# Table of Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Introduction</td>
</tr>
<tr>
<td>5</td>
<td>Market Overview</td>
</tr>
<tr>
<td>6</td>
<td>• Executive Summary</td>
</tr>
<tr>
<td>7</td>
<td>• Market Maps</td>
</tr>
<tr>
<td>10</td>
<td>• Demand Drivers</td>
</tr>
<tr>
<td>13</td>
<td>ALM Pacesetters: Cybersecurity Services</td>
</tr>
<tr>
<td>23</td>
<td>Market Leaders</td>
</tr>
<tr>
<td>24</td>
<td>• Market Segments Map</td>
</tr>
<tr>
<td>25</td>
<td>• Insurance Market</td>
</tr>
<tr>
<td>30</td>
<td>• Legal Market</td>
</tr>
<tr>
<td>35</td>
<td>• Management Consulting Market</td>
</tr>
<tr>
<td>41</td>
<td>• Technology Market</td>
</tr>
<tr>
<td>47</td>
<td>Appendix</td>
</tr>
<tr>
<td>48</td>
<td>• Research Methodology &amp; Definitions</td>
</tr>
<tr>
<td>51</td>
<td>• About ALM</td>
</tr>
</tbody>
</table>

## Related ALM Research & Tools

- Law.com: Cybersecurity
- Law.com: Legal Technology
- Law.com International: Cybersecurity
- The Legal Intelligencer, Special Supplement: Cybersecurity 2020
- Propertycasualty360.com: Cybersecurity
- Treasury & Risk: Technology

Our readers turn to ALM publications, events, and intelligence to keep at the forefront of their professions.

For more information, visit the ALM Intelligence website at [www.alm.com/intelligence](http://www.alm.com/intelligence)
Professional services providers work with businesses of all sizes and types, offering advice and operational support to help organizations improve performance, manage risk, and achieve their strategic growth objectives. In its research focused on the consulting sector, ALM Intelligence has observed a trend towards convergence across professional services markets, and we think the time is right to expand our focus. The ALM Pacesetters research series aims to explore the shifting dynamics that characterize the provision and sourcing of professional services in today’s rapidly changing economy and regulatory environment. We welcome your feedback and the opportunity to start a dialog.

What is an ALM Intelligence Pacesetter?
ALM Intelligence combines qualitative and quantitative research methods to identify the top professional services firms which are moving the ‘services’ needle to solve clients’ challenges and support their business needs. ALM Pacesetters are identified and evaluated using 5 core criteria.

How are ALM Intelligence Pacesetters identified?
ALM Intelligence Pacesetters are identified and selected by a panel of experts comprised of ALM editors, journalists, and research analysts, in collaboration with external professionals and academics who have experience working with professional services providers.

Who should read ALM Pacesetters research?
ALM Intelligence Pacesetters provides independent, objective research to providers and buyers of professional services coupled with practical insights that inform the decision-making process for strategic planning and procurement professionals.

Sell-side
- Practice Leaders
- Analyst Relations
- Sales, Marketing & Public Relations
- Investor Relations
- Ecosystem Partners

Buy-side
- C-Suite & Board
- Business Unit Leaders
- Procurement
- Supply Chain Partners
- Shareholders
ALM analyzed and profiled 18 Market Leaders across four market segments for ALM Intelligence Pacesetter Research: Cybersecurity Services 2020. Four providers were identified as ALM Pacesetters: AXA XL, Baker & Hostetler, EY Consulting, and Kroll (*).

Introduction: Report Scope

Note: Multidisciplinary service providers are segmented based on the core capabilities that characterize their business model's center of gravity.
Market Overview
I’m going to deviate from the traditional executive summary to talk about convergence. The convergence trend is a key driver behind ALM’s decision to shift its approach to covering business-to-business (B2B) professional services in its market research, and we think using this space to share our rationale will help you understand the purpose of Pacesetter research.

When I was a student of interactive telecommunications in the 1990s, I read about Nicholas Negroponte’s theory of convergence. Negroponte, who founded M.I.T.’s Media Lab in 1985, posited that the digitalization of computing, communications, and content creation would break down the barriers between these three disciplines to transform the media industry. His theory has not only proven right, it also convincingly extends to other industries.

Consider fintech, a field that combines traditional banking and transactional finance using digital business models that has profoundly impacted banking’s relationship with its customers, in a very positive way. How long would it be before convergence extended to the sphere of B2B professional services?

I will argue the convergence trend gathered momentum about ten years ago when management consulting providers began acquiring digital design agencies to enhance advisory services in marketing and process design. By 2017 – the year Accenture, Deloitte, and McKinsey spent a collective $1.2 billion to acquire digital agencies – what looked like a pattern of strategic acquisitions was coalescing into an entirely new way of doing business. The professional services ecosystem business model was born, and traditionally one-trick pony advisors were empowered to bring a more diverse toolkit to solving clients’ challenges on a larger scale at a faster pace.

Granted, this is an oversimplification of the ecosystem business model’s evolution, but it illustrates two important consequences of convergence. One is the large-scale transformation of industries, and the other is the smaller scale transformation of individual businesses, as well as their products and services. These mutually reinforcing consequences have resulted in new ways for B2B service providers to create value for clients and pursue growth opportunities in new markets; but there also are challenges, most notably from unexpected sources of competition.

ALM Pacesetter Research is the natural outcome of ALM’s strategy to expand its reach into markets adjacent to its core business in legal information, media, and data services. Over the past five years, ALM has acquired media and research businesses that have had a front row seat to the convergence trend in management consulting, insurance, financial advisory, and real estate. ALM Pacesetter Research dissolves the boundaries between these vertical specialties to bring a multidisciplinary view of how the B2B market is evolving and what that means to buyers of professional services.

Cybersecurity Services is one of the first reports to be published using this new model. The research explores the dynamics of convergence across insurance, law, management consulting, and technology, as well as the key drivers of demand in each market segment. There are profiles of 18 market leaders that detail value propositions, service offerings, and where each provider currently places on the convergence continuum. Within this group, 4 providers were identified as Pacesetters for the ways in which they are moving the needle to deliver professional services in a converging marketplace.

We realize this is a unique approach to analyzing professional services and expect our methodology to evolve in tandem with market developments and feedback from our readers. Please do not hesitate to share your observations with me or another contact you may have at ALM. We welcome the give-and-take that comes with an audience of intelligent professionals whose opinions are shaped on the front lines of business and will take it to heart as we evolve our value proposition for ALM Pacesetter Research.
The cybersecurity services market is dominated by an oligarchy of multiservice and technology giants operating at the core of a fragmented, diverse landscape where service providers compete in some circumstances and partner in others.

B2B Cybersecurity Services Market

Managed Services
Business Services
Vertical Market Services
Technology & Network Services

Demand Drivers
The COVID-19 pandemic is reshaping demand as organizations prioritize their shift to a digital business model in an increasingly virtual operating environment. Providers' abilities to respond are challenged by the scarcity of cybersecurity talent, ever-shortening lifespan of new technologies, and human behavior. Key demand drivers include:

- Accelerated adoption and commissioning of cloud technologies by large and middle market companies seeking rapid digital transformation
- Intensified threat exposure to corporate networks from remote workers using unsecured devices and video communication platforms
- Increasing incidence of advanced persistent threats (APTs) exploiting the pandemic
- Regulatory regimes, e.g., GDPR, advancing to enforcement and reporting stage

Sources of Competitive Advantage
Management commitment to innovation provides the most sustainable competitive advantage in the cybersecurity services market. Providers must be capable of rapidly adapting innovation strategies to shifting environment shaped by systemic risk and technology advances. Key sources of competitive advantage include:

- Digital transformation services that embed privacy- and security-by-design principles into the business and operating model
- Governance frameworks structured to link risk management and regulatory compliance in one model
- Advanced capabilities for managing, governing, and monetizing ecosystem relationships
- Endpoint security solutions that protect the full range of remote device applications (IoT, mobile, SaaS) and network environments (on-premise, cloud, critical infrastructure)
- Security solutions that leverage advanced analytics (e.g., artificial intelligence, deep learning), maturing cyber capabilities from focus on defense toward detection and protection

Acronyms
EPP – Endpoint protection platform
MSSP – Managed security service provider
Cybersecurity is an enterprise issue requiring the orchestration of multiple stakeholder interests and a disciplined procurement process to ensure professional services are scoped and aligned to the organization’s business context and risk appetite.

