CYBER RISK MANAGEMENT SERVICES

Is Your Company Prepared for a Cyber Attack?

ALSTON&BIRD


IDENTIFY
Senior Management and Board-Level Cyber Risk Consultation
Information Life Cycle Assessment
Cybersecurity Risk Assessment
PROTECT
Cybersecurity Program Legal and Compliance Review
Internet of Things and Technology Cybersecurity Risk Review
Third-Party Vendor Security Review
DETECT
Information Sharing Programs and Cyber Threat Intelligence
Vulnerability Disclosure Programs
RESPOND
Incident Readiness and Plan Review
Cyber Response Plan Testing and Tabletops
RECOVER
Cyber Insurance Review
SEC Disclosures Review

Cyber attacks are a reality of doing business in the 21st century. As a result, "check the box" cybersecurity—the idea that an organization can secure itself by implementing a predefined set of controls—is now antiquated, superseded by a new, risk-responsive framework: cyber risk management. Although it is by no means a new concept, cyber risk management has gained significant influence in recent years, not least because of NIST's 2014 *Framework for Improving Critical Infrastructure Cybersecurity*. The Framework encourages organizations to develop agile cyber risk management strategies that can adapt to keep pace with evolving threats. NIST broadly divides the Framework Core—a set of cybersecurity activities and desired outcomes—into five functions: Identify, Protect, Detect, Respond and Recover.

We understand the critical role that in-house counsel should play in helping their organizations become "cyber risk ready." Our goal is to help our clients bridge the gap between law, technology and security and overcome the hurdles between the Legal, IT and Information Security departments as they manage and mitigate cyber risk. Alston & Bird's Cyber risk Management Services are specifically designed around the five core functions of the NIST Framework with cyber risk management in mind. Our services leverage the strengths of our Cybersecurity Preparedness & Response Team, which includes former federal cybercrime prosecutors, information security professionals and attorneys with decades of experience working on global cybersecurity and other technical matters both in the private and public sectors and in the context of a wide variety of legal and regulatory settings.

These services have helped many of our clients—among the most sophisticated and complex multinational enterprises in the world—to effectively navigate the complete life cycle of cyber risk management. By focusing on preparing for cyber attacks, data breaches and other cybersecurity events, as well as demonstrating the requisite level of commitment to cyber risk issues, organizations of all sizes and maturity can reduce enterprise risk and increase the bottom line despite the inevitability of cyber attacks. These services can be offered on a flat-fee or alternative fee basis that is customized for each client's specific needs.

IDENTIFY

Understand and manage cybersecurity risks to systems, assets, data and functions

KEY FOCUS AREAS FOR IN-HOUSE COUNSEL

Senior Management and Board-Level Cyber Risk Consultation

In an era of increased cybersecurity scrutiny and litigation, it is important for senior management and directors to educate themselves on the cybersecurity risks the company may face, as well as those risks that any director may face individually. Board members must also involve themselves in the company's cybersecurity strategy before and after a data breach.

SERVICES:

Our services assist in providing senior management/board-level information security and cyber risk presentations and/or training covering responsibilities pre-breach and post-incident, emerging trends in cybersecurity corporate governance and strategies to minimize cyber risk exposure.

KEY EXPERIENCE:

- Developed training materials for the boards of directors of several companies, including major banks, one of the world's largest construction and industrial equipment rental providers, a global non-car vehicle manufacturer, a global digital media company and a large insurance company. The presentations and materials highlighted the companies' cybersecurity risks and the legal and regulatory landscape and provided recommendations for overseeing improvements to their companies' data security posture as part of cyber risk management.
- Presenting annually to the board of directors of one of the largest U.S. financial institutions on issues of cyber risk and cybersecurity, including evaluating the board's duties in this area.

IDENTIFY

Information Life Cycle Assessment

What data does your organization create and receive? Where is it located? How is it used? How long is it retained? What is your retention policy? How is your data protected? Who has access to your data? What laws govern the data you collect? Understanding what data you have, what your crown jewels are and where that data resides is the first step in understanding how that data needs to be protected.

