Navigating a Cyber Crisis: GC at the Helm

The Action Plan

A cyber crisis hits. What do you do? Where do you start? Who gets involved? These are the questions that test every organisation's resilience and readiness in a fast-moving and high-stakes situation. For General Counsel, these situations demand strategic action and decisive leadership. This action plan highlights key preventative measures and responsive strategies tailored for GCs to prepare for, manage, and mitigate the impact of a cyber crisis.

Understand your obligations – Understand what legal, regulatory and compliance obligations your organisation must meet, both now (proactively) and in the event of a serious incident, such as a data breach. Monitor and review these obligations to account for the changing regulatory environment.

Build bridges – Collaboration between legal counsel, IT, your communications teams, and senior stakeholders is key to responding effectively to cybersecurity and privacy regulatory requirements and real crises, such as data breaches and litigation. Build relationships with key stakeholders early and seek to understand their roles and challenges.

Partner with communications – It is important to establish a two-way partnership with your communications teams or external communications support. Communications and legal advice are most effective when it is coordinated and consistent, recognising the need to keep stakeholders informed in the event of a crisis.

Map the terrain – You can't protect what you don't know exists. Identify what systems and data are vital to your organisation and where these systems and data live. This should extend to data held on your behalf by other organisations. Because you can't lose what you don't have, consider disposing of data you don't need to hold.

Assess your maturity and compliance – Benchmark the maturity of your cybersecurity and privacy functions against industry standards, such as the NIST Cybersecurity Framework, and measure your compliance with cybersecurity and privacy regulations on an ongoing basis. Consider seeking independent expertise in conducting these assessments.

Communications and legal advice are most effective when it is coordinated and consistent, recognising the need to keep stakeholders informed in the event of a crisis.

Implement change – Work with key stakeholders to uplift your cybersecurity and privacy maturity so your organisation complies with its legal, regulatory and compliance obligations and is less likely to suffer a serious data breach or cybersecurity incident.

Change the culture – Train your staff to recognise cybersecurity threats and handle data appropriately, per your privacy obligations. Embed and enforce security and privacy by design in new systems, products and initiatives your organisation plans to implement.

Prepare to fail – Legal counsel holds one of the most important roles in a real crisis such as a data breach. Hold tabletop exercises and crisis simulations with key stakeholders, such as the executive team and the Board, to prepare you and the organisation for a crisis. Develop data breach and security incident response plans to train first responders so that you can fail better.

With proactive planning and clear coordination, GCs can help protect their organisations from severe reputational and operational damage while maintaining stakeholder trust.

STRENGTHEN YOUR CYBER PREPAREDNESS & INCIDENT RESPONSE

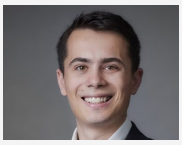
With proactive planning and clear coordination, GCs can help protect their organisations from severe reputational and operational damage while maintaining stakeholder trust. FTI Consulting can help you design tailored strategies and tools, ensuring you're prepared to respond effectively to a cyber crisis.

For more information, contact one of our experts below.

CARLA LIEDTKE
Risk & Investigations
+61 402 853 223
carla.liedtke@fticonsulting.com

CHRIS HATFIELD
Information Governance, Privacy & Security
+61 437 373 130
christopher.hatfield@fticonsulting.com

DAVID WHITELY
Crisis Communications Planning & Response
+61 475 110 928
david.whitely@fticonsulting.com



ED HOPKINS
Cybersecurity
+61 427 557 784
ed.hopkins@fticonsulting.com