Best Practices for California Attorneys Advising Corporate Clients on Mitigating Cybersecurity Incidents

Cybersecurity risk has never been more complex and fraught with peril for California companies and the attorneys advising them. As more sophisticated and frequent attacks leverage artificial intelligence, geopolitical conflict and other disruptive forces, organizations are left scrambling to keep pace with evolving threats and mitigation expectations. Corporate espionage — often facilitated by insider mistakes or overlooked vulnerabilities — also poses a growing and often understated risk. Many of the most destructive cyberattacks are state-sponsored, with governments in China, Russia, North Korea and elsewhere funding massive operations.

Meanwhile, general counsels (GCs) across industries **report increasing fatigue** due to the relentless onslaught of attacks, ballooning responsibilities and limited internal resources. This combination of escalating risk and exhaustion can result in an environment where inaction becomes the default response, precisely when proactive measures are most needed. In an era of rapid technological change, understanding the human, legal and systemic dimensions of cybersecurity threats is critical to protecting clients and ensuring compliance.

This guide explores the evolution of cybersecurity threats, offering practical advice to help attorneys counsel clients on avoiding and mitigating incidents.

Understanding the threats

As attackers become more agile and better resourced, traditional approaches to cybersecurity training and awareness may no longer provide adequate protection against increasingly persuasive and technically sophisticated attacks. Here's what to know about the current and emerging threats.

Human vulnerabilities

The sobering truth about cybersecurity is that, despite growing investments in advanced technology and infrastructure, the vast majority of attacks begin with an email. Whether through mass phishing or highly targeted "spear phishing" campaigns, many attackers rely on a single human misstep, such as clicking a link, opening a file or responding to a seemingly legitimate request. This makes employees the most vulnerable entry point.

Rather than leveraging sophisticated malware, some of the most damaging breaches simply involve convincing impersonations of CEOs, vendors and IT staff seeking credentials or wire transfers. AI is exacerbating that problem, as attackers can now use generative tools to draft emails and messages that mirror a company's tone, context and even internal workflows. Phishing attempts that used to be easy to spot — thanks to egregious spelling errors and suspicious requests — have become highly personalized, grammatically flawless and contextually convincing.

Mitigate this risk with:

- **Regular phishing awareness training:** Educate employees on recognizing phishing attempts, focusing on new and evolving tactics, including AI-powered attacks.
- **Simulated phishing exercises:** Run regular, real-world phishing simulations to assess employee awareness and preparedness, followed by targeted follow-up training for those who fail the tests.
- **Multi-factor authentication (MFA):** Require MFA for accessing sensitive systems to add an extra layer of security in case credentials are compromised.
- **AI detection tools:** Invest in AI-powered tools to help detect and block AI-generated phishing attempts or malicious messages that mimic internal communication.
- **An incident response plan:** Develop and communicate a clear process for employees to report suspected phishing attempts and other suspicious activity immediately. CEB's Cyber Threat Response Kit explains how to draft a robust plan.

GC fatigue

The more cybersecurity threats escalate, the more fatigue GCs are reporting, especially as they're asked to do more with fewer resources. Juggling incident response planning, vendor due diligence, evolving regulatory frameworks and board-level expectations, many GCs are stretched thin.

This chronic strain can lead to decision fatigue, delayed action or even strategic paralysis — right when cyber threats are becoming more sophisticated and relentless. This fatigue is not just a symptom but a risk factor in itself. When legal teams are overwhelmed, vulnerabilities multiply.

Mitigate this risk by:

- **Outsourcing certain cybersecurity functions:** Consider bringing in external cybersecurity professionals to handle certain aspects of incident response, compliance monitoring and vendor management to ease the burden on in-house GCs.
- **Prioritize risk management:** Develop a tiered approach to managing cybersecurity risks based on their severity and potential impact, allowing GCs to allocate resources efficiently.
- **Automate routine tasks:** Leverage automated tools for routine compliance checks, monitoring and risk assessments to reduce manual workload and decision fatigue.
- **Cross-departmental collaboration:** Encourage collaboration between legal, IT and HR departments to share the responsibility for cybersecurity initiatives and reduce the load on any one department.
- **Cybersecurity insurance:** Consider insurance to mitigate financial and operational risks in the event of an incident, allowing GCs to focus on more strategic decisions.

State-sponsored cybercrime and corporate espionage

Cyberattack groups typically operate independently but are often state-sponsored. For instance, Russia has a long history of backing cybercriminal groups to further its geopolitical goals. Ransomware activity dipped in 2022 due to Russia redirecting its hackers toward Ukraine during the war, but attacks **rebounded in 2023**.