### Cybersecurity Services Stakeholder Heat Map

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Cybersecurity Service Providers</th>
<th>Stakeholder Roles and Interests</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO</td>
<td>Insurance, Legal, Management Consulting, Technology</td>
<td>The Chief Executive Officer collaborates with the Board in a fiduciary oversight role, ensuring the work of internal and external advisors in enterprise-wide cybersecurity programs creates desired business outcomes</td>
</tr>
<tr>
<td>CFO</td>
<td>Insurance, Legal, Management Consulting, Technology</td>
<td>Finance manages the funding of cybersecurity resources and programs; analyzes the impact of cyber events on the bottom line; monitors and reports on the ROI of security spending; and oversees the purchase of cyber insurance</td>
</tr>
<tr>
<td>COO</td>
<td>Insurance, Legal, Management Consulting, Technology</td>
<td>The Chief Operating Officer controls the first line of defense in a cyber event with responsibility for assessing, controlling, and mitigating cyber risks impacting day-to-day operations and business processes</td>
</tr>
<tr>
<td>CIO, CISO</td>
<td>Insurance, Legal, Management Consulting, Technology</td>
<td>Information technology/security officers have primary responsibility for monitoring and enforcing technology and data security practices, however, their roles are expanding to better integrate with the business, manage technology and data risks more strategically, and work toward a culture of cyber risk ownership across the enterprise</td>
</tr>
<tr>
<td>GC</td>
<td>Insurance, Legal, Management Consulting, Technology</td>
<td>General Counsels oversee cybersecurity compliance for regulatory and legal obligations; ensure the collection &amp; preservation of cyber incident evidence; contact relevant parties affected by cyber events; and guide cybersecurity governance structures</td>
</tr>
<tr>
<td>CHRO</td>
<td>Insurance, Legal, Management Consulting, Technology</td>
<td>HR provides workforce planning, learning and leadership development, and change management services to ensure the organization has the right talent and skills to meet cybersecurity policies and cultures; HR also consults on data protection policies as this function owns a significant portion of employee information</td>
</tr>
<tr>
<td>CPO</td>
<td>Insurance, Legal, Management Consulting, Technology</td>
<td>Procurement collaborates with IT to identify points of attack in supply chain processes, audits third party cyber security capabilities; and builds cybersecurity measures into procurement processes</td>
</tr>
<tr>
<td>CRO</td>
<td>Insurance, Legal, Management Consulting, Technology</td>
<td>The Chief Risk Officer cultivates and convenes cross-departmental relationships for the purpose of building strong and uniform cybersecurity practices that operate in near or real time across the enterprise</td>
</tr>
</tbody>
</table>

**Acronyms:**
- **CEO** - Chief Executive Officer
- **CFO** - Chief Financial Officer
- **COO** - Chief Operating Officer
- **CIO** - Chief Information Officer
- **CISO** - Chief Information Security Officer
- **GC** - General Counsel
- **CHRO** - Chief Human Resources Officer
- **CPO** - Chief Procurement Officer
- **CRO** - Chief Risk Officer
The Risk Matrix positions peer groups in terms of their capabilities to create client impact through a mix of services supporting a spectrum of risk strategies. See Appendix for detailed risk matrix definitions.

- Management consulting firms and technology providers offer the most comprehensive approaches to cybersecurity risk management. They go to market with multidisciplinary service offerings that enable organizations to embed cyber risk upfront in strategic planning, operating model design, systems architecture, and transformation initiatives.

- Management consulting firms, in some cases, provide advisory and managed services by an external third party or internal practice that is subject to regulatory oversight, such as tax or legal. The services are nonetheless a component of the provider’s value chain of cybersecurity services. However, buyers are cautioned to inquire about independence to avoid potential conflicts of interest or service limitations the provider observes to manage its own risk in a regulated environment.

- Providers across all segments except law offer predictive services that are either customized, e.g., cyber risk gap analyses, or contextual, such as use cases and claims scenarios that illustrate the provider’s approach to solving cybersecurity challenges by industry, company size, or other parameter.

- Law firms currently contain their services to the “reactive” end of the risk spectrum, although there are elements of proactive risk in contract and data privacy law. There is potential for law firms to provide upstream services, such as Security by Design in legal function transformation, or predictive services that leverage litigation data related to data privacy or intellectual property rights.
As first responders of the Fourth Industrial Revolution, cybersecurity services providers have a unique ability to deliver mission-critical services using a sprint approach. The rapid and sudden disruption to business caused by coronavirus has amplified this capability amidst a surge of new demands from clients struggling to maintain security and business continuity. Data breaches have grown in frequency and intensity; complex supply chains are revealed as inherently vulnerable; and the cyber risks caused by human error have increased exponentially as more and more people work from home. Providers, who had been evolving their capabilities at a rapid pace prior to the pandemic, quickly pivoted to deliver reactive cyber risk services in the initial phase of the crisis.

As the dust begins to settle, it is increasingly clear that providers have not lost sight of their longer-term strategies to help clients build resilient cyber functions and processes. They continue to invest in growing their capabilities, in addition to reshaping service delivery models constrained by social distancing mandates. They are adapting to clients’ shifting priorities by re-scoping projects and realigning cyber risk frameworks to the pandemic’s recovery cycle. Their top priorities remain, as always, to help clients navigate the external market forces that drive cyber risk and build an organizational capability for cyber resilience.

Rapid digital transformation
The COVID-19 pandemic has lit a fire under organizations of all sizes and type across geographies to accelerate their shift to a digital business model in order to move services and employees online. In the second quarter earnings season, technology providers reported a surge in new demand for the digital, cloud, and security-related services that underpin digital transformation, coupled with requests to fast-track ongoing transformation projects. Furthermore, clients are requesting shorter time horizons, asking providers to implement what were normally five-year projects in 18 months. These trends are echoed anecdotally by management consulting providers whose services lean towards digital and business process transformation and cybersecurity consulting.

Demand Drivers: Cybersecurity Services

Implications for Providers

- Encourage clients to revisit their cyber and data risk governance frameworks and business process management documentation and adjust for changes in operating and staffing models, managed services contract renewals, and overall outlook for the emerging “new normal” of the post-pandemic world
- Reexamine how your managed services offerings can support clients by filling talent gaps they may have recently incurred from pandemic cost-cutting action plans
- Map your cybersecurity ecosystem against that of your client:
  - Analyze complementary capabilities that have the potential to support clients’ needs when combined
  - Extend coverage in additional geographic markets
  - Identify areas of overlap that may require a stronger defense in competitive selling situations

(1) “IT, BPM companies see sharp rise in digital transformation deals,” Economic Times CIO.com, 10 August 2020
Rapid digital transformation (continued)

Cybersecurity providers found themselves immersed in assessing clients’ cyber-readiness and creating COVID-19-related checklists for CISOs under pressure to secure connections in the overnight shift to a remote work environment. Providers involved in re-scoping transformation projects are using the opportunity to involve CISOs from the earliest stages of the discovery process to ensure security is a foundational component of digital transformation. Working together, providers and CISOs are leveraging the moment to build alliances with senior leadership and focus on security as a competitive differentiator and enabler of innovation.

Convergence of data privacy and security

Organizations have distinguished between data privacy and data security for many years, managing each under separate corporate functions. To this day, compliance, with input from legal, governs the collection and use of personal data according to global laws and regulations (data privacy), while IT manages the technology and tools used to protect personal information from bad actors (data security).

These boundaries are blurring as a growing body of regulations require companies to comply with different definitions and requirements for data privacy, including some that include elements of data security. At the same time, definitions of data privacy are being questioned in the context of machine learning and artificial intelligence, where massive amounts of personal data are used to develop new products and services, often without individual consent.

Providers are responding with frameworks that map data governance frameworks to cybersecurity function operating models, clearly articulating the steps involved in defining roles and clarifying decision rights around access and ownership. In an interesting move, many of the leading law firms are structuring their service offerings around the data life cycle to illustrate the intersection of privacy and security.

Implications for Buyers

- Review contracts negotiated with professional services providers pre-COVID to validate terms following post-COVID cybersecurity actions
  - Clarify cyber-insurance policy terms and coverages specific to data breach incidents
  - Request details about dispute resolution mechanisms, such as arbitration and litigation
  - Engage appropriate stakeholders in contract review (GC, CISO, COO, etc.); revisit governance frameworks, if necessary
  - Communicate changes in policy guidelines following review to appropriate stakeholders (employees, customers, shareholders)

- Identify all cloud providers that touch your company’s network; confirm they are enrolled in your organization’s third-party vendor management program and are following prescribed guidance on how to protect the data they’re storing

- Take advantage of all training and awareness programs offered by the multiple cybersecurity providers that support your organization
Managed security services

Managed security and as-a-service offerings are an important component of all providers’ services and another fast-growing vertical of cybersecurity services overall. Most clients realize that outside expertise from providers who run Cybersecurity Intelligence Centers, Security Operations Centers (SOCs), laboratories, and innovation centers will stay ahead of the learning curve of even the most forward-thinking organizations. Preferred delivery models will vary depending on the size of the client organization and their needs, but whether it is on-premise, co-sourcing, or outsourcing with consulting and advisory support, most organizations will adopt managed services to maintain the most effective security protection.

Providers are focusing on advanced security services that incorporate next generation technologies such as AI, machine learning, advanced analytics, sensors, platforms, and other security development operations (SecDevOps) services. Managed security services can provide intelligence-led cyber defense capabilities, advanced threat detection (sharing threat data and finding the most likely threats for a specific organization), cyber-as-a-service (CaaS), red teaming, managed detection and response (MDR), compromise assessments, secure data lakes, and expertly-run, real-time security operations centers (SOCs).

For providers, managed services add value in two ways: stronger and stickier client relationships, and recurring revenue. The challenge is to manage and coordinate across their ecosystem of third-party partners to ensure delivery of quality services in a timely manner.

Cybersecurity skills shortage

The lack of certified cybersecurity professionals within organizations is driving demand for consulting, advisory, and technology services. Many providers roll some form of training into their service offerings, which may include skills training, cyber risk awareness, and change management sessions to shift mindsets and behaviors. They will also provide staff augmentation and virtual CISOs where necessary.

