcement, insurers and other third parties
- Communicate with affected individuals, if appropriate

Be proactive and reactive

- Use automated systems to identify incidents and take immediate action
- Prioritise incident response to resolve issues expediently
- Alert incident response team
- Engage other key stakeholders early in the response cycle

on incomplete information and the possibility of latent security flaws. If these issues are not picked up quickly and acted upon, organisations are susceptible to problems down the line and greater exposure to cyber-threats.

Q: If a major incident does occur, what are the immediate steps an organisation should take to respond?

A: It's something every executive fears: that call in the middle of the night saying that there has been a major cyberincident. The speed of response is vital; as much information as possible must be gathered in those very early moments to understand what information and systems have been compromised. Has this happened before and does it indicate a systemic issue? What is the risk to the organisation, its reputation and its customers? Establishing that initial snapshot assessment is incredibly important as it will drive not only the prioritisation of the response, but the entire process. If an incident is correctly identified as high risk at the onset, the response timeline will accelerate, with organisational resources deployed more appropriately.

Q: Once that initial risk assessment is complete, what should happen next?

A: Principally, it's about damage limitation and controlling the incident, so understanding the mitigating factors that might help to reduce risk to the business is key. If information has been lost or stolen, for example, was that information subject to encryption? Is it in a format that would be useless to a third party? Did the incident involve theft of a device that has since been recovered? If, following that risk assessment, you conclude that it is a major, high-risk incident, then the response must be fast. It may be necessary to first internally escalate by notifying the executive committee or wider board. External legal counsel should be involved as early as possible so they are on call to respond whenever needed throughout the incident. Engaging legal counsel has the added benefit of establishing privilege in certain circumstances, which can protect sensitive discussions from future disclosure should there be an investigation or litigation. Forensic IT experts are also an essential part of the damage limitation process, particularly in identifying the threat, understanding what went wrong and taking the appropriate measures to stem the tide. Regulators need to be informed as soon as possible, as should affected individuals, where organisations are legally required to do so.

Q: What elements of response are sometimes overlooked?

A: Public relations plays an often overlooked, but absolutely crucial, role in controlling the narrative and allowing the organisation to present the best and most accurate representation of the incident. At each stage of the response process, it is also vital to preserve evidence and record details of every action and decision that was made. You may look back and determine that, in hindsight, poor decisions were made, but if you can show precisely what information guided those decisions at the time, it can be beneficial in the event of an investigation or litigation. Of course, excessive retention of records and information can also present challenges, but legal counsel will be able to assist in striking the right balance.

Q: How does White & Case support companies in this important area?

A: Cybersecurity incidents do not respect national borders. Companies are often affected in multiple jurisdictions, with different regulators and laws in relation to disclosure obligations and timeframes. White & Case's global Cyber Incident Response team has extensive experience working with clients that have a multi-jurisdictional footprint. While we work with these clients through all stages of the preparedness, response and review process, we are uniquely positioned to assist during the critical incident response phase. This is due to our global presence and cross-disciplinary team of cyber-experts who are constantly collaborating with each other and with PR, IT forensics, internal compliance and incident response teams, helping to deliver crisis management and legal advice whenever and wherever it is needed

For more information please visit **whitecase.com/cybersecurity**.

Contacts

Tim Hickman
Partner, London

T +44 20 7532 2517
E tim.hickman@whitecase.com

John Timmons
Associate, London

T +44 20 7532 1598
E john.timmons@whitecase.com

whitecase.com

In this publication, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case LLP, a limited liability partnership incorporated under English law, and all other affiliated partnerships, companies and entities.

This publication is prepared for the general information of our clients and other interested persons. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.

© 2020 White & Case LLP

LON0820002_04