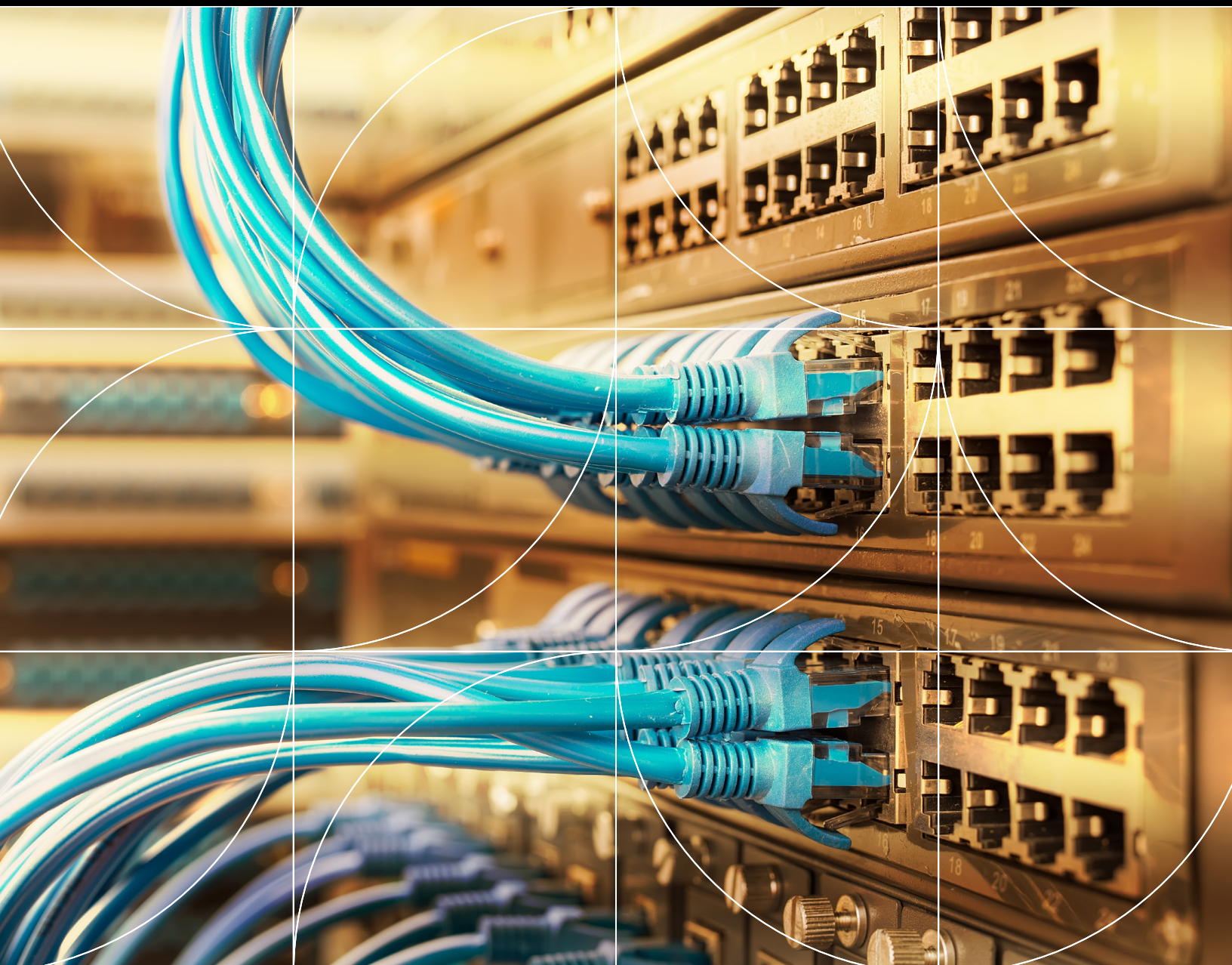
Seyfarth

Cybersecurity



Cybersecurity is a universal problem and no customers or clients are immune from it.