Providers themselves are feeling the talent shortage pain, but have found ways to compensate by actively recruiting and training students, veterans, and others with formal and on-the-job training. Many providers are forming partnerships with universities and other institutions in the hopes that they will have direct access to the next generation of cybersecurity talent.
The ALM Pacesetters
Business model: Cybersecurity Market Leaders overall are leveraging the ecosystem business model to provide predictive, proactive, and reactive cybersecurity services. EY Consulting’s Security By Design approach exemplifies this strategy with its top-down, bottom-up service offering that adapts to a broad range of client challenges and strengthens clients’ cyber resiliency with a program of managed services. AXA XL and Kroll show significant capabilities for managing ecosystem relationship by directly engaging in the coordination and access of these services to their clients.

Value proposition: Pacesetters stand out for value propositions that speak to an enterprise risk approach to cybersecurity. In some cases, these value proposition reward clients that have worked to advance their cybersecurity posture to a degree of maturity that strengthens an organization’s first line of defense. AXA XL, for example, offers selected services from ecosystem partners at no charge during the first policy year if the client qualifies based on a cyber posture assessment. Kroll also offers clients favorable rates and benefits for services offered by ecosystem partners to encourage a proactive approach to risk mitigation.

Service delivery: No matter which segment the Pacesetter belongs to, they go to market with integrated teams led by the professional that represents their core capability, e.g., a consultant, lawyer, or broker. This approach requires an investment in diverse talent with technical expertise in cyber analytics, systems architecture, and risk management. For Baker & Hostetter and AXA XL, adopting this strategy signifies a level of confidence in managing talent that is new for providers in the insurance and legal segments.

Client enablement: The greatest variation in Pacesetter scores was for this criterion. Helping clients build an organizational capability for cyber resiliency is a new challenge for providers in law and insurance. AXA XL and Baker & Hostetter are gaining ground by virtue of offering proactive risk services through ecosystem partners. They likely do not aspire to the strong capabilities that EY Consulting and Kroll have developed over the years, but there is room for them to explore ways in which they can incorporate the capabilities of their ecosystem partners in service delivery.

Brand eminence: It would be impossible to differentiate in the cybersecurity services market without a strong brand defined by thought leadership, intellectual property, and research partnerships. AXA XL’s reputation for innovation is bolstered by its work with U.K.-based Oxbotica on the cyber risks of autonomous vehicles. Baker & Hostetter is unique for how it leverages the firm’s incident response data and experience in an annual study anticipated by professional services providers and buyers alike for benchmarking performance. EY Consulting and Kroll strengthen their brands by incorporating emerging technologies, such as AI and machine learning, in smart solutions designed to anticipate cyber risks.

Cybersecurity Services Pacesetters 2020

<table>
<thead>
<tr>
<th>Market Segment</th>
<th>Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insurance</td>
<td>AXA XL</td>
</tr>
<tr>
<td>Legal</td>
<td>Baker &amp; Hostetter</td>
</tr>
<tr>
<td>Management Consulting</td>
<td>EY Consulting</td>
</tr>
<tr>
<td>Management Consulting</td>
<td>Kroll</td>
</tr>
</tbody>
</table>

ALM Pacesetter Methodology Notes

The ALM Pacesetter Research methodology evaluates Market Leaders against five core criteria.
1. Business model
2. Value proposition
3. Service delivery
4. Client enablement
5. Brand eminence

Providers whose aggregate score is 85 and above qualify as an ALM Pacesetter.

In this research, elements of three criteria are weighted due to their importance in achieving competitive differentiation in cybersecurity services: ecosystem and innovation (business model) and risk management (service delivery).
AXA provides cyber and technology liability insurance through its specialty risk division, AXA XL, going to market with a solutions-oriented approach that combines insurance coverage with a mix of tools, services, and resources to proactively manage cyber risks. AXA XL delivers on this approach with the help of a broad network of data breach response partners, including consulting and technology providers, law firms, and public relations agencies.

AXA XL asserts that its cyber policies use terminology and expanded coverage to provide clients with the broadest coverage possible, including for emerging risks. For example, “outsourced provider” is redefined to include any third party contracted to do business on behalf of the insured, a definition that significantly expands the range of business interruption triggers covered by the policy. Cyber insurance is offered globally and designed to protect from risks through agreements that cover network security, privacy, business interruption, media liability, and errors and omissions.

AXA XL has achieved a reputation for innovation in the insurance industry. CyberRiskConnect, the branded solution for clients in North America, was launched in 2018 and is continually evolving to help clients proactively manage risk and respond quickly to events. The solution offers complimentary pre-breach services (e.g., incident and GDPR readiness assessments) during the first policy year from pre-qualified vendors, including FireEye and Kroll. The service is supported by a dedicated claims team of experienced attorneys that operates on a 24/7 basis to help clients navigate, respond, and recover from a cybersecurity breach. Clients also have access to resources and response services through CyberRiskConnect.com. Additional innovations include:

- A cyber policy designed for small- and medium-sized U.S. businesses available through a partnership with Slice Laboratories, an on-demand insurance cloud platform. The policy is discounted to qualified customers who represent a lower insurance risk based on a security posture assessment
- Accenture’s Cyber Incident Response Services for international clients; in the U.S., the service is one of 14 options
- A policy for autonomous vehicles that covers specific types of cyber risk, an outcome of its research partnership with U.K.-based Oxbotica to develop risk management solutions for autonomous technology products

### Cybersecurity Services

#### Cyber Insurance Coverage
- Business interruption and extra expense
- Cyber extortion and ransomware
- Data recovery
- Privacy and security liability
- Privacy regulatory defense costs and coverage for any fines and penalties assessed
- Enhancements (PCI, social engineering, system failure, and dependent business interruption)

#### Cyber Risk Consulting
- Cyber security conformity to check compliance levels
- Security by Design
- Cyber security managed systems to define, update or redesign information security policies
- Multi-risk site evaluations to assess physical infrastructure and sites of high cyber impact, such as data centers and server facilities

#### Third-Party Services
- Call center operations for breach incidents
- Credit and ID monitoring
- Crisis response and communications
- Digital forensics and eDiscovery
- Expert testimony
- Incident response and recovery services (fee and retainer)
- PCI forensic investigations
- Ransomware containment & bitcoin negotiation
- Regulatory response & breach litigation counseling

<table>
<thead>
<tr>
<th>Pacesetter Criteria</th>
<th>Pacesetters Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Model</td>
<td>Value</td>
</tr>
<tr>
<td>Impact Scale:</td>
<td>None</td>
</tr>
</tbody>
</table>
## How AXA XL is moving the needle

<table>
<thead>
<tr>
<th>Pacesetter Criteria</th>
<th>Qualitative Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Model</td>
<td>AXA XL is mastering the ecosystem business model to deliver a mix of proactive and reactive risk services to clients of its CyberRiskConnect product, including advanced endpoint protection and security services, privacy awareness training, compliance assistance, incident response planning, and third-party contract review</td>
</tr>
<tr>
<td>Value Proposition</td>
<td>AXA XL’s core cyber insurance products are underwritten to provide clients with the broadest coverage possible, including for emerging risks. Also, selected ecosystem services are available at no charge for a limited time (about one year) to clients that qualify based on an assessment of their organization’s cyber posture</td>
</tr>
<tr>
<td>Service Delivery</td>
<td>AXA XL works closely with its ecosystem partners to provide their underwriters and clients with access to threat intelligence, risk mitigation, and post-breach services to cultivate more informed decision-making about cyber risks and improve post-breach outcomes</td>
</tr>
<tr>
<td>Client Enablement</td>
<td>AXA XL’s ability to help clients build a capability for cyber resilience relies on the strength of their ecosystem partnerships, however, the firm is developing insights and frameworks that incorporate risk management into its claims scenarios to better communicate how their services build cyber awareness and resilience</td>
</tr>
<tr>
<td>Brand Eminence</td>
<td>AXA XL has achieved a reputation for innovation in its approach to underwriting cyber insurance and leveraging insurance technology start-ups to distribute its policies downstream (e.g., the middle market) and to specialty markets (e.g., autonomous vehicles)</td>
</tr>
</tbody>
</table>
Baker & Hostetler goes to market with a business-led approach to information security that positions data as a critical asset of today's digital enterprise. The firm entered the market for cyber legal services over a decade ago when it launched a Privacy and Data Protection team. Through lateral hiring and organic growth strategies, Baker & Hostetler expanded beyond compliance to offer legal advisory and litigation services in data privacy specific to industries (advertising, healthcare, media), technology, and transactions. In January, the firm merged these practices into the Digital Assets and Data Management Group (DADM), a global multidisciplinary practice of 100+ attorneys and technology professionals who provide services aligned to the life cycle of data, defined by Baker & Hostetler as create-collect-store-use-share-reuse-archive-destroy.

Services are delivered by integrated teams to ensure clients benefit from the practice's interdisciplinary capabilities in the business and legal matters of data privacy. Structurally, resources are organized in seven domains that blend expertise in digital risk advisory, data privacy and compliance, digital asset management, litigation, and emerging technologies. Services are targeted to c-level and board executives, GCs, strategy and corporate development professionals, CIOs, and CISOs in retail, healthcare, hospitality, education, and financial services.