Also on the rise is corporate espionage, whether perpetrated by foreign actors or competitors. Be on alert not just for overt attacks but also subtle efforts to access intellectual property, strategy documents or financial data — especially as remote and hybrid work blurs the boundaries between personal and corporate systems.

Mitigate this risk by:

- **Securing critical infrastructure:** Prioritize securing the most sensitive intellectual property, financial data and strategic plans against potential corporate espionage using encryption and advanced security protocols.
- **Creating backups:** Implement redundant systems and backup data to mitigate the impact of potential disruptions or attacks from state-sponsored entities.
- **Ensuring cross-border compliance:** Ensure that your cybersecurity practices comply with international regulations, especially regarding state-sponsored threats targeting global operations.
- **Protecting remote work:** Establish strict security measures for remote and hybrid workforces, including virtual private networks (VPNs) and endpoint security tools.

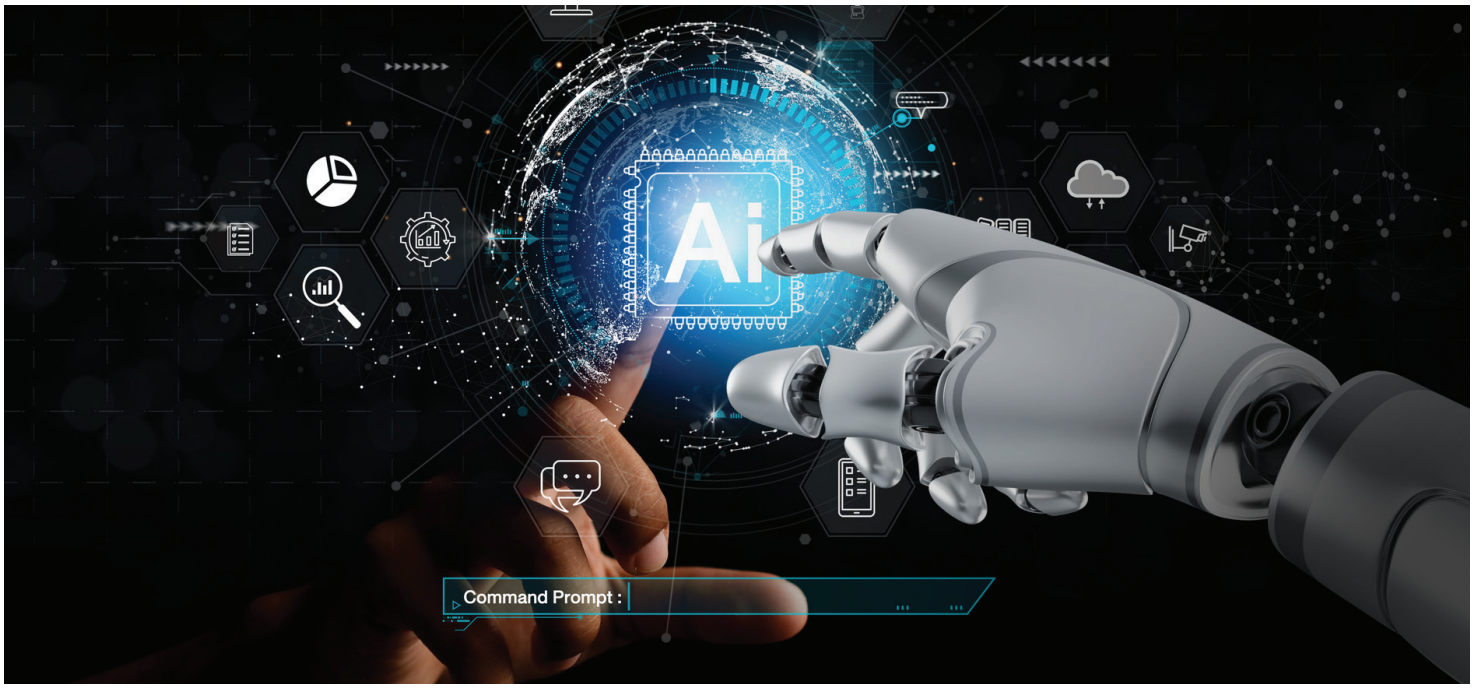
AI amplification

AI is amplifying cybersecurity risks by enabling bad actors to weaponize existing tools, accelerate the speed and frequency of attacks and create more convincing phishing campaigns. Tasks that once took hours or days for attackers can now be accomplished in seconds.

