Perkins Coie

PRIVACY & SECURITY

Top 10 Security Issues To Consider

Cyber is a top risk across every industry, and every guide will tell you to engage leadership, develop an incident response plan, and know your data. Below are ten more specific strategies our data security professionals have identified for dealing with current cybersecurity risks and threats.

1. **Develop and practice an incident response plan that includes ransomware.** Incident response plans are a cornerstone of preparedness. Ransomware often creates more complex and public challenges, under a tighter time frame, than other types of incidents. A team that practices those circumstances will be better positioned to respond quickly.

2. **Educate employees on phishing.** Compromising a single employee's credentials is often the way in for ransomware and other security incidents. Ensure employees are regularly made aware of their role on the front lines of your company's security.

3. **Log potential access to sensitive information.** Whether it's your email, external storage systems, or proprietary systems, consider what you would know about an unauthorized actor's access—not just whether they got in, but what they did. Would you know if they accessed your most sensitive files?

4. **Look for ghost data.** Data of which a company is unaware can often cause problems. Review departments with access to sensitive employee and user data and look for backups, duplicates, data exports, and other unnecessary caches of sensitive information that can be removed or secured.

5. **Prepare for bot login attacks.** Bad actors use bots to launch credential stuffing or password spray attacks that attempt a large number of credentials against a login portal. They rely on users' poor password hygiene and exploit poorly segmented or secured online environments. Review measures to limit the impact and scope of attacks, including rate limiting, IP blocks, zero trust principles, and limiting visible sensitive information.

6. **Check your insurance.** Review your insurance coverage to ensure it covers your likely risks and costs and includes your preferred counsel and other vendors.

7. **Review the SEC disclosure rules.** Public companies must disclose material cybersecurity incidents like they do for any other significant events. Ensure that your incident response plan includes notifying securities counsel and be aware of forthcoming new rules from the U.S. Securities and Exchange Commission (SEC) about a deadline on such disclosures.

8. **Review compliance with known cyber frameworks.** Compliance with known and respected cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework or International Organization for Standardization (ISO) 27000 series, can provide benefits beyond the diligence required to comply with the framework's requirements. Compliance can provide a safe harbor from litigation in a growing number of states and is increasingly expected as a standard for "reasonable" data security.

9. **Review new compliance regimes.** If your company does a significant amount of business in California or is in the financial or health space, substantial new security and breach notification obligations are changing this compliance landscape. Incident response plans and other security processes may need updates to comply.

10. **Assess risks related to ERISA plans.** The U.S. Department of Labor (DOL) recently issued detailed cybersecurity governance related to employers' duties to protect assets in employee benefit plans--often an overlooked segment of a cyber program. Companies need to ensure that their program covers employee and plan data and can be produced to the DOL in the event of an audit.

How We Can Help

Our experienced incident response professionals have handled hundreds of incidents of all sizes, from complex advanced persistent threats (APTs) and widespread international consumer data breaches to sensitive employee disclosure issues. We assist with matters ranging from triaging a minor occurrence to support for a major incident with our deep bench experience coordinating law enforcement, forensics, data analysis, and breach services vendors. But outside of a crisis, we can also bring a wide variety of skills to help with the issues raised in this bulletin, and more.

Cybersecurity risk assessments. An effective risk assessment allows senior management with any level of technical knowledge to fully understand what is going on "under the hood" of their information security function. We regularly work with technical consultants to manage enterprise cybersecurity risk assessments, with a focus on ensuring that legal risks (presented by the constantly growing body of cybersecurity regulations) are identified and meaningfully presented under privilege, alongside the technical results of an assessment.

Incident response plan development and assessment. Compliance with legal breach notification and documentation requirements requires a robust program to identify and address security incidents occurring throughout your company and its service providers. We review your existing plan(s) to ensure that you are properly staffed and prepared to efficiently address technical, practical, and communications issues that create legal risk for the company.

Tabletop exercises. Tabletop exercises test a company's incident response against its existing team's resources. They can serve a variety of purposes, from high-level team building to specific skill development to the exposure of particular weaknesses. We work with our clients to identify specific goals and customize sessions, providing follow-up to help address vulnerabilities and revise the incident response plan.

Security program review. We review and revise written security plans for compliance with evolving state, federal, and international requirements and best practices and help companies expand and deepen their policies as they grow.

Insurance checkup. We work closely with lawyers in the firm's nationally recognized Insurance Recovery practice to help clients assess insurance coverage and potential indemnification rights. Our insurance lawyers can quickly evaluate clients' policies to determine the scope of any coverage and whether triggering coverage is advisable. We also work with our clients to advocate for control over the litigation and the selection of counsel.

Securities counsel. Collaborating with public company securities counsel, we help develop policies and procedures and ensure timely assessment of reporting obligations arising from security incidents.

Law enforcement introductions. We can provide industry-specific and often local introductions to cyber law enforcement across the country to help establish relationships before a crisis develops.

Employee training. We develop and present employee training on privacy and security issues, as well as assist companies with reviewing existing training for legal compliance.

Privacy solutions. Our firm's proprietary tools help clients streamline key privacy and data security compliance obligations, including Data Navigator, our data mapping tool, and the Privacy Starter Kit, a compilation of roadmaps, checklists, templates, and guidance documents designed to help clients comply with the General Data Protection Regulation (GDPR) and omnibus state privacy laws.

David Aaron
SENIOR COUNSEL
WASHINGTON D.C./NEW YORK
DAaron@perkinscoie.com

Amelia Gerlicher
PARTNER
SEATTLE
AGerlicher@perkinscoie.com

Todd Hinnen
PARTNER
SEATTLE
THinnen@perkinscoie.com

Andrew Pak
SENIOR COUNSEL
LOS ANGELES
APak@perkinscoie.com