Baker & Hostetler stands out for its incident response research and services. Its lawyers have been helping clients manage breaches for more than 15 years with services that include the provision of pre-incident preparedness and compliance counseling through a partnership with FireEye Mandiant Solutions. The firm's annual Data Security Incident Response report has become a much-anticipated resource for the comparative statistics and insights it offers based on an analysis of the 1,000+ incidents the firm manages each year.

IncuBaker is Baker & Hostetler’s research and development team that collaborates with technology providers to design and develop tools for the firm and its clients. The team also provides workshops on risk mitigation and advanced analytics and manages third-party subscriptions to specific analytic applications and machine learning tools such as ROSS, the legal research engine that leverages IBM Watson's cognitive technology. IncuBaker conducts research, including the aforementioned incident response study, and ongoing analyses of 400 legal technology vendors to identify the best solutions for clients' customized use cases.
**How Baker & Hostetler is moving the needle**

<table>
<thead>
<tr>
<th>Pacesetter Criteria</th>
<th>Qualitative Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Model</strong></td>
<td>Baker &amp; Hostetler models a business-led approach to data privacy and security by combining legal and technology talent to address the spectrum of risks across an organization’s digital assets. The firm’s research and development team, IncuBaker, collaborates with technology providers to design and develop tools for the firm and its clients.</td>
</tr>
<tr>
<td><strong>Value Proposition</strong></td>
<td>The firm’s value proposition is grounded in an evidence-based approach incident response that is supported by insights from FireEye that articulate how GCs can collaborate with CISOs to demystify complex incident response and impact mitigation processes.</td>
</tr>
<tr>
<td><strong>Service Delivery</strong></td>
<td>Services are delivered by integrated teams to ensure clients benefit from Baker &amp; Hostetler’s interdisciplinary capabilities in the business and legal matters of data privacy.</td>
</tr>
<tr>
<td><strong>Client Enablement</strong></td>
<td>This is Baker &amp; Hostetler’s lowest score, which is more a factor of law firms’ not providing a breadth of services to help clients strengthen their cyber resilience, for example, change management or leadership development.</td>
</tr>
<tr>
<td><strong>Brand Eminence</strong></td>
<td>Baker &amp; Hostetler leads the law firm peer group in how it leverages its experience in research-based thought leadership, that is, the firm’s annual Data Security Incident Response Report of insights based on an analysis of the 1,000+ incidents the firm manages each year. The report is produced by IncuBaker and used in risk mitigation workshops that IncuBaker provides to clients.</td>
</tr>
</tbody>
</table>

*Note: BakerHostetler is the marketing brand of Baker & Hostetler LLP*
EY Consulting goes to market with Security by Design, a systems engineering approach to managing cyber risk by prioritizing security features in the design of technology and data architectures. EY accomplishes this mission by developing and implementing solutions that assure clients’ businesses are secure, resilient, and capable of adapting at scale to new ways of creating value. Security by Design is a pillar of EY’s Trust by Design platform, which embeds risk management into all aspects of the client’s business and operating models, from technology and processes to people and ecosystems. These platforms are critical enablers of EY’s overall approach to transformation consulting, called Transformation Realized.

Services are delivered by EY’s Global Cybersecurity practice through a blend of advisory, consulting, implementation, and managed services. Professionals are supported by a global network of cybersecurity innovation and operations centers; Wavespace centers that focus on technology and innovation; an IoT/OT client experience center in Warsaw; and a multitude of ecosystem partnerships through which EY operates as a systems integrator (e.g., as a Gold Partner for IBM’s Resilient Platform and Splunk’s Data-to-Everything Platform) and solutions partners (e.g., cyber defense solutions supported by Microsoft security technologies). The firm has made several strategic acquisitions over 2019-20, including specialist players including Sila Solutions Group (identity and access management specialist), Elevated Prompt (managed detection and response services firm), and Aleron (cyber strategy, architecture design and implementation).

EY can introduce cybersecurity services through multiple touchpoints in an organization. The firm supports the CISO organization in its work to optimize the benefits from cybersecurity and resilience investments and infrastructures. Consultants also support the C-suite and board in their fiduciary oversight roles to ensure enterprise cybersecurity programs achieve desired outcomes. Entry points include digital transformation projects, compliance/continuous assurance engagements, and SOC transformations.

EY is well-known for its managed and as-a-service offerings, including Cybersecurity-as-a-Service (CaaS). The firm launched TPMR-as-a-Service this year to help clients build third party risk management (TPRM) functions that assess vendors’ risk profiles and alerts to hidden risks, such as vendors’ use of mobile apps to support remote working.

---

### Cybersecurity Services

EY Consulting blends cybersecurity advisory, technology strategy and implementation and managed services across five service lines.

**Strategy, Risk, Compliance & Resilience**
- Strategy, governance, risk quantification, benchmarking & maturity assessments, CxO dashboarding, 3rd party risk management

**Data Protection & Privacy**
- Data privacy, discovery, governance, loss prevention, encryption & data rights management
- Legal services for data privacy & protection and data breach investigations

**Identity & Access Management**
- Identity governance & administration, access & authentication, and privileged access management

**Architecture, Engineering & Emerging Technology**
- Secure cloud, blockchain, cognitive analytics, ICS/OT, IoT and SAP 4.0

**Next Generation Security Operations & Response**
- Application security; vulnerability management; IT/OT SOC deployment, operations & optimization; threat hunting, monitoring & response; and IR & forensics

---

### Pacesetter Criteria

<table>
<thead>
<tr>
<th>Business Model</th>
<th>Value Proposition</th>
<th>Service Delivery</th>
<th>Client Enablement</th>
<th>Brand Eminence</th>
<th>Pacesetters Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>99</td>
<td>88</td>
<td>90</td>
<td>82</td>
<td>77</td>
<td>93.4</td>
</tr>
</tbody>
</table>

Impact Scale: None, Low, Moderate, Significant, High, Very High
**How EY Consulting is moving the needle**

<table>
<thead>
<tr>
<th>Pacesetter Criteria</th>
<th>Qualitative Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Model</td>
<td>EY Consulting organizes the breadth and depth of its capabilities in management, operations, and technology consulting; legal, finance, and tax advisory; and systems architecture engineering in Security By Design, a service offering designed to build resilience into clients’ enterprise cybersecurity processes and functions</td>
</tr>
<tr>
<td>Value Proposition</td>
<td>EY Consulting’s value proposition is in a systems engineering approach to transformation consulting that contextualizes cybersecurity as a core driver of value creation. This sensibility informs the delivery of standalone cybersecurity projects, as well as enterprise-wide transformation initiatives</td>
</tr>
<tr>
<td>Service Delivery</td>
<td>EY Consulting works on cybersecurity projects with multiple stakeholders across an organization’s front, middle, and back offices, as well as the C-suite and board directors, using a service delivery model that adapts to the level of strategic and tactical support required by the stakeholder</td>
</tr>
<tr>
<td>Client Enablement</td>
<td>EY Consulting works with clients from project initiation to implementation, using multiple strategies and tools to help clients build a sustainable organization capability for effective cybersecurity management. The practice leverages adjacent consulting capabilities in change management, leadership development, and strategic communications to boost user adoption of cybersecurity tools and reengineered processes</td>
</tr>
<tr>
<td>Brand Eminence</td>
<td>One of EY Consulting’s strongest capabilities is its ability to innovate solutions using emerging technologies (AI, machine learning, etc.) that support the delivery of consulting services and are built into managed services platforms, for example, Cybersecurity-as-a-Service</td>
</tr>
</tbody>
</table>
Kroll goes to market with a mission-oriented approach to protecting clients’ data, people, operations, and reputation. The firm’s Cyber Risk practice is much like an elite special operations force that deploys contained teams of experts with specialist skills in cybersecurity, intelligence, investigations, and risk to manage the various implementation components of client engagements. With experts around the world, Kroll delivers end-to-end cyber risk management services including breach notification and identity theft, notification call center operations, and identity monitoring and restoration solutions.

Kroll’s framework for building what it calls a Defensible Security Strategy is structured around five pillars: governance, policies and procedures, infrastructure and standards, people and training, and relationships. It’s a straightforward, common sense approach to designing a strategy that is noteworthy for the fifth pillar stressing the importance of cultivating a support network of external experts and service providers. This advice is not only practical, but also reflects Kroll’s evolution from “response shop” to trusted adviser with its own deep relationships across the cybersecurity and intelligence ecosystems. Among these are extensive relationships with 50+ cyber insurance carriers, a number of law firm cyber risk practices, and law enforcement agencies.

While Kroll is technology agnostic, the firm partners with a number of specialists to develop solutions for managed services offerings. Kroll CyberDetectER® Endpoint, for example, is a managed detection and response (MDR) platform that combines the advanced endpoint hunting and response capabilities of Red Canary with Kroll’s global capabilities for investigating, managing, and mitigating cyber incidents and network intrusions. The firm has additional partnerships with Carbon Black, Coveware, Dauntless, and Cloud Range.

Kroll delivers services using a flexible engagement model that rapidly scales to the client’s challenge and provides non-surge base pricing and flexible retainer arrangements.