The technology has lowered the barrier to entry for less sophisticated hackers while allowing more advanced groups to automate complex operations and better evade detection. As these tools become more accessible, the volume and sophistication of cyber threats are expected to grow.

Mitigate this risk with:

- **Advanced threat detection tools:** Invest in AI-powered threat detection systems that can identify unusual behavior and prevent advanced phishing or malware attacks.
- **Behavioral analytics:** Monitoring deviations from normal user activity can help identify AI-generated malicious activity.
- **AI-powered response plans:** Consider incorporating AI-based response systems that can automatically contain and mitigate attacks in real time, such as isolating compromised devices or accounts.
- **AI defense training:** Train internal teams on the risks posed by AI-enhanced attacks and how to combat them.
- **Continuous monitoring:** Implement continuous monitoring tools that can detect and flag unusual activity or anomalies potentially related to AI-assisted attacks.



Polyworking

One emerging and underappreciated cybersecurity concern is polyworking, where remote employees hold multiple jobs at once, often without employer knowledge. While still considered a fringe practice, it introduces real risks. If a device used for one employer is compromised, it could inadvertently expose another company's sensitive data or systems, causing a chain reaction of legal and security issues.

Mitigate this risk with:

- **Clear polyworking policies:** Establish policies on remote working and polyworking, outlining acceptable use of devices, data handling procedures and conflict-of-interest expectations.
- **Secure BYOD (Bring Your Own Device) policies:**
  If polyworking is allowed, implement strict security protocols for personal devices used for work, including mandatory security software, encryption and regular monitoring.
- **Regular audits:** Regularly audit devices and accounts to ensure they comply with internal security standards, especially in remote and hybrid working environments.
- **Data segmentation:** Dividing data into distinct categories or groups based on various factors ensures the most sensitive data is stored and accessed separately from personal or less secure devices.
- **Employee monitoring and reporting:**
  Develop tools and procedures to detect unauthorized access to systems or suspicious activity, and encourage employees to report any concerns about polyworking practices.

Third-party vendors

It's not enough to keep your own house in order. As organizations increasingly rely on third-party vendors for critical services and operations, each partnership introduces significant cybersecurity risks. Vendors often have access to sensitive systems and data, making them an attractive target for attackers seeking to exploit weaker security measures outside the organization's direct control. A single compromised vendor can create a cascading effect, exposing multiple companies to breaches or operational disruptions.

One of the greatest challenges is the lack of visibility into vendors' security practices. Many organizations assume their partners adhere to robust cybersecurity standards, but this is not always the case. High-profile incidents like the SolarWinds breach have demonstrated how supply chain vulnerabilities can lead to widespread consequences, affecting thousands of businesses globally.

Mitigate this risk with:

- **Vendor risk assessments:** Conduct thorough security assessments before onboarding third-party vendors, evaluating their cybersecurity posture and compliance with industry standards.
- **Contractual safeguards:** Include cybersecurity clauses in vendor contracts that require vendors to meet specific security protocols, undergo regular security audits and notify the organization promptly of any breaches.
- **Vendor access control:** Limit vendor access to only the systems and data necessary for their specific role, using the principle of least privilege to minimize the exposure of sensitive information.
- **Risk management tools:** Use automated third-party risk management platforms to continuously monitor and assess the cybersecurity practices of vendors and other external partners.
- **Incident response coordination:** Ensure that third-party vendors have an incident response plan in place that aligns with the organization's own procedures, including breach notification and remediation timelines.

Cybersecurity is a cultural issue too

Today's cybersecurity challenges are not just technological but also human and organizational. Protecting sensitive data and systems requires more than the latest technologies — it demands a shift in mindset across an organization to foster an environment where security is not an afterthought but a core value.

GCs and outside counsel play a pivotal role in shaping this culture, especially when it comes to creating an environment where admitting mistakes is not feared but encouraged. Cyber incidents often escalate when employees are too afraid to report mistakes or breaches, fearing repercussions.

The cost of inaction is too high. In addition to complying with relevant laws such as the California Consumer Privacy Act, adopt clear strategies, invest in employee education, vet vendors and encourage openness and accountability to spot and address issues early, minimizing damage.

For more insights into handling security breaches and California data privacy laws, get in touch to schedule a free demo.

CEB

Contact us at 1-800-232-3444 or visit us online to learn more.