CISO legal responsibilities in the event of a breach

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable, "CISO legal responsibilities in the event of a breach," on September 3, 2020. CISOs explored the actions they should take to protect their enterprises, the public and even themselves.

CISO legal obligations are much in the news. As the U.S. Department of Justice (DOJ) pursues prosecution of a high-profile CISO in a breach case, other CISOs are asking important questions. What are the legal responsibilities and obligations of the CISO in the event of an incident? How should CISOs engage with the C-suite, the board and public authorities? How can we manage financial and reputational risk during a rapidly evolving crisis?

Our speakers—including Accenture Security subject-matter experts, an experienced cybersecurity attorney, and peer CISOs—discussed the challenges and responsibilities of addressing an incident. The session was hosted by Andy Vautier, Accenture CISO and ACF chair.

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.

Is the DOJ targeting CISOs in the new threat landscape?

CISOs who protected their enterprises from bad actors used to be perceived as heroes, even though they rarely sought the limelight. Today, most cybersecurity leaders aspire to be "one of the world's quietest CISOs," Vautier said. But it may be difficult to avoid the limelight, given a growing volume of threats and incidents, particularly high-profile ransomware attacks; new work practices driven by the COVID-19 disruption; complex SEC reporting requirements; and heightened public interest in cybersecurity risks.

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

Most criminal cases originate in an FBI field office. The FBI's cyber capabilities are much more technical and far better integrated with the CIA, NSA and the like in tracking nation-state activity.

Legislators and regulators are scrutinizing how enterprises are responding to incidents. 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

ACF members regard recent public events as a valuable catalyst for disciplined maturation of the CISO's legal responsibilities and incident response strategy:

1. **Don't stand alone on an island**—Rely on legal counsel. For example, no CISO should be required to unilaterally decide what kinds of information need to be shared in the event of an incident. Use the "cc:" function broadly in e-mails. Inform people of what to do when an incident occurs. Story-telling is an effective means of communication that engages non-technical audiences.
2. **Build trust**—Ambiguous situations require mutual trust, which 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, scenario planning—with all key members of the response team, including the board of directors and the audit committee. If you convene as a team for the first time during a crisis, the trust likely won't be there. A series of fire drills to refine the enterprise's decision framework around legal and brand obligations can help the team establish a productive working relationship.
3. **Address the pressure**—Unfortunately, some CISOs have been asked to withhold information about an incident. Ensure that your voice is heard so that you are not forced into a decision you are uncomfortable with. Raise governance issues head-on, asking difficult questions such as how the enterprise would respond in specific situations.
4. **Document everything**—Consider assigning someone to document all conversations and decisions during fast-paced incident response situations. A precise audit trail can prevent problems later on. Document how decisions are made relative to disclosure notification.

Best practices

Experts cited five things every CISO should be doing:

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; and reporting relationships and governance responsibilities. Documenting the scope of available resources is particularly important during the COVID-19 disruption when resources may be in short supply.
2. **Document incident identification and classification**—The response playbook should detail how threats are classified, prioritized and escalated. The legal implications of language are increasingly important. For example, the term "breach" has a legal definition in all 50 US states. Use the term "incident" until the use of "breach" is more appropriate, accurate and legally required.
3. **Establish clear information governance**— Ensure that you 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**—Every playbook should include a third-party communications plan that addresses customers, regulators, partners and all other important stakeholders. This is one of the areas that is most fraught with peril for many CISOs. 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 notification requirements. But an important question is, what do you tell them? You don't want to share privileged information.
5. **Lock down incident communications channel security**—Particularly during an incident, when "the fog of war" makes communications difficult, 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 collaboration, preparation and documentation will be best equipped 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; conducting scenario testing that builds capability and trust; and strengthening communications by using secure channels and pre-approved templates. Documentation should be precise, whether detailing the terms of an employment contract or describing how decisions will be made in the heat of the moment.

CONTACT

Andy Vautier

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

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.