### Pacemaker Criteria

<table>
<thead>
<tr>
<th>Business Model</th>
<th>Value Proposition</th>
<th>Service Delivery</th>
<th>Client Enablement</th>
<th>Brand Eminence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Pacemaker Impact Score

- [ ] None
- [ ] Low
- [ ] Moderate
- [ ] Significant
- [ ] High
- [ ] Very High

### Cybersecurity Services

#### Governance and Risk Advisory
- Virtual CISO (vCISO)
- Security Culture-as-a-Service
- Third-party cyber risk
- Board advisory
- Privacy/DPO consultancy

#### Incident Response & Litigation Support
- 24x7 incident response and hotlines
- Digital forensics
- Global eDiscovery services
- Cyber litigation support
- PCI forensic investigator
- Data recovery and forensic analysis
- Malware and advanced persistent threat detection
- Incident response threat simulations

#### Systems Assessments and Testing
- Cyber risk/privacy assessments
- Regulatory and standards-based assessments
- Cloud security assessments and services
- Web application security assessments
- Penetration testing
- Vulnerability scanning
- Ransomware preparedness

#### Notification, Call Centers and Monitoring
- Data breach notification
- Call center services
- Credit and ID monitoring
- ID restoration and consultation

#### Managed Security Services
- 24/7 managed detection and response (MDR)
- CISO Advisory
- Vulnerability and penetration testing
- Cyber due diligence for corporate transactions
- Security culture training and phishing exercises
- Dark web monitoring
- Social media threat monitoring
- Cyber threat intelligence
**How Kroll is moving the needle**

<table>
<thead>
<tr>
<th>Pacesetter Criteria</th>
<th>Qualitative Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Model</strong></td>
<td>Kroll is unique among the Pacesetter cohort for a business model focused on maintaining an elite team of security professionals. They are nonetheless fully engaged in helping clients coordinate the services within their broad ecosystem of law firms, insurance providers, and managed security services providers (MSSPs)</td>
</tr>
<tr>
<td><strong>Value Proposition</strong></td>
<td>Kroll’s value proposition is differentiated by a global, end-to-end cyber risk offering that supports the entire incident lifecycle - incident response, e-discovery, notification, monitoring, and proactive services. The company’s deep relationships with corporate executives and ecosystem providers worldwide simplifies the engagement lifecycle and, in some cases, offers clients favorable rates and benefits</td>
</tr>
<tr>
<td><strong>Service Delivery</strong></td>
<td>Kroll’s professionals are the Navy Seals of incident response. They are global, mobile, and organized in their tactical response to cyber incidents. For example, they are familiar with the legal holds of multiple jurisdictions and will ensure that forensic evidence for possible litigation is collected during and after an emergency response</td>
</tr>
<tr>
<td><strong>Client Enablement</strong></td>
<td>Kroll’s strength is in its response capabilities; however, the firm is investing in proactive services and solutions that will support clients in their work to build organizational cyber resilience</td>
</tr>
<tr>
<td><strong>Brand Eminence</strong></td>
<td>Kroll is ahead of the curve in use of artificial intelligence to proactively detect and respond to threats across endpoint surfaces and the dark web. The firm also regularly offers educational webinars and manages a resource library of timely, relevant insights and checklist assessment tools on its website</td>
</tr>
</tbody>
</table>
Segment Leaders
Technology providers and a subset of management consulting providers currently have the most established presence across the cyber risk services value chain; insurance is gaining ground through their relationships with prequalified panel providers, while law firms remain focused on reactive cyber risk services.

Acronyms:
NIST – National Institute of Standards & Technology

Key:
- Services not provided
- Services provided by ecosystem partners

Cybersecurity Services - Market Segments

NIST Cybersecurity Framework

Key:
- Services not provided
- Services provided by ecosystem partners

Acronyms:
NIST - National Institute of Standards & Technology
Demand Drivers
The cyber insurance market is one of the fastest growing segments of the insurance industry. The global market was valued at $4.80 billion in 2018, with 42% of that share attributed to the U.S., where the market grew from $2.03 billion in 2018 to $2.25 billion in 2019, an 11% growth rate.(1) Expectations are for further growth in 2020 driven by a combination of idiosyncratic and systemic risk factors.

• The digital transformation of business, accelerated by the social distancing mandates of the COVID-19 pandemic, is driving the most demand for cyber insurance solutions. Within this context, organizations do not have as much time as they need to build organizational cyber resilience from the ground up. Cyber insurance providers offer a strategy combining risk transfer and risk mitigation that can be implemented quickly. Companies that have suffered from cyberattacks can justifiably finance short-term recovery efforts through cyber insurance claims, and companies that have not suffered an attack can build a first line of defense with insurance providers’ pre-breach services.

• The impact of cyber regulation on corporations and consumers. In the U.S., cyber regulations require companies to report cyber incidents to customers and regulatory authorities. In Europe, data privacy regulations impose additional requirements on companies, e.g., data security. In both regions, aspects of these regulations may apply to companies doing business in their respective jurisdictions. Cyber insurance supports a company’s efforts to recover from a data breach by providing access to expert resources and financial support through investigation, notification, recovery and post-recovery activities related to a data breach event.

• Small and middle market companies face unique challenges when it comes to cybersecurity. They may not have the budget to deploy the tools an insurer requires to qualify for coverage and they also may not have the personnel to manage a cybersecurity function. This market has emerged as an attractive target for global insurers serving downstream, less saturated markets with specialized products; insurance technology start-ups offering cloud-based, on-demand, pay-per-use insurance platforms; and agencies specializing in the excess insurance market.

(1) AM Best, Allied Market Research; market size is based on direct premiums written (DPW)
Robust approaches to cyber risk reflected in sophisticated pricing models, advanced risk modeling tools for calculating premiums, and cybersecurity posture assessments necessary to qualify for service-related coverage

Massive war chests to invest in cyber insurance innovations

Global business models that guarantee knowledge of cyber regulations in regional jurisdictions

Understanding of cybersecurity dynamics and how they impact customer experience, pricing, and business growth objectives

Volume of actuarial and claims data to leverage for innovative underwriting of cyber insurance

Broad-based client portfolios to mine for insights into buy-side experience and perceptions of cyber risks that can be used to develop claims scenarios for product development and sales

Broad-based knowledge of insurance markets that can inform understanding of cyber risk

Lack of standards and commonalities around affirmative underwriting strategies creates confusion among brokers and their ability to effectively sell, e.g., policy overlaps or where to cover cyber-related bodily injury

Decentralized delivery of cyber-related services, e.g., incident response, weakens ambition to shift client relationships from passive to active engagement

Lack of information security (infosec) knowledge empowers data breach coaches in emergency decision-making process

New entrants from the insurance technology start-up sector, such as cloud-based, on-demand, pay-per-use insurance platform provider Slice Laboratories, and Coalition, a provider of cybersecurity insurance, tools, and services for small to mid-sized businesses

Reputational risk caused by ecosystem partners that do not deliver insured services, for example, post-breach communications or forensics
Beazley was one of the first insurance providers to act on the industry’s earliest instincts about the connection between an organization’s cyber resilience and the cost of covering cyber losses. Since it first started offering standalone cyber insurance in 2006, Beazley has evolved what it calls a 360° approach that combines insurance coverage with detailed guidance on cyber risk prevention and mitigation and incident response services. The Cyber & Executive Risk line of business delivers these services with the support of a global network of law firms, computer forensics specialists, breach notification call centers, and providers of breach resolution and mitigation services. Beazley is continually expanding the international reach of its cyber service offerings. In the first half of 2020 alone, Beazley invested in underwriting and breach response talent for Canada, Colombia, Spain, and the U.S. Midwest region.

Beazley’s flagship solution is Beazley Breach Response (BBR), a suite of pre-breach and post-breach services managed by a dedicated in-house team for policy holders in North America. Launched in 2010, BBR brings together expert forensic, legal, notification, and credit monitoring services to satisfy legal requirements and strengthen cyber resilience. In addition to breach response services, BBR coordinates client education services; cyber claims management; cyber defense consulting from wholly owned subsidiary Lodestone Security; and several web portals with interactive resources for clients and brokers serving small to medium-sized companies. BBR pricing is tied to the clients’ level of cyber insurance coverage with some services available at no charge when the client’s policy meets a minimum threshold.

Beazley prides itself on an ability to design cyber and executive risk policies that are both innovative and competitive. In 2019, the company introduced 10 new products, including a parametric-style reputational risk product for global organizations and an affirmative cyber policy covering both operations and information technology exposures for the maritime industry. BBR’s policy design leverages multiple towers of coverage to provide clients with extra limits that ensure breach response costs are covered. Beazley claims this approach provides more coverage per premium dollar than competitive products.

### Cybersecurity Services

#### Cyber Insurance Coverage
- Cyber and tech insurance
  - Business interruption
  - Cyber due diligence in M&A
  - Cyber extortion
  - Data recovery
  - eCrime
  - Information security and privacy
- MediaTech, (coverage combining errors and omissions, media liability, and cyber risk)

#### Cyber Risk Consulting
- Compliance readiness assessments
- Incident response operations design and implementation
- Information security strategy and road mapping
- Posture assessments (including external network vulnerability, insider threat, application, policy/procedure/standards, network architecture)
- Risk assessments
- Security awareness training and education
- Security program development
- Social engineering awareness evaluation

#### Beazley Cybersecurity Services
- Incident response (pre- and post-breach)

#### Third Party Cybersecurity Services
- Computer forensics and investigations (including breaches involving payment card information)
- Credit and identity monitoring
- Notification and call center services (external to BBR service)
- Privacy law

---

**Beazley**

**Primary Practice**

**Cyber & Executive Risk**

Beazley was one of the first insurance providers to act on the industry’s earliest instincts about the connection between an organization’s cyber resilience and the cost of covering cyber losses. Since it first started offering standalone cyber insurance in 2006, Beazley has evolved what it calls a 360° approach that combines insurance coverage with detailed guidance on cyber risk prevention and mitigation and incident response services. The Cyber & Executive Risk line of business delivers these services with the support of a global network of law firms, computer forensics specialists, breach notification call centers, and providers of breach resolution and mitigation services. Beazley is continually expanding the international reach of its cyber service offerings. In the first half of 2020 alone, Beazley invested in underwriting and breach response talent for Canada, Colombia, Spain, and the U.S. Midwest region.