Historically, cybersecurity has focused on protecting the perimeter of a company's IT infrastructure, which generally meant cybersecurity was considered as a technical problem to address. Today, companies operate under a "presumed breach" approach, recognizing that a determined adversary will ultimately be able to breach any environment. As a result, the focus in cybersecurity now shifts from preventing an attack to quickly detecting the attack, containing the spread of the attack, mitigating damage, and investigating root cause. This has resulted in many companies taking risk-based approaches to managing its cybersecurity efforts. Managing risk in this area also naturally includes the legal risks to the company that are introduced by cyber incidents.

A major differentiator for Seyfarth in the Cybersecurity Legal Services area is that our attorneys who practice in this area are not just cybersecurity lawyers but are also experienced information technology and security professionals. The attorneys who do this work have degrees in Computer Science and Mathematics, are certified ethical hackers, and are certified digital forensic examiners. They also have industry experience including software, network, and systems engineering and administration, programming, and a wide range of other information technology disciplines. Our attorneys truly understand the complex technical issues which give them much greater insight in addressing the legal issues as well as minimizing the need to hire other technical experts to assist the lawyers as many of Seyfarth's competitors do. Where specialized third party technical experts are needed, Seyfarth is also adept at managing scope to control client costs. We understand not only the big picture, but which details are necessary and unnecessary when handling a cybersecurity incident, including early incidia of potential legal ramifications and loss mitigation.

Cybersecurity Legal Services

Seyfarth's eDIG practice group specializes in a variety of Cybersecurity services, including:

Incident Response

Data breach notification statutes and regulations have been around for a long time. However, more recently, the Global Data Privacy Regulation ("GDPR") as well as recent state regulatory efforts have wildly accelerated the time to notify regulators of a data breach, including in some instances "72 hour" notice provisions. When a security incident is suspected or detected, Seyfarth is experienced in helping clients take immediate first steps toward investigation, assessment, containment, and recovery.

Key services include:

Privileged Incident Response Investigations

We are frequently engaged at the very beginnings of a suspected data breach as part of a company's overall incident response program. Being engaged at the beginning, and working hand in glove with the information security group, we can maximize the opportunities to claim attorney client privilege over any investigation.

Data Breach Notifications

The term "data breach"is commonly overused. A security incident is not a data breach until verified. For those clients whose matters escalate to an actual breach of data, we have a long history

of assisting clients in their legal and regulatory obligations. First and foremost, this requires an understanding of the technical nature of the breach—determining what we "know," what we "believe," and what is "possible" are not easy questions and require an understanding of both the technical and legal aspects of the incident.

Assisting Legal Department in Data Breach Management
Many law departments have found themselves taking a key role in the management of data breaches. A breach triggers many more issues than the pure legal obligation to report. Even if the technical requirements are not met, companies increasingly have found themselves wanting to share information with the public, shareholders, and with regulators in a much more proactive way. If the breach involves "ransomware," the law department must consider the pros and cons of paying the ransom. Decisions also must be made as to the desirability of notifying law enforcement. Further, the decisions of whether to obtain cyber insurance as well as how to ensure that you get the most out of your coverage are often issues for the law department. We regularly assists clients in these areas and has active relationships with cyber insurance brokers.

Client Program Development

Preparedness is the best defense. Our clients turn to Seyfarth for help developing programs within their companies to understand potential risks, establish best practices to reduce them, and internalize a culture of risk-reduction for best results.

Maturity Assessment
We have assisted many clients in assessing the maturity of their cybersecurity and information governance programs. We have done this work, sometimes in conjunction with an information security consultant group, on all ranges of the spectrum—whether you are a company trying to initially develop your program and want to understand where to start or are a company that has a very mature program, Seyfarth has considerable experience performing these assessments under attorney client privilege and with a thorough understanding of the sensitivity of the results of these assessments.

Vendor Assessment and Master Service Agreement (MSA) Negotiation
Seyfarth believes it's important to have resources identified, including vendors, well ahead of the breach. We have aided clients in identifying those resources and negotiating and executing those arrangements including often three party agreements between the vendor, the client, and the law firm.

Policy and Practices Development
We have assisted clients in the development of their information security policies and practices.

Testing your Practices
A written policy or practice is of little use if it's not ready to be executed. We assist clients in performing table top exercises and other drills to ensure that the client is ready to execute in the event a data breach investigation commences.

Training
Humans unfortunately play a major role in increasing cybersecurity threats. A majority of successful cybersecurity incidents involve some form of human failure. Many times, attackers utilize social engineering to pray on company employees human nature and willingness to help to coerce them to violate policy. Hackers often study target companies and prepare social engineering attacks for months prior to utilizing any technical attack vector. Having a robust training regimen with rigorous employee testing is paramount to successfully upholding front lines of defense against cyber threats. Seyfarth has developed, as part of its @Work platform, a thorough training module for cyber education for employees. This initial training, when paired with periodic, unannounced employee testing (such as managed test "phishing" attacks, for example), allows an organization to discover their employees' aptitude in noticing threats.

Regulatory Guidance

With the volume and complexity of regulatory activity in any area, companies are challenged to stay abreast of their applicable requirements.

In the areas of security and privacy, our clients want to work with legal counsel that is completely up to date and informed of any moving issues that might affect them. Seyfarth attorneys counsel on requirements and regulations from all federal and other governmental agencies. This includes rules and guidance, issued by or in regard to, the Securities and Exchange Commission ("SEC") rules, adherence to Sarbanes Oxley requirements, the New York State Department of Financial Services ("NYDFS"), the Federal Trade Commission ("FTC"), Federal Acquisition Regulations (FAR cybersecurity requirements), and many more.

National Institute of Standards and Technology (NIST)

We also provide guidance in accordance with the US Commerce Department's NIST Framework for Improving Critical Infrastructure Cybersecurity including the related NIST special publication 800-171 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." The framework is a guide for voluntary adherence which helps organizations find and mitigate risks in cybersecurity which was originally initiated with a particular focus on industries at risk of greatest economic and military security threats. It has since evolved for adoption by organizations of all sizes and is updated regularly, most recently with Version 1.1 in April of 2018.

Federal Acquisition Regulation Cybersecurity Requirements

Seyfarth attorneys in multiple areas within our firm are astutely experienced in handling legal matters surrounding the regulations. We advise on FAR and DFAR legal requirements within the context of government contracts matters. Our eDiscovery practice group will work in tandem with our government contracts practice group.

Internal Audit Approach to Risk Assessment

Some companies choose to use internal audit as a means to maturing cybersecurity programs. Rather than taking a traditional approach of audit finding, management response, and conditions for closure, we have worked with clients to work with internal audit and sometimes outside consultants to assess and develop advisory opinions to aid in the further maturing of the cyber program. Taking this approach, our clients have the benefit of attorney privileged communications working with Seyfarth. This overlay of additional confidentiality is not available through consultants, and neither are consultants able to counsel on the legal risks at play while performing the audit. An effective tool for the audit process is our use of "Red Team/Blue Team" Exercises. In these arrangements, we work with our client's Red Team or outside Red Teams to conduct in-depth attacks that are tailored to a likely threat actor and to reinforce findings in the advisory opinion or in areas where the Chief Information Security Officer may believe the cyber program is reasonably mature—and all under confidential legal privilege.

Privacy & Security Issues Training

Client education is a big part of our firm's culture and customer service focus. Cybersecurity issues are especially sensitive to training quality due to the high number of potential risks that exist from internal, external, and third party sources. We work with our clients to provide education content, materials, and presentations to Executive Boards and corporate C-Suite personnel. Additional training for managers within our clients' organizations is also key so they can in turn educate employees on a daily basis and by example. An example of training we have provided our clients includes a training session involving real time feedback.

Track Record of Results

Our attorneys represent numerous leading companies—including Internet retailers, financial institutions, hotel franchisees, transportation companies, real estate management companies, software companies, third-party administrators, consumer electronics manufacturers, and retail grocery stores—have enlisted our firm to assist in responding to security incidents, developing responsive programs to privacy and security threats, advising on new business and technology models, and negotiating with parties up and down the supply chain. We understand our clients' challenges to preparedness and help overcome

them. Our focus is to help Seyfarth clients mitigate risk potential across their data and cyber information outlets.