SERVICES:

Our information life cycle services are designed to get your organization on top of its data use practices and then regularly review its data practices to minimize ongoing exposure. These services generally include data inventorying and information-transfer analysis, IT environment-mapping exercises, privacy compliance analysis and information policy and privacy statement review and development.

KEY EXPERIENCE:

- Develop and coordinate information inventory, data flow and risk assessment initiatives for leading global brands in industries such as transportation and logistics, travel, hospitality and quick-service restaurants. Our work has included designing information lifecycle assessments, coordinating data flow diligence, quantifying liability and regulatory risk issues and developing recommended mitigation paths for senior executive management.

- Support privacy functions at client organizations in developing internal information governance models and policy, standards and guidelines development and implementation.

Cybersecurity Risk Assessment

To effectively manage cybersecurity risk, organizations need to know both where their cybersecurity program currently stands and where they think it needs to be. Indeed, in order to understand what controls and safeguards are necessary to mitigate cybersecurity threats, and implement effective detection methods for those threats, the starting place is often a cybersecurity risk assessment.

SERVICES:

Our Cybersecurity Preparedness & Response Team assists clients in this undertaking by performing privileged cybersecurity legal and risk assessments of their cybersecurity programs, often working with third-party

security consultants that specialize in this area to take advantage of their technical expertise and sophisticated tools. These assessments typically consist of two phases: (1) onsite interviews with subject-matter experts to understand how they view the organization's practices and to identify relevant documentation for our review; and (2) presentation of our findings in a written report.

KEY EXPERIENCE:

- Advising an independent county agency in a privacy and data security assessment regarding its policies, practices and procedures. The project includes conducting detailed client interviews, policy review and preparation of memoranda regarding identified gaps.

- Performed cybersecurity legal reviews for clients in many industries, such as transportation.

- Worked with an international monetary organization in connection with a multiphased, comprehensive information security risk assessment based on the global information security standard ISO 27001. Our involvement included leading a "threat-modeling workshop" to help the company understand its current threats and defenses and identify any known gaps in its information security infrastructure, in particular with state-sponsored and other sophisticated attacks.

- Worked with a multiservices organization in connection with a multiphased, enterprise-wide security risk assessment in which we led an incident response workshop and cyber tabletop exercises to identify any known weaknesses in incident response processes and procedures, in particular with scenarios related to sophisticated cyber attacks and intrusions.

- Worked with a large global consulting firm in an assessment of the company's practices, controls, policies and procedures that manage the ease with which sensitive client data and confidential company data could leave the company's systems, whether by an inadvertent act by an employee or a malicious act by an insider or an outsider.

Cybersecurity Program Legal and Compliance Review

Domestic and international legal regimes provide a vast array of rapidly evolving data privacy, security and data breach notification compliance obligations. Many laws on the books were written before many modern technologies were even conceived. Our Cybersecurity Preparedness & Response Team works with an international network of firms to help our clients first identify which laws apply to their business, and then stay on top of important changes. We go beyond most firms in this regard, helping implement and advise on additional corporate compliance and risk assessment initiatives. Importantly, companies with established cybersecurity programs should consider evaluating their program against the rapidly changing domestic and international legal regulatory environment, whether those changes are based on new regulatory guidance, enforcement actions or regulations.

SERVICES:

Our Cybersecurity Preparedness & Response Team assists clients in these evaluations with a defined methodology based on industry and the company's cybersecurity risk profile. We customize our reviews based on the applicable regulatory standards, controls or recommended frameworks. Our typical services in this area include compliance obligations identification and review, formal risk assessment practices review and a client security questionnaire review and strategy.