Beazley’s flagship solution is Beazley Breach Response (BBR), a suite of pre-breach and post-breach services managed by a dedicated in-house team for policy holders in North America. Launched in 2010, BBR brings together expert forensic, legal, notification, and credit monitoring services to satisfy legal requirements and strengthen cyber resilience. In addition to breach response services, BBR coordinates client education services; cyber claims management; cyber defense consulting from wholly owned subsidiary Lodestone Security; and several web portals with interactive resources for clients and brokers serving small to medium-sized companies. BBR pricing is tied to the clients’ level of cyber insurance coverage with some services available at no charge when the client’s policy meets a minimum threshold.

Beazley prides itself on an ability to design cyber and executive risk policies that are both innovative and competitive. In 2019, the company introduced 10 new products, including a parametric-style reputational risk product for global organizations and an affirmative cyber policy covering both operations and information technology exposures for the maritime industry. BBR’s policy design leverages multiple towers of coverage to provide clients with extra limits that ensure breach response costs are covered. Beazley claims this approach provides more coverage per premium dollar than competitive products.

### Pacesetter Criteria

<table>
<thead>
<tr>
<th>Business Model</th>
<th>Value Proposition</th>
<th>Service Delivery</th>
<th>Client Enablement</th>
<th>Brand Eminence</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Low</td>
<td>Moderate</td>
<td>Significant</td>
<td>High</td>
</tr>
</tbody>
</table>

Impact Scale: None Low Moderate Significant High Very High

**Pacesetters Impact Score**

---

**Cybersecurity Services**

#### Cyber Insurance Coverage
- Cyber and tech insurance
  - Business interruption
  - Cyber due diligence in M&A
  - Cyber extortion
  - Data recovery
  - eCrime
  - Information security and privacy
- MediaTech, (coverage combining errors and omissions, media liability, and cyber risk)

#### Cyber Risk Consulting
- Compliance readiness assessments
- Incident response operations design and implementation
- Information security strategy and road mapping
- Posture assessments (including external network vulnerability, insider threat, application, policy/procedure/standards, network architecture)
- Risk assessments
- Security awareness training and education
- Security program development
- Social engineering awareness evaluation

#### Beazley Cybersecurity Services
- Incident response (pre- and post-breach)

#### Third Party Cybersecurity Services
- Computer forensics and investigations (including breaches involving payment card information)
- Credit and identity monitoring
- Notification and call center services (external to BBR service)
- Privacy law
Chubb goes to market with a data-driven, risk-oriented approach to insuring cyber risk. The company has been handling cyber incidents, underwriting cyber exposures, and processing cyber claims for more than 20 years. It’s a unique experience that Chubb has captured in an arsenal of cyber loss data that is regularly mined for insights into the strategic and financial impact of cyber-attacks and successful mitigation strategies. Over time, this has translated into a powerful case for defending against cyber risk with an enterprise solution. Chubb activates this value proposition in an approach to underwriting cyber insurance that grounds risk transfer with loss mitigation and post-incident services.

The Cyber Enterprise Risk Management solution (Cyber ERM) embodies Chubb’s underwriting strategy, providing a model the company adapts across a product range tailored to the needs of companies of all sizes and type across industries and geographies. Cyber ERM offers first-party and third-party liability coverage and additional coverage (endorsements) for losses due to cyber fraud. The Cyber Incident Response Team helps clients select and implement loss mitigation and incident response services available through a global network of pre-qualified, third-party service providers. This network also provides clients with access to legal advice, computer forensics, breach notification and call center support, public relations and crisis communications, fraud consultation, and more.

According to Chubb’s Chief Digital Officer Sean Ringsted, Chubb spends about $1 billion on technology every year with much of that investment supporting digital innovation and improving the customer experience. (1) The Cyber Risk practice leverages this investment to help clients proactively defend against cyber-attacks, developing solutions such as a secure password management system and tools such as Cyber Alert®, a mobile app that provides 24/7 incident reporting and response service resources.

Chubb Cyber IndexSM is regularly enhanced, as well, and has evolved beyond its original purpose of analyzing Chubb’s proprietary claims data to generate reports on historical, current, and predictive cyber threat trends. Recent upgrades include an online calculator that estimates the cost of incident response support services, insights on cyber insurance limits and deductibles by industry and geography, international data, and a research library. These enhancements illustrate the Cyber Risk practice’s commitment to using digital channels for helping clients take better control of their cyber risks.

### Cybersecurity Services

- **Cyber Insurance Coverage**
  - Business interruption
  - Crisis communications and reputation mitigation
  - Data loss and restoration
  - Errors and omissions
  - Funds transfer fraud
  - Incident response and investigations
  - Liabilities from failure to maintain data confidentiality
  - Liabilities from unauthorized use of network
  - Network or data extortion
  - Online media liability
  - Payment card loss
  - Regulatory defense and investigations
  - Social engineering fraud
  - Telephone toll fraud
  - Third party fraud

- **Third Party Cybersecurity Services**
  - 24/7 Incident response
  - Breach notification call center operations
  - Claims management
  - Compliance for HIPAA, PCI, and other standards
  - Computer forensics and investigations
  - Credit card monitoring
  - Crisis communications
  - Endpoint protection
  - Enterprise security operations
  - Identity restoration
  - Information encryption
  - Insider threat and ransomware monitoring
  - Loss mitigation
  - Personal cyber risk assessment

### Pacesetter Criteria

<table>
<thead>
<tr>
<th>Business Model</th>
<th>Value Proposition</th>
<th>Service Delivery</th>
<th>Client Enablement</th>
<th>Brand Eminence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Moderate</td>
<td>Low</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

Impact Scale:  
- None
- Low
- Moderate
- Significant
- High
- Very High

1 Digital evolution must happen across the entire insurance ecosystem (29 June 2020)
Travelers is the longest tenured insurance carrier in the cybersecurity market by way of its Global Technology practice’s 35-year history insuring technology start-ups, scale-ups, unicorns, and Fortune 500 companies worldwide. Informed by this experience, the Cyber Insurance practice offers clients a simple but straightforward proposition to protect their business with cyber liability insurance and breach support services.

Travelers offers four cyber insurance products targeted to specific markets. CyberRisk is the most flexible product, designed to cover industries and companies from small local businesses to global multinationals and nonprofits. It’s available as a standalone policy or as part of a more comprehensive business insurance package. The remaining three are CyberFirst for Technology Companies, CyberFirst for Public Entities, and CyberFirst for Small Businesses. All provide essential coverage related to cyber threats and include options to add coverage for specific cyber breach expenses.

Travelers’ commitment to cyber risk mitigation is strengthened by pre-breach services available through two technology alliances. Symantec services include cyber resilience readiness assessment and consulting, helpline support, and discounts on selected services, including Symantec Managed Security Services. The recently announced alliance with SentinelOne adds endpoint security solutions for remote environments, an urgent priority for organizations accelerating their transition to a virtual office model in the pandemic era.

Travelers diverges from its peers, however, regarding third party legal, forensic, and other services by not tying coverage to a pre-qualified vendor panel. The company believes this practice can slow the incident response process by adding a layer of approvals and decision-making on the insurance side. If there is no conflict of interest and the vendor is qualified, Travelers prefers clients use their providers of choice under the guidance of a breach support team that includes HIPAA and data breach coaches and Symantec’s cybersecurity helpline.

<table>
<thead>
<tr>
<th>Cybersecurity Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Insurance Coverage</td>
</tr>
<tr>
<td>- Business interruption</td>
</tr>
<tr>
<td>- Claims management</td>
</tr>
<tr>
<td>- Communications and media liability</td>
</tr>
<tr>
<td>- Computer fraud</td>
</tr>
<tr>
<td>- Computer program and electronic data restoration expenses</td>
</tr>
<tr>
<td>- Computer system improvements following a security breach (betterment)</td>
</tr>
<tr>
<td>- Crisis management event expenses</td>
</tr>
<tr>
<td>- Data breach coaches</td>
</tr>
<tr>
<td>- Data restoration</td>
</tr>
<tr>
<td>- E-commerce extortion</td>
</tr>
<tr>
<td>- Funds transfer fraud</td>
</tr>
<tr>
<td>- HIPAA coaches</td>
</tr>
<tr>
<td>- Network and information security liability</td>
</tr>
<tr>
<td>- Public relations</td>
</tr>
<tr>
<td>- Regulatory defense expenses</td>
</tr>
<tr>
<td>- Security breach remediation and notification expenses</td>
</tr>
<tr>
<td>- System failure</td>
</tr>
<tr>
<td>Third Party Cybersecurity Services</td>
</tr>
<tr>
<td>- SentinelOne endpoint detection and response</td>
</tr>
<tr>
<td>- Symantec Pre-Breach Cybersecurity Services</td>
</tr>
<tr>
<td>- Cyber resilience readiness assessment</td>
</tr>
<tr>
<td>- Cyber security awareness training videos</td>
</tr>
<tr>
<td>- Symantec security coach helpline</td>
</tr>
<tr>
<td>- Norton for small business software</td>
</tr>
<tr>
<td>- DeepSight™ intelligence</td>
</tr>
<tr>
<td>- Incident response plan gap analysis</td>
</tr>
<tr>
<td>- Tabletop assessments</td>
</tr>
</tbody>
</table>

Managed Services
- Symantec Managed Security Services
Demand for law firms’ data privacy and security services is driven more by the persistent threat of cybercrime’s impact on business operations than it is by economic cycles. This has been made painfully clear in today’s operating environment, where firms are concerned about cybercriminals targeting isolated employees working from home. This concern is driving client conversations with legal advisors despite the economic slowdown caused by COVID-19. In their annual data breach study, IBM and Ponemon Institute estimate that the remote workplace business model will increase the average annual cost of a data breach in 2020 to $4 million, up from $3.92 million in 2019. Law firms report that the threat has strengthened demand for legal advisers who can help companies both respond to a data breach and mitigate risk.