Our Qualifications

Exceptionally Technical and Experienced Attorneys

Seyfarth cybersecurity and privacy attorneys bring a robust knowledge base on all areas of importance in this sensitive area of legal services, such as: Anti-hacking, programming/scripting, network security, system administration, intrusion detection system (IDS) monitoring for malicious activity or policy violations, active defense, databases, firewalls, law enforcement liaison, and more. This depth of knowledge is critically important to our clients, and it allows us to operate at the highly technical level of working closely with CIO/CISOs at Fortune 500 and higher companies.

Privilege Protection

The inherent value of legal confidentiality and the informational protection granted by that privilege cannot be understated. Indeed our actual assessment of risk involved is all taken in through the eye of a legal professional—again, under privilege. Third party security consultants cannot provide this benefit, either in consultation or attempts at risk assessment. Mitigating legal ramifications of our clients' threatening risks is as important as protecting the IT system, or the information itself. Our role is to protect the company, and legal privilege is a key tool in providing that valuable protection.

Single Point of Contact for All Breach Response Resources

True to our Seyfarth Lean roots, Seyfarth attorneys remain focused on our clients and efficiently meeting their needs. Operating with ultimate efficiency is a natural extension of our Lean culture and philosophy. As a result, working with Seyfarth for your security and privacy issues gives you a highly knowledgeable, single point of contact who is intimately familiar with your company's data concerns. Knowing who to call on a moment's notice is cost-saving for clients—time is not wasted trying to figure out next steps. Simply call Seyfarth. We offer our clients a highly technical "quarterback" to run security breach response activity, augmented by the full team of security experts.

Agility of Response

Because of our client service focus, our cybersecurity single point of contact organization style, and the deeply experienced nature of your proposed team, Seyfarth clients get the correct answer—quickly—without the need for extensive legal research. Our practitioners maintain constant, practical knowledge of emerging technologies and issues, keeping Seyfarth ahead of the curve. Indeed, client service is our focus in all areas, providing prompt responses in technology and security areas especially.

Industry Leadership

Seyfarth attorneys are also closely Integrated within the industry and related government programs which affect security and data privacy matters. It is important to note that key Seyfarth attorneys are affiliated with the FBI in regard to its InfraGard Project. InfraGard is a partnership between the FBI and the private sector. It is an association of people representing businesses, academic institutions, state and local law enforcement agencies, and their participants dedicated to sharing information and intelligence to prevent hostile acts against the US Our attorneys are long-time affiliates with the organization and was appointed as Chairman of InfraGard's Legal Industry Special Interest Group for the Pacific Region.

Our Washington, DC office is also home to Seyfarth's Government Relations and Policy group, dedicated to identifying key legal and regulatory issues of interest to clients, to coordinate clients around certain regulatory issues, and to develop solutions and defenses for our clients in the employer community. This group also authors the firm's Policy Matters Newsletter of regular updates on the actions of Congress, administrative agencies, and other lawmakers at the federal, state, and local levels.

About Seyfarth Shaw LLP

With more than 900 lawyers across 17 offices, Seyfarth Shaw LLP provides advisory, litigation, and transactional legal services to clients worldwide.

Our unique combination of high-caliber legal representation and advanced service delivery allows us to take on our clients' unique challenges and opportunities—no matter the scale or complexity. Whether navigating complex litigation, negotiating transformational deals, or advising on cross-border projects, our attorneys achieve exceptional legal outcomes. Our drive for excellence leads us to seek out better ways to work with our clients and each other. We have been first-to-market on many legal service delivery innovations—and we continue to break new ground with our clients every day. This long history of excellence and innovation has created a culture with a sense of purpose and belonging for all. In turn, our culture drives our commitment to the growth of our clients, the diversity of our people, and the resilience of our workforce.

SEYFARTH IS:

BOLD
We are strong in the face of uncertainty, leading our clients through a rapidly changing landscape.

INVESTED
We are committed to partnership for the benefit of our clients, our people, and our community.

INVENTIVE
Our work makes a big impact through skill, creativity, and collaboration.

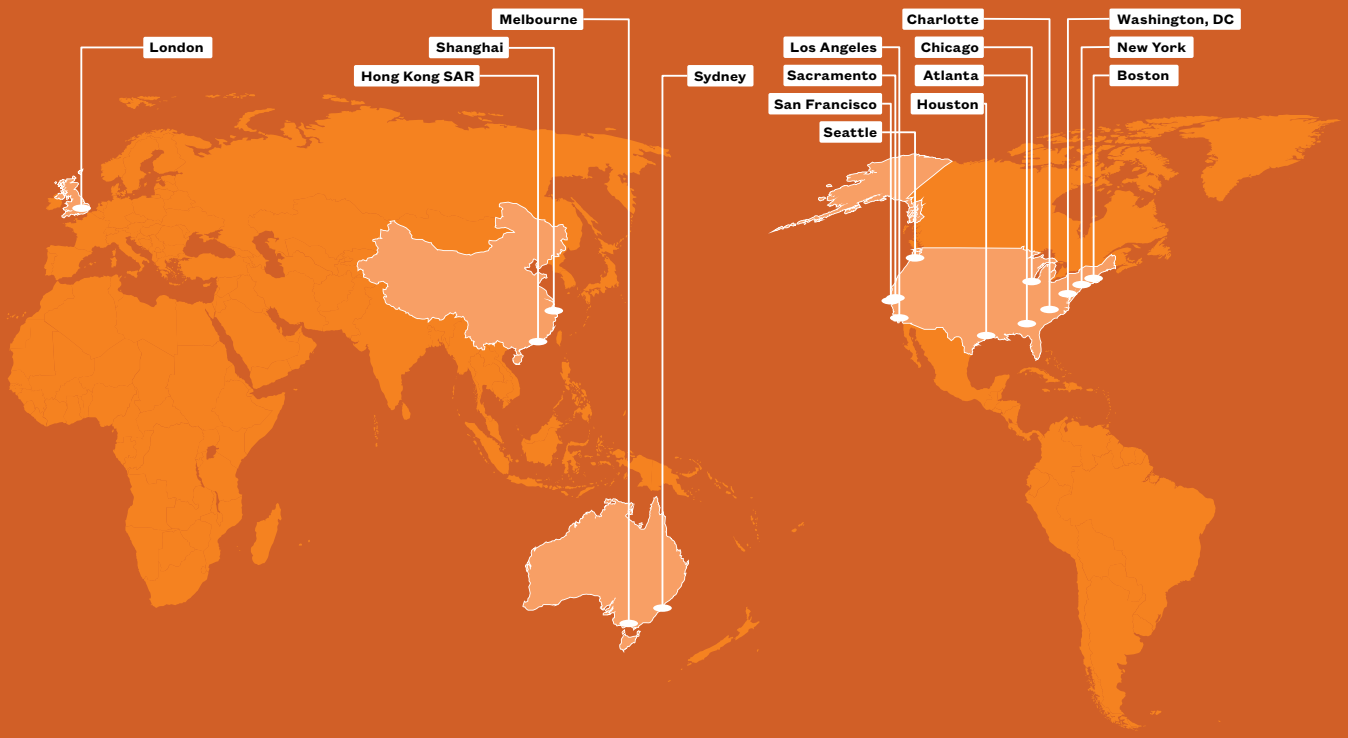
CONFIDENT
We are excellent at what we do, delivering exceptional results with purpose and determination.

Our innovation, culture, and legal work have been recognized by top-tier organizations around the world:

- Association for Corporate Counsel
- Chambers Asia-Pacific
- Chambers USA
- Financial Times Innovative Lawyers
- Human Rights Campaign Corporate Equality Index
- The Legal 500
- The Legal 500 Asia-Pacific
- Working Mother

Your needs serviced through an international model.

AN INTERNATIONAL FOOTPRINT



www.seyfarth.com

#19-6911 M4