KEY EXPERIENCE:

- Conducted a cybersecurity preparedness legal review for a large state bank, assessing its cybersecurity program against guidance from federal and state financial regulators, and presented findings to the board.
- Conducted an enterprise-wide privacy and data security assessment for a large entertainment media company, assessing its practices for managing and securing sensitive information against a number of laws, regulations, enforcement actions and guidance materials from regulators. Assisted in performing a risk assessment using the NIST Framework to enable the company to prioritize its remediation and improvement activities.

Internet of Things and Technology Cybersecurity Risk Review

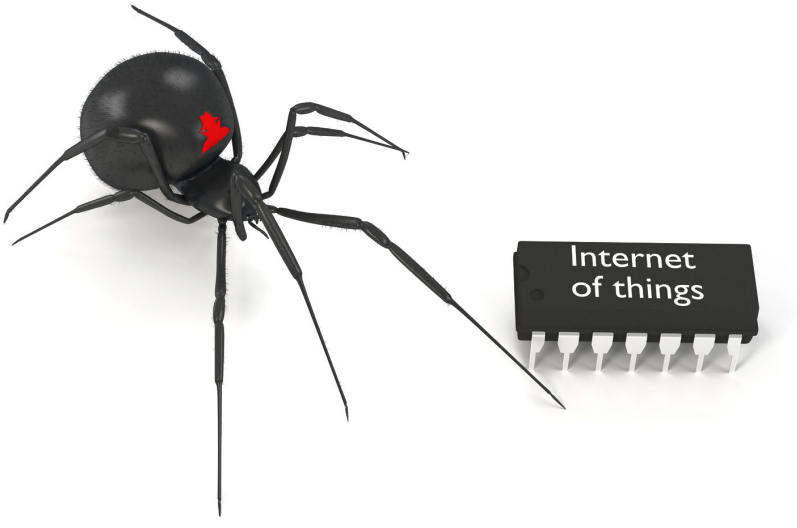
With the increasing attention to security vulnerabilities in products and services, and connected devices in particular, companies are increasingly expected to be actively, and even proactively, engaged with vulnerability management and incorporating sound security practices into the design of new products and services.

SERVICES:

Our Cybersecurity Preparedness & Response Team assists clients in cybersecurity risk reviews of new products and technologies early in the development process to help ensure the security practices are consistent with regulator expectations and industry standards. We also conduct reviews of security-related technologies to identify whether specific uses may raise any federal or state statutory or constitutional concerns, such as implicating the federal Computer Fraud and Abuse Act or state and federal Wiretap Acts.

KEY EXPERIENCE:

- Conducted privacy impact assessments and reviews in coordination with security risk assessment processes on emerging technologies and innovative new products for numerous clients across industries.
- Analyzed new security-related technology and service offerings for financial firms and technology companies for compliance with the CFAA, Wiretap statutes, and state privacy statutes and identification of state and federal constitutional implications.



IDENTIFY

Third-Party Vendor Security Review

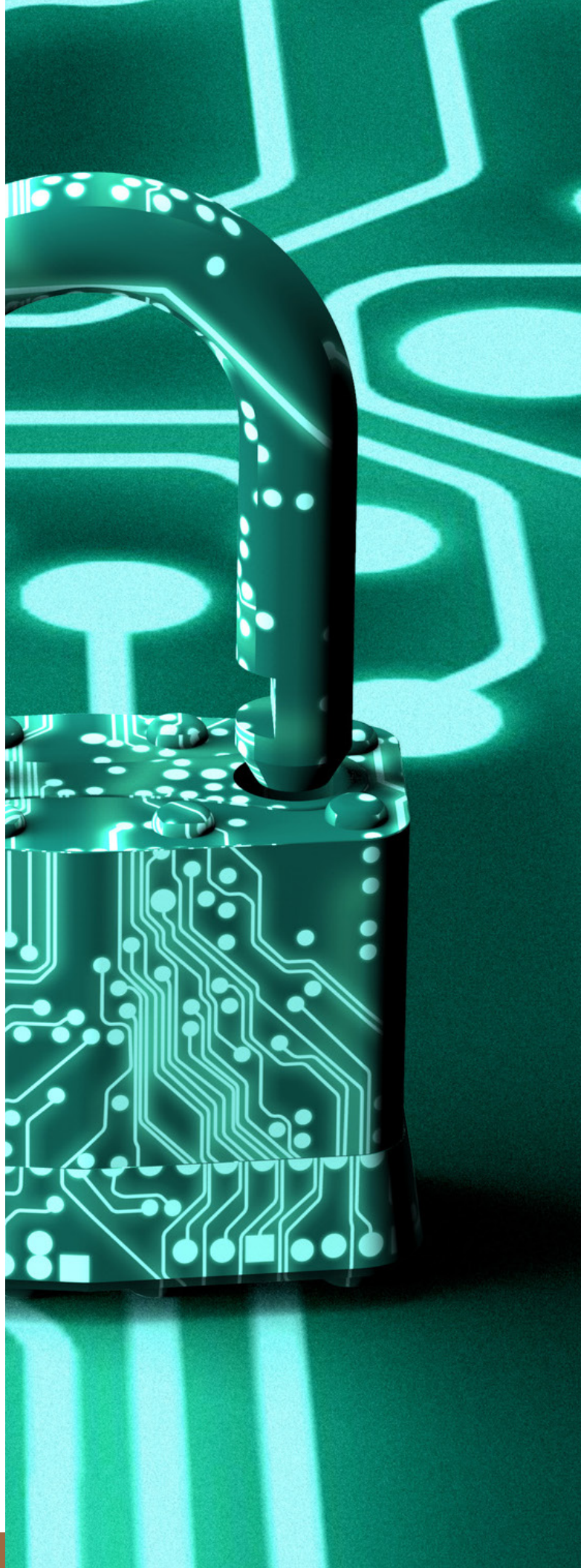
Ask any CISO where their biggest data security concerns lie, and third-party vendors will be at or near the top of their list. Many third-party contracts were signed long before data privacy and security concerns were hitting company radars. In many instances, third-party vendors have nearly unrestricted access to the operating systems critical to your day-to-day operations, yet frequently have minimal obligations to protect your company.

SERVICES:

Our services are designed to bring your existing vendor contracts up to date and in line with regulatory requirements (such as in the government contracts space), enhance your vendor form agreements and generally update your vendor risk management practices. We also work extensively with clients on comprehensive vendor management initiatives and deliver fixed- and alternative-fee arrangements for program startup and continuation. These services often include third-party vendor identification and data exchange review, contract review and update, and ongoing security maintenance.

KEY EXPERIENCE:

- Negotiate information security terms including security program requirements, technical security standards, industry standard certifications and compliance, security incident handling and liability allocation, and audit and oversight rights for customers and service providers across industries. Examples include requirements for hardware suppliers in product development and engineering and standards compliance.
- Develop standard form information security requirements for vendor contracts and develop associated vendor diligence policies for the world's largest transportation and logistics provider.
- Develop "best practice" provisions addressing data privacy and cybersecurity for inclusion in vendor contracts, and associated negotiation guidance, for financial services clients.



PROTECT & DETECT

Develop controls and safeguards to mitigate cybersecurity threats; identify cybersecurity-related events in real time

KEY FOCUS AREAS FOR IN-HOUSE COUNSEL

Information Sharing Programs and Cyber Threat Intelligence

Companies, especially those designated as critical infrastructure, need to keep abreast of cybersecurity developments and initiatives by the federal government, regulators, industry trade groups and public-private sector information-sharing groups. Receiving some form of cyber threat intelligence is considered to be a critical part of an entity's cybersecurity program. In some industries, companies are expected to participate in information-sharing groups, whether ISACs, ISAOs or less-formal platforms. In addition, in light of the passage of the Cybersecurity Information Sharing Act in 2015, companies should consider incorporating cyber threat intelligence sharing into their risk management processes.

SERVICES:

A sampling of our services in this area includes overall cybersecurity policy development; information-sharing risk framework development, legal requirements and disclosure protections; cyber-intelligence-gathering mechanisms and strategy development; and reporting on ongoing government initiatives and developments.

KEY EXPERIENCE:

- Representing a financial services information-sharing advisory association on various issues related to information sharing and cybersecurity in the financial services sector.
- Represented a retail industry trade association on issues related to cybersecurity information-sharing mechanisms and related congressional testimony.
- Worked with a global transportation company in developing cybersecurity policies and strategies. The project included ongoing monitoring of federal government initiatives dealing with critical infrastructure cybersecurity and development of appropriate responses, policies and procedures related to cyber intelligence gathering, information sharing and cybersecurity practices.

Vulnerability Disclosure Programs

Many companies are beginning to understand that they do not need a data breach to face regulatory and litigation exposure from cyber risk. Security vulnerabilities alone can bring them under scrutiny for their cybersecurity practices. As a result of the potential exposure to cybersecurity vulnerabilities—or because of regulatory expectations, depending on industry—many companies are considering, or adopting, vulnerability disclosure programs (or "bug bounty" programs) to encourage individuals who discover vulnerabilities in products and services to bring them to the attention of the company before going public.

SERVICES:

We help companies evaluate, design and implement vulnerability disclosure programs in line with regulator expectations and based on the company's cyber risk profile.

KEY EXPERIENCE:

- Assisted a global e-commerce company in evaluating and redesigning its vulnerability disclosure program after numerous reports made pursuant to the existing program caused unwanted (and unwarranted) attention.
- Assisted a medical device company in reviewing its vulnerability disclosure program in line with regulator expectations.

RESPOND & RECOVER

Develop and maintain effective incident response processes and continuity plans to maintain resilience following a breach

KEY FOCUS AREAS FOR IN-HOUSE COUNSEL

Incident Readiness and Plan Review

The potential financial, reputational and legal exposure of a breach is too great to not be adequately prepared. In addition to data loss from a breach, cyber incidents can also disrupt, and in some cases destroy, systems and networks, causing a significant operational impact. We counsel clients on recommended practices to prepare relevant corporate stakeholders for the eventual cyber incident or data breach and help them develop a strong incident management process that is tailored to their company and appropriately builds in business continuity and cyber resilience planning.

SERVICES:

We advise entities on developing one-, two- or three-tiered incident management processes depending on the size and scope of a company's operations and regulator expectations pertinent to their industry. For many companies, we recommend the development of a three-tiered structure where entities have (1) a technical response plan to handle the IT and evidentiary aspects of investigating security incidents (and incidents that only require a technical response); (2) a business/legal response plan to address noncrisis security incidents that require legal involvement; and (3) a cyber crisis management plan that sits above these plans and brings together an executive-level team to handle incidents that could have a severe impact on the organization. Many companies may be more suited to having a single, comprehensive incident response plan covering all these aspects, which can be equally effective. We work with companies so that we understand their business and culture to develop a management process that is suitable to their unique needs. We also review existing cyber response plans to incorporate appropriate legal standards, rules and regulator expectations and integrate them with existing business continuity processes and procedures.

KEY EXPERIENCE:

- Representing one of the world's largest retailers in the development of its worldwide data breach response plan.
- Developed global breach response plans for a global insurance company with operations in 27 countries.
- Developed security incident and/or data breach response plans for several global insurance companies, financial institutions, e-commerce companies, retailers, global consulting firms and digital media corporations.

Cyber Response Plan Testing and Tabletops

Companies are not only expected to have incident response and data breach response plans in place but they are also expected to test the plans to ensure they are effective within the environments where they will be used.

SERVICES:

Our services assist clients in formulating an effective mechanism to test these plans—including for both domestic and global operations, including:

- Developing scenarios for tabletop exercises and simulations.
- Advising on appropriate content, structure and attendees for exercises, including participation of various outside parties.
- Assistance with input of governmental agencies in advanced testing scenarios.
- Directing and supervising the testing exercises.

KEY EXPERIENCE:

- Developed and facilitated cyber tabletop exercises for one of the largest shipment and logistics companies in the world, a global provider of health services, one of the largest financial institutions in the U.S. and several large global insurance companies.
- Conducted international tabletop exercises in several Asian and South American countries for a global insurance company.
- Assisted all of these companies with enhancing their breach response strategies and procedures through prioritized recommendations and corrective action plans.

RESPOND & RECOVER

Cyber Insurance Review

As a key part of their incident response plans and procedures, companies should carefully consider whether they have adequate insurance coverage for cyber security risks, including coverage for forensic investigation, consumer notification, credit monitoring, call center operation, public relations, cyber extortion, regulatory investigations, payment card brand assessments and other third party claims.

SERVICES:

Our Cybersecurity Preparedness & Response Team has assisted many clients in assessing their current level of cyber insurance coverage, as well as identifying exclusions, conditions, and limitations that they should avoid.

KEY EXPERIENCE:

- Evaluated existing and/or proposed cyber insurance coverage for numerous clients across a wide range of industries, including media, restaurant, manufacturing, payment processing, shipment, merchant, and various other types of companies.
- Drafted proposed language to include in insurance policies to clarify the scope of coverage and narrow limitations and exclusions.
- Negotiated cyber insurance requirements in vendor contracts to ensure vendor systems and data are appropriately covered.
- Counseled clients regarding the pursuit of coverage and preserving their rights in the aftermath of cyber security incidents.

SEC Disclosures Review

Many public companies are well aware of the SEC's guidance on cyber risk disclosures, and the SEC's continued interest in reviewing such disclosures in the wake of a significant cyber event.

SERVICES:

Our Cybersecurity Preparedness & Response Team has assisted many public company clients in reviewing their cyber-related public filings to ensure that they are appropriate and sufficient, including by comparison to the disclosures of industry peers based on their industry presence and market capitalization.

And if you are the victim of an attack . . .
we are prepared to help you respond

CYBER INCIDENT RESPONSE SERVICES

Alston & Bird's Cybersecurity Preparedness & Response Team has helped companies large and small, international and domestic, and operating in a wide array of industries, both regulated and unregulated, respond to data breaches and cybersecurity incidents. Our attorneys have handled incidents of all sizes, from sophisticated cyber attacks by organized criminal groups (triggering data breach laws and regulations in more than 50 countries) and state-sponsored attacks to an employee accidentally sending an email with personal information outside the company (potentially triggering a single state breach notification law) and attacks causing disruption or destruction to systems and operational impacts to organizations, such as distributed denial of service attacks on websites and ransomware attacks locking up multiple employees' workstations. We also recognize that security vulnerabilities alone can bring our clients scrutiny for their cybersecurity practices, and we have helped our clients respond to reports from security researchers, government officials and others claiming a vulnerability in their systems, products, services or networks.

The depth of our Cybersecurity Preparedness & Response Team enables us to appropriately and sufficiently staff any incident response engagement regardless of the scale or level of complexity. Our team members are experienced in applying their skills and talent in the hypercharged environment that accompanies a sophisticated data loss event, cybersecurity incident or security vulnerability disclosure.

We have also established relationships with a wide variety of global security consultants during our security incident response engagements, which provides our clients with ready access to the latest forensic and investigatory tools on a moment's notice. If appropriate under the circumstances, we engage consultants directly in a manner designed to establish and enhance the attorney-client privilege for their activities. These relationships allow us to offer integrated services with cost-effective and efficient results, rather than deploying newly assembled teams where roles and responsibilities have not yet been established and may leave critical issues untouched.

Our team is prepared to assist you with incidents of any nature or scope. We are available to assist you 24 hours a day, seven days a week.

If you have any questions or would like additional information, please contact Kimberly Peretti, Jim Harvey or Michael Zweiback.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ALSTON&BIRD