- **Data privacy and security** is the cornerstone of law firms’ cybersecurity service offerings. End-to-end services range from privacy assessments and policy reviews to regulatory investigations and class action litigation. Many provide incident response services, either directly or indirectly through insurance panels as pre-qualified providers. In much the same way that consultants help clients develop a business case for organizational cybersecurity, law firms help clients develop a “reasonable security” précis for regulators and litigators about how they approach and implement data protections. A handful of law firms have what could be called a first-mover advantage in this practice area, attributable to portfolios of long-standing, high technology clients who were early entrants to the internet economy. These firms also lead the market for legal advisory services in blockchain and cryptocurrencies.

- **Data privacy** drives a substantial portion of law firms’ business, in particular for data breach notifications, data privacy litigation, and privacy compliance. Every state in the U.S. has its own laws detailing when to let consumers know their personal information has been breached and what to do about it. On large scale data breaches, a large part of the defense attorney’s job is helping clients navigate the patchwork of laws. Data privacy litigation is expected to grow in 2020 and beyond, as plaintiffs’ lawyers and litigation funders capitalize on the pandemic to bring COVID-19 related class actions, many of which include claims of data breach and privacy violations specific to companies’ management of personal health data.

- **Data risk management** is a relatively new service offered by law firms seeking a more proactive role helping clients strengthen their cyber defenses. The service takes many forms and can include pure advisory on data risk assessment, threat modeling, and privacy by design, as well as training and awareness. Law firms will also apply their in-depth understanding of data flows to routine reviews of clients’ products and services to identify and resolve privacy and security issues.

### Procurement Priorities

- **Request security audit report for law firm**, paying special attention to data privacy practices and security certifications
- **Pre-breacht due diligence.** Involve in-house legal counsel proactively in pre-breach due diligence process to surface legal risk exposures that need to be remediated with or without the assistance of outside cyber-legal experts
- **Insurance panels.** Query law firm as to whether they are a preferred provider on cyber insurance panels, and, if so, what is the scope of services offered through that relationship and the extent to which the cyber insurance policy covers legal expenses
- **Legal training.** Request employee training on processes and policies to prevent data breaches

### Cybersecurity Services Market Leaders

<table>
<thead>
<tr>
<th>Law Firms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baker &amp; Hostetler</td>
</tr>
<tr>
<td>Cooley</td>
</tr>
<tr>
<td>Hogan Lovells</td>
</tr>
<tr>
<td>Perkins Coie</td>
</tr>
</tbody>
</table>

**(Cost of a Data Breach Report 2020 (IBM and Ponemon Institute, July 2020, pgs. 8 & 9)**
### STRENGTHS
- Unparalleled depth of knowledge about data privacy laws and regulations as they apply to engaging with customers and employees across regions and industries
- Increasing ability to raise data/cyber awareness and influence decision-making among board directors and C-suite executives as GCs evolve their role as trusted adviser
- Business development opportunities through practice referrals, especially high technology clients; alumni network of corporate GCs and lawyers; leads generated from online legal resource repositories targeted to technology start-ups

### WEAKNESSES
- Under-developed ability to institutionalize cybersecurity experience (e.g., case law) and litigation data in knowledge-based products and thought leadership for the business community
- The ever-shortening life cycle and application of emerging technologies challenge law firms’ ability to form timely opinions about inherent data privacy implications
- Consensus-driven partnership model is barrier to strategic investing in legal innovations for data privacy and security services

### OPPORTUNITIES
- Adopt a professional services model that blends teams of lawyers, consultants, and technologists to deliver data privacy advice and data security solutions in line with clients’ business and technology strategies
- Explore opportunities to institutionalize data privacy and security expertise in managed service offerings
- Adopt NIST, SOC-2, and other cybersecurity certification frameworks to assure clients that the firm’s information systems, processes, and data are secure

### THREATS
- Shortage of talent with “future of law” skills in data privacy and security, e.g., knowledge of relevant systems and analytics, data science tools and techniques, related legal disciplines, and project management
- Emerging role of independent attorneys as data breach coaches who provide legal advice for selecting cyber insurance policies and can project manage third-party data breach services
- Category management approach to legal procurement favors bargaining power of buyers who bring deep, professional expertise in cybersecurity to the negotiating table
- Insufficient resources and capacity to continually stay abreast of regulatory and legislative developments in the cybersecurity space

---

Law firms’ competitive advantage is their depth of technical knowledge and proficiency interpreting the laws that govern data privacy and cybersecurity.

Note: SWOT analysis is generalized to the market segment; strengths and weaknesses vary between providers.
Cooley has built a brand that communicates entrepreneurship and leadership in all matters related to technology and intellectual property. Founded in 1920, Cooley's bona fides as the legal avatar of the technology industry stems from an office move in the 1980s to Palo Alto, California, the epicenter of technology innovation that would become known as Silicon Valley. The firm's work with venture capitalists, life sciences companies, and emerging technology startups now encompasses innovators in artificial intelligence, big data, cloud solutions, digital currencies, and cybersecurity. Cooley's Cyber/Data/Privacy practice of 54 lawyers worldwide burnishes this brand, as does Cooley GO, a legal and business resource innovated for entrepreneurs of all sizes.

The Cyber/Data/Privacy practice anchors Cooley's talent and resources for matters related to data privacy and protection. The practice addresses all phases of the information management life cycle - collection, use, storage, disclosure, destruction - and includes protecting the infrastructure that supports the data. Cooley attorneys have extensive experience litigation and investigating regulatory compliance, breach preparedness, and transactional matters. Additionally, the team has defended 50+ class actions in recent years for clients including Facebook, Google, Instagram, Sony, and Tesla, as well as the data breach class actions against eBay and LinkedIn.

Services are delivered by integrated teams that include legal talent from related practice areas, including crisis management, commercial class action litigation, communications regulatory, and technology transactions. The firm’s intellectual property practice includes a dedicated team of patent lawyers who specialize in patent protection for cybersecurity technologies and provide counseling for monetizing those assets. They also advise on cybersecurity issues to companies in traditional industries, including healthcare, telecommunications, and higher education.

In 2014, Cooley launched Cooley GO, a platform for assisting startups throughout all stages of growth. The mobile-enabled microsite provides free legal documents and business content covering business formation, financing, talent, IP, M&A, IPOs, and more. The site is managed by the 200+ lawyers in Cooley’s emerging companies practice with additional content in the form of insights and interviews provided by Cooley attorneys worldwide.

### Cybersecurity Services

**Advisory**
- Board of director advice and consultation
- Consumer and employee privacy
- Corporate services for cybersecurity companies (capital markets support, venture & debt financing, data breach preparation, compliance mapping, government investigations, employment-related privacy issues)
- Cybersecurity risk management
- Data due diligence for M&A
- Incident response planning and preparedness
- Intellectual property (IP) litigation, counseling, and prosecution for cybersecurity technologies
- Data creation, use, and commercialization strategies
- Data governance, compliance, outsourcing, and licensing
- Data retention, security, and destruction programs
- Privacy and data breach litigation
- Vendor management, including fast-track contract negotiations with breach ecosystem service providers (forensic, cybersecurity, crisis communication, etc.) as needed for incident response situations

**Managed Services**
- 24/7 incident response team

---

**Pacesetter Criteria**

<table>
<thead>
<tr>
<th>Business Model</th>
<th>Value Proposition</th>
<th>Service Delivery</th>
<th>Client Enablement</th>
<th>Brand Eminence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact Scale:</td>
<td>None</td>
<td>Low</td>
<td>Moderate</td>
<td>Significant</td>
</tr>
</tbody>
</table>

---

**Paceseters Impact Score**

- 86.6
Hogan Lovells’ entry into the market for cybersecurity services can be traced to 2005, when predecessor firm Hogan & Hartson hired a lawyer with expertise in data privacy. Five years later, as data privacy was developing into a full-fledged legal discipline, Hogan launched a global privacy and cybersecurity practice with seven lawyers. Today, Hogan has 200 lawyers practicing data privacy law and a cybersecurity practice comprised of lawyers, risk consultants, and professionals with technical and subject matter expertise in complementary services such as crisis communications and information technology. The mix of talent and competencies positions Hogan as a legal advisor with a business sensibility, capable of helping clients respond to, manage, and mitigate their cyber risks.

Cybersecurity services are anchored in two practices - Privacy & Cybersecurity and Cyber Risk. Each practice is comprised of focus areas specializing in industry sectors and specific cybersecurity functions, such as incident response. Hogan operates across a spectrum of industry sectors and has developed strengths in cybersecurity matters specific to automotive manufacturers and healthcare providers.

Hogan’s in-house Strategic Communications group provides crisis communications and reputation management services to Privacy & Cybersecurity clients. These services are coordinated by Hogan’s Crisis Leadership Team, which was launched in November 2019 to support clients in two ways. One is when they are amid a crisis, and the other is to help build a crisis management capability that strengthens organizational resilience. This group sponsors the Crisis Leadership Portal and mobile app, a resource for in-house counsels to assess their organization’s crisis readiness, review case studies, and access tailored guidance packages on emergency preparedness and response. Hogan co-develops the portal’s resources in partnership with Elevate, a provider of consulting, technology, flexible resourcing, and managed services to law firms.

---

### Hogan Lovells

<table>
<thead>
<tr>
<th>Business Model</th>
<th>Value Proposition</th>
<th>Service Delivery</th>
<th>Client Enablement</th>
<th>Brand Eminence</th>
</tr>
</thead>
</table>
| Pacesetters Impact Score

**Advisory & Consulting**

- Cyber Risk
  - Cyber regulatory
  - Program development
  - Vendor evaluation and selection
- Privacy & Cybersecurity
  - Breach preparedness, response, investigation, and communications
  - CCPA
  - Corporate and commercial transactions
  - Data privacy risk management, governance, and compliance
  - E-discovery and information management
  - Fintech
  - Health privacy and cybersecurity
- Strategic Communications

**Managed Services**

- Cyber Risk: Incident and crisis response
- Cyber Risk: Training and awareness

---

Source: ALM Intelligence, 2020
Perkins Coie goes to market with a perspective that positions data protection and privacy as a business advantage. The firm assists organizations with risk-intelligent strategies and services related to the collection, use, storage, protection, sharing, and disposal of personal and other types of regulated information. As such, legal advisory services are delivered with a legal operations mindset that integrates "privacy by design" principles into data privacy services and programs.

The firm’s Privacy & Security practice of 89 professionals delivers end-to-end services, from privacy assessments and policy reviews to regulatory investigations and class action litigation. Select advisory services are backed by managed and outsourcing services in cyber enforcement and incident response. Attorneys work largely with stakeholders in the board, C-suite, and General Counsel’s office, ensuring they are current on the impact of data privacy regulatory and statutory developments for mobile applications, online and mobile advertising, electronic surveillance, and cloud computing.

The Seattle-based firm has been directly connected to the U.S. Pacific Northwest’s high technology sector since it was selected as Boeing’s legal advisor in 1912, the year Perkins Coie was founded. Boeing is still a client, as are Amazon, Facebook, Google, Microsoft, Starbucks, Twitter, and other major corporations. The Privacy & Security practice has successfully represented social media giants in multiple class actions regarding privacy issues and claims of unfair competition by app developers. The firm also targets technology start-ups and was one of the first to establish Fintech and blockchain practices that now serve virtual currency exchanges, large and small blockchain innovators, payment processors, investors, and industry associations. Outside of technology, the firm serves a broad range of clients across the private and public sectors, including Democratic Party and left-of-center political candidates in the U.S. and non-profit clients worldwide.

The connection to high technology has imbued Perkins Coie with an appetite for innovation. In 2015, the firm launched Perkins Coie CoinLaw, a mobile app designed to provide snapshots of the status of virtual currency regulations in individual countries and access to the firm’s Virtual Currency Report Blog. The firm also created a workflow management tool to collaborate with clients’ in-house legal teams and track projects as part of its Client Advantage program. The tool enables clients to have more control over how their work is resourced and charged.

### Cybersecurity Services

**Advisory & Consulting**
- Product and General Privacy and Security Counseling
- Electronic Surveillance and User Information Requests
- Online and Mobile Advertising
- Privacy Reviews, Assessments and Data Transfers
- Network Intrusion and Data Breaches
- Privacy Litigation and Regulatory Investigations
- Cyber Enforcement
- International Privacy and Data Flows
- Privacy by Design
- Telephone Consumer Protection Act (TCPA) Compliance and Defense

**Managed Services**
- Cyber enforcement outsourcing
- Incident response

**Client Services**
- Client Advantage Program (legal project management, strategic pricing and budgeting, matter performance, continuing education, professional development, and more)
Demand Drivers
The economic slowdown anticipated by COVID-19 points to challenging years ahead for consulting, a business whose growth has always been tied to economic cycles of expansion and retraction. The global consulting market is expected to contract in 2020, as clients reduce or eliminate discretionary expenses, including the use of external advisors. The exceptions to this outlook are digital transformation and cybersecurity consulting, which should be no surprise in view of the global shift to an online operating environment that has accelerated demand for both categories of service.

It should be noted that the objectives, business models, and operating models differentiate peer groups within the consulting segment, exposing relative positioning regarding cybersecurity program assessments, improvements, and developments. The common denominator across these groups is a risk management-led approach informed by a comprehensive understanding of market trends.

• **Building organizational cyber resilience** is a shared objective across the consulting segment. The collective effort is showing success as measured by the increasing adoption of enterprise-wide cybersecurity incident response plans, which IBM/Ponemon research reports has grown by 44% since 2015.¹ These providers bring a comprehensive storefront of tools and technologies to drive a risk-based approach that incorporates Cybersecurity by Design principles into all aspects of business and operating model design and ecosystem management. They also are playing an invaluable role helping executives cultivate a deeper understanding of data privacy as an essential function of cybersecurity, advancing the business case for using tools and technologies across functions to ensure protection against cyber threats to information, as well as infrastructure and applications.

• **Managed cybersecurity services**, including those for data privacy, have been an important deliverable that enables providers’ end-to-end consulting and implementation capabilities. The provision of managed cybersecurity services is a core pillar of providers’ mergers and acquisitions strategies, which have focused largely on acquiring cybersecurity boutiques with expertise in specific functions, such as managed detection and response and threat intelligence, that are built using next generation technologies, such as AI and advanced analytics. The pandemic has focused organizations on strengthening their defenses for a remote working environment, giving rises to acquisitions of endpoint security solutions that build in multifactor authentication and artificial intelligence for better detecting vulnerabilities tied to human behavior.

(¹) Cyber Resilient Organization Report 2020 (IBM Security, Ponemon Institute, 2020, pg. 5)
### STRENGTHS

- Strategic approach aligns cybersecurity priorities with business strategy for an enterprise perspective that promotes executive awareness and buy-in
- Capable of improving both the operating system of technologies used to enable cybersecurity functions and the management system for mobilizing and directing resources across the enterprise to execute the cybersecurity strategy
- Agnostic position brings informed, objective perspective of the technology landscape and an ability to design customized cybersecurity solutions that interoperate with legacy systems
- Commitment to corporate development of cybersecurity capabilities through organic and inorganic strategies

### WEAKNESSES

- Inflexible approach to negotiating pricing
- Outdated governance frameworks and/or insufficient capacity for monitoring cybersecurity hygiene of external ecosystem, that is, third party providers of advisory services (e.g., law firms), risk transfer products (insurance brokers, insurance on-demand platform providers), and infrastructure support (network and cloud services, security platforms, etc.)

### OPPORTUNITIES

- Elevate board mindset from awareness to tactical appreciation of cybersecurity as an enterprise risk, for example, by engaging directors in scenario planning that leverages virtual reality tools and with financial reports that quantify cybersecurity ROI and impact on profitability
- Develop case study examples that illustrate a correlation between cybersecurity and market-focused outcomes, for example, how strengthening endpoint security improved the customer experience (external market) and the employee experience (internal market)
- Integrate cybersecurity strategies and training in leadership development programs

### THREATS

- Demand for cybersecurity technology and data science talent far outstrips supply while competition for senior consulting talent with industry, public sector, and military cyber experience is intensifying, challenging providers to develop employee value propositions that strengthen their unique brand in the open talent marketplace
- Underestimating the importance of market differentiation in cybersecurity’s crowded, fragmented landscape coupled with the lack of consistent attention and investment in marketing function activities, including customer experience research, competitive intelligence, and the development of timely content that communicates knowledge and brand value

---

Note: SWOT analysis is generalized to the market segment; strengths and weaknesses vary between providers
BCG goes to market with an approach grounded in management and industry consulting to help clients build a cyber secure environment. Services are provided by the Cybersecurity practice, a virtual network of blended talent drawn from across BCG’s internal ecosystem of traditional management consulting practices and the digital, technology, and analytics capabilities of DigitalBCG. BCG engages the board of directors and C-suite on cyber strategy and risk tolerance, while it works with security, risk, and IT departments to integrate cyber strategies across the organization’s technology infrastructure, workflows, and people practices. It’s a top-down, bottom-up approach laser-focused on helping clients improve their organization’s cyberresilience.

BCG Cybersecurity delivers services through four offerings: evidence-based cyber strategy, cyber risk analytics, cyber capability build, and cyber industry & ecosystem advisory. Each offering has a clear set of deliