CISO legal responsibilities in the event of a breach

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable on September 23, 2020, to discuss **"CISO legal responsibilities in the event of a breach**." We explored how Asia Pacific security leaders can address the challenges of responding to an incident, and the actions they can take to meet their legal obligations and individual responsibilities.

Recent public events—including litigation by the Australian Securities & Investments Commission (ASIC) against an Australian financial services firm alleging deficient cybersecurity practices; cyber attacks on the New Zealand stock exchange; foreign government attacks on Australia; and U.S. Department of Justice (DOJ) prosecution of a CISO for obstruction of justice—have thrust into the limelight the CISO's legal responsibilities in the event of an incident. How can CISOs best manage personal and enterprise risks during a crisis? How should CISOs engage with the C-suite, the board and public authorities?

Our speakers included Accenture Security subject-matter experts, legal advisors and peer CISOs. The session was co-hosted by Andy Vautier, Accenture CISO and ACF chair; and Andrew McLauchlan, Accenture Security managing director and Asia Pacific lead.

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

Are CISOs under greater scrutiny?

In the current environment, it may be difficult for CISOs to avoid the limelight, given a growing volume of threats and incidents, particularly high-profile ransomware attacks; complex regulatory requirements; and heightened public interest in cybersecurity risks.

Is the current DOJ case indicative of a trend? Many legal advisors think not. The DOJ does not appear to be escalating efforts to prosecute CISOs generally, and the case appears to represent a "one off," given the unique facts and context of the case, rather than a new precedent. Law enforcement will likely be looking for outlier criminal behavior, rather than intending to criminalize good-faith efforts to respond to incidents and cooperate with regulators.

Legislators and regulators on a global scale are scrutinizing how enterprises are responding to incidents. For example, *Australia's Cyber Security Strategy 2020* is expected to drive changes in the nation's critical infrastructure framework and increase enterprise cybersecurity obligations. Authorities in each country and region have jurisdiction over cybercrime and information privacy; CISOs will need to rely on legal counsel to navigate the complexity. CISOs are aware that as authorities redefine the enterprise's reporting requirements and other obligations, additional investment may be needed.

In addition, as ransomware attacks increase, there may be legal risks in payments made to sanctioned countries. The concern is growing globally.

Heed the wake-up call

Recent public events are a valuable catalyst for closely examining the CISO's legal responsibilities and the enterprise's incident response strategy:

1. **Don't go it alone**—Rely heavily on legal counsel to help protect yourself. For example, no CISO should be required to unilaterally decide what kinds of information need to be shared in the event of an incident.
2. **Set realistic expectations**—In reality, resolving an incident can take weeks or months; forensics alone often take 45 days or more. Ensure that senior management understands the time and effort required to address different kinds of attacks.
3. **Build trust before an incident**—Mutual trust is essential to success during a high-pressure incident response. The way to build trust is to do the pre-work—such as conversations, tabletop exercises, recurrent simulations and scenario planning—with all key members of the response team, including the board of directors and the audit committee. Gain the support of executive leadership and the board in fostering a security culture. Avoid technical jargon that can cause other executives to tune out. Get them to come on the security journey with you.
4. **Use fire drill exercises regularly**—Embed exercises as a normal part of "business as usual" to test run books and incident response team plans. Extend the exercises to independent observers.
5. **Address the pressure**—Unfortunately, some CISOs have been asked to withhold information about an incident. CISOs need to ensure that their voice is heard so that they are not forced into decisions they are uncomfortable with. Raise governance issues head-on, asking difficult questions such as how the enterprise would respond in specific situations. Ultimately, it's not the CISO's responsibility to decide, but rather to inform those who make the decision.
6. **Document everything**—Consider assigning someone to thoroughly document all conversations and decisions during fast-paced incident response situations. A precise evidence trail can help resolve problems later on.
7. **Pressure-test the incident response playbook**—Table-top exercises often lack the "grit" of an actual incident. Apply the playbook during an incident, and document gaps and other areas for improvement. Tests should not be an annual compliance exercise. Consider testing five likely scenarios (such as ransomware, theft of personally identifiable information, intellectual property theft, and insider attack) and strengthen those incident response plans. Delegate decision-making authority appropriately. Even with a strong playbook, managing conflicts among individuals and delegating authority during a simulated incident can be difficult. The CISO should make clear: "I'm leading this and you're not."
8. **Run scenarios with insurers**—Don't leave policy terms open to interpretation after the fact. Particularly in ransomware events, as cybercriminals make greater demands, coverage can be an important factor in decision making. For example, insurers often require that only one negotiator be engaged with cybercriminals. Include any insurance panels, such as legal or technical, in your exercises.

Best practices

In the current environment, there are several best practices that CISOs and their enterprises should consider adopting:

1. **Have an employment contract**—Even at-will CISOs should document their relationship and role with the enterprise. Important information includes a detailed job description, terms of termination, reporting relationships, and governance responsibilities. Personal liability insurance may not be required, but CISOs need to understand the directors' and officers' coverage provided by the company. Documenting the scope of available resources is particularly important in light of the COVID-19 disruption when resources may be in short supply. Talk in terms of business risks: Start a conversation with the CEO by indicating that you are concerned about the risks the company faces from cybersecurity threats.

2. **Establish an escalation and classification system**—The response playbook should detail how threats are evaluated and prioritized. Spell out how incidents should be classified and escalated. Keep the information flow going. Be clear on what the enterprise is going to say, when, by whom. Use the "cc:" line effectively in e-mails to inform all the right people (including your lawyers and chief accountability officer) during an incident response.

   The legal implications of language are increasingly important. For example, the Notifiable Data Breach (NDB) scheme of the Office of the Australian Information Commissioner (OAIC) specifies when to notify affected individuals and the OAIC about an eligible data breach.

3. **Establish clear information governance**—Ensure that the CISO and the rest of the response team (such as legal, communications, CEO, CFO) are assigned specific communications roles and responsibilities for reporting internally and externally.

4. **Prepare a third-party communications plan in advance**—Communication with third parties—customers, regulators, law enforcement, insurers and business partners—deserves particular attention; it is an area often fraught with peril for many CISOs. The incident response playbook should include a third-party communications plan that addresses all important stakeholders. Identify disclosure obligations. For example, GDPR requires disclosure of an incident within 72 hours, but requirements often differ by jurisdiction. Most insurance coverage includes 24- to 48-hour incident response notification requirements.

5. **Build communications channel security**—Particularly during an incident, when communications can be difficult, encryption and a dedicated secure channel for collaboration can be invaluable. Pre-approved templates for sensitive communications can increase speed and accuracy.

Conclusion

CISOs who commit to continued collaboration, preparation and documentation will be best prepared to manage the legal, business and reputational risks in the threat landscape. Collaboration should extend from enterprise legal counsel to, when appropriate, regulators and law enforcement. Preparation should include updating incident response playbooks; running simulations and scenario testing to build capability and trust; and strengthening communications with secure channels and clear lines of authority. Documentation should be precise, whether detailing the terms of an employment contract or how decisions are made in the heat of the moment.

CONTACT US

Andrew McLauchlan
Managing Director and Asia Pacific Lead
Accenture Security
andrew.mclauchlan@accenture.com

Joseph Failla
Managing Director and Australia/New Zealand Lead
Accenture Security
j.failla@accenture.com

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 509,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

Visit us at www.accenture.com

Follow us @AccentureSecure
Connect with us

Copyright © 2020 Accenture All rights reserved.
Accenture, its logo, and High Performance Delivered are trademarks of Accenture.