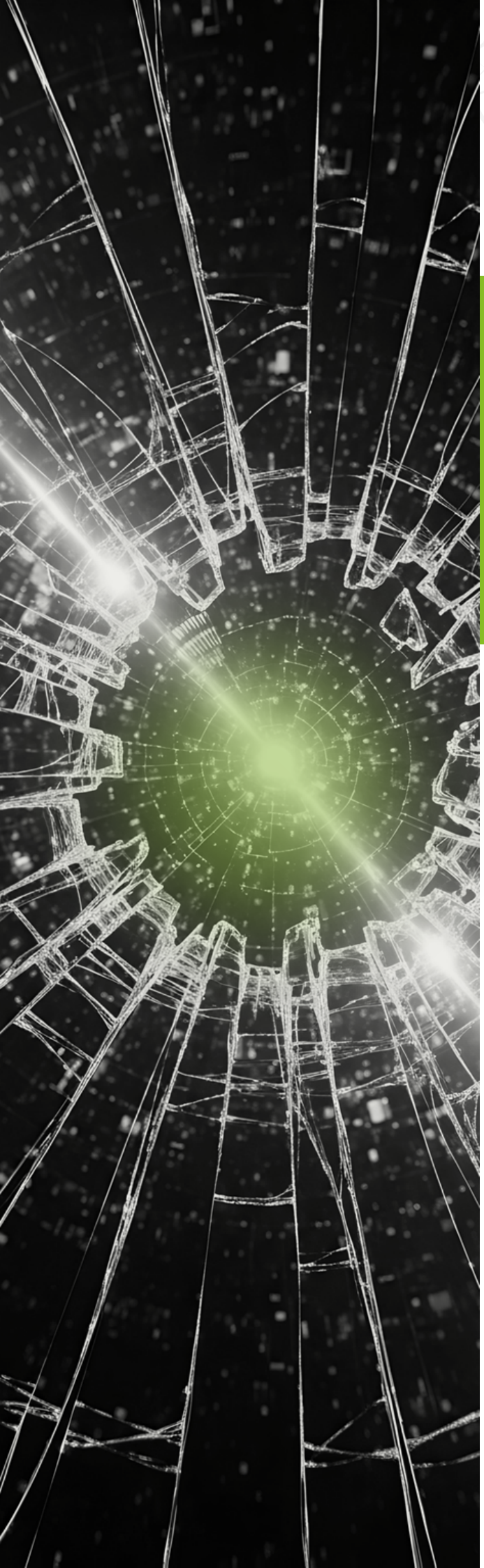
Deloitte.
Legal

Issue Averted

From crisis to confidence

Finding the way forward when hackers get in



With forethought and a sound strategy, your legal team can help manage a cybersecurity incident to limit harm and better prepare for future risks.

Cybersecurity incidents can disrupt business operations in an instant, turning an ordinary workday into a defining moment for an organization. When a company's IT systems are attacked, breached, or disabled by malicious actors, swift and decisive action becomes critical. The organization's Chief Legal Officer (CLO) can help guide the organization through their response to minimize negative impact.

While the days following a breach can be demanding, effective legal leadership can transform a crisis into an opportunity for resilience and recovery. With a clear strategy and sound decision-making, the CLO and legal team play a vital role in limiting harm and setting the stage for a stronger future.

What you're trying to avoid

Sometimes, people don't know who can make a certain decision, such as isolating a network environment. Everyone looks at each other and says, "I thought you had the authority to do that!" That's where advanced planning with your legal team can help.

No cybersecurity threat is the same. The initial report from the IT group to the CLO might be that hackers got into the system and have stolen, or are stealing, important information and data. Malware rooted in the network could have shut everything down—maybe a ransom has even been demanded. There might even be a denial-of-service attack curtailing your company's ability to do business.

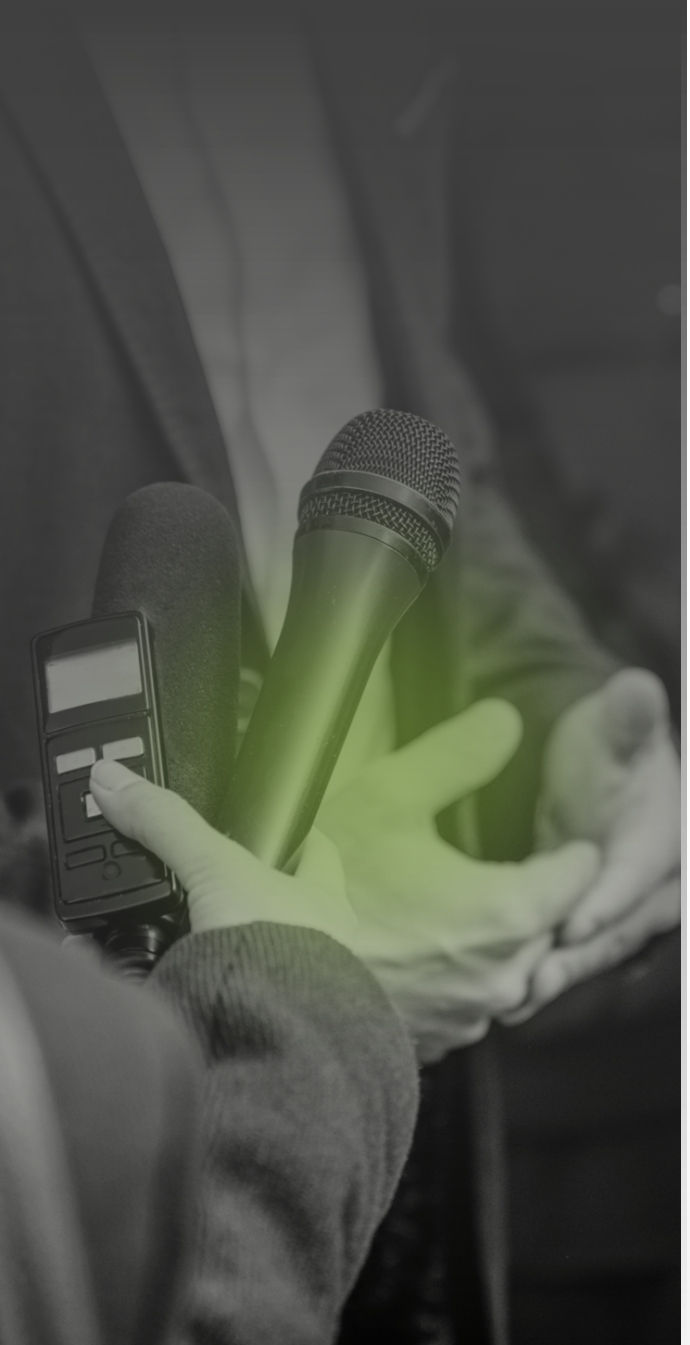
Whatever the threat or breach, the legal department—in close collaboration with crisis leadership—must help coordinate steps that can define the effectiveness of your company's response. These steps fall into two areas: decision-making and communications.

So, what you're really trying to avoid is:

Indecision

Decisions need to be made quickly to isolate or shut down certain systems. And this might have leaders from the IT group or even the C-suite wondering: Who *actually* has the authority? In a ransomware attack, for instance, a pay-or-not-pay decision can be wrenching, especially if your legal department hasn't been looped in to help you game out a response ahead of time. Advanced planning by your legal team can help to organize and facilitate these fast, difficult decisions, making clear who's responsible for what when it matters most.

Your legal specialists can work to guide external communications that are accurate, consistent, and legally sound, to help prevent making the legal or reputational consequences worse.



Flawed communications

Someone will need liaise with law enforcement authorities, and someone will need to reach out to regulators. Depending on the nature of the event, there may be highly sensitive communications that need to go to customers, employees, or other stakeholders. There will also be interactions with insurance carriers.

So, from the start, communications challenges demand the involvement and guidance of your CLO to establish attorney-client privilege protection. Discussions that happen before the shield of legal privilege can create additional litigation risk from regulators, affected individuals, business partners, and others. Where applicable, attorney-client privilege can help keep sensitive communications from disclosure, but the scope of this privilege varies across jurisdictions and may not always apply in regulatory proceedings.

Incorrect information can make matters worse. Statements to stakeholders or the public, if poorly conceived or improperly vetted, can create lasting reputational harm. External communications must not only be accurate and consistent but also comply with applicable legal reporting obligations, like mandatory notifications to regulators or data subjects under data protection laws. Alternatively, freezing and saying nothing also creates its own problems: When personal customer data has been compromised, notification timelines from regulators can trigger fines or sanctions.

When cybersecurity incident management proceeds without a sound strategy or adequate legal leadership, the initial impacts of lost data, stolen intellectual property, business interruption, regulatory and legal liability, and reputational harm can all be multiplied.

How to avoid ugly outcomes

If your lawyers are not dealing with a breach as you read this, there is still time to prepare. Because while the CLO plays a vital role in legal regulatory compliance, others dealing with the attack—like the chief information security officer (CISO)—will remain responsible for technical containment, forensics, and remediation. To help create an effective incident response across business functions, now is the time to think through and even practice what responsibilities will fall to the legal team.

Planning before

Be active in the development of your company's cyber breach response plan from day one, with a playbook that includes detailed legal guidance, describes the preplanned actions they will take, and the information they will need from other crisis responders to contribute to effective decision-making.

Companies will typically work with an outside legal team that has appropriate cyber expertise. The plan should outline when to activate their prearranged services and emphasize the importance of establishing attorney-client privilege. The risk assessment that underpins the response planning may also inform decisions about how much insurance to carry.

Those questions about who has the authority to make key decisions during a breach? They should be addressed in the plan, with trip wires and authorities mapped for a range of scenarios and spelling out procedures for external communications with a range of statement templates with pre-vetted, ready-to-use language.

The final step, once a plan is ready, is practice. The legal department can be responsible for training across the organization on key legal principles and processes. Repetitive tabletop exercises or simulations will help make the practice feel real, but more importantly develop "muscle memory" to allow the crisis team to respond more rapidly and with confidence. A lot can be gained by introducing key people to each other and reviewing planned communications, creating a positive feedback loop to strengthen your plan.

Acting during

If (when) the day comes, the first step is to activate your retainer and establish attorney-client privilege. Your legal response can help maintain control while directing communications and decision-making.

An effective response to a cyber breach hinges on seamless collaboration between your legal, business, communication, regulatory, and IT teams. Legal leadership's assessment is vital to prioritizing actions and addressing potential liabilities.

Coordination and cooperation will be important for success. Your legal team can expect to be embedded with the IT group. The goal is to help others understand the consequences of the breach through a legal lens.

While IT managers and engineers focus on fixing systems, preserving data, and restoring functionality, legal leadership can assess the scope and severity of the losses and damage. The legal department is in a better position to understand the implications, including any impact on personal data, intellectual property, and other intangible assets.

Regulatory compliance may involve notification requirements, a step made more complex because most cyberthreats cross national or jurisdictional borders. Potential legal liabilities need to be managed. Customer relationships may need repair. Your CLO, including outside counsel, will guide interactions with law enforcement and insurance carriers.

Learning after

As your organization recovers from a cybersecurity incident, the goal may not be to restore things to how they were before. Instead, there may be a better place to end up, with systems that are better protected and with the organization more resilient.

For example, if hackers breach an on-premises email system, restoring it to the status quo might not be the best solution. The breach affords the organization the ability to rethink its resiliency strategy by considering transitioning to more secure cloud technologies and adopting innovative recovery capabilities, among other measures. Financial or human resources systems or customer interfaces that were compromised may be re-examined to see how they can be made more secure.

These may be steps that could have been taken earlier, but now there is a catalyst. If the breach leads to systems change, or if transformation was overdue, your organization may emerge with more agile and efficient systems as the disruption recedes.

What your company gains

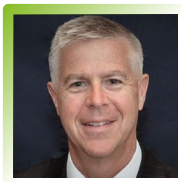
Understandably, the potential financial and reputational damage from a cyber breach is scary. But it's possible, when damage mitigation is successful and communications are thoughtful, that your company will emerge stronger than before, with your reputation intact—and possibly even improved.

A breach comes with important lessons. And customers and other stakeholders will observe whether you've learned them. Leadership might even consider proactively and deliberately sharing lessons learned with peer industry experts and the broader business community.

Cybersecurity is always changing, so a robust legal framework is not a nice-to-have, it's a necessity. By creating a proactive incident response plan, fostering seamless collaboration between legal, IT, and crisis teams, and prioritizing transparent communication, companies can not only mitigate potential damages but also emerge stronger and more resilient.

The silver lining of a cyberattack lies in its lessons: those who are prepared can transform challenges into opportunities for growth and innovation. As threats continue to rise, vigilant organizations will be those who see beyond the immediate impacts and invest in a cybersecurity future fortified by a proactive, strategic relationship between the legal team and all other actors involved in a robust, cross-functional response.

Authors



John Gelinne

Cyber Resilience Leader
Deloitte Global
US

Melinda Upton

Partner
Deloitte Tax & Legal
Australia

Nikola Werry

Partner
Deloitte Legal
Germany

Deloitte Legal has 2,500+ legal professionals in 75+ geographies.

Find key contacts by solution, industry, and in your country.

Deloitte.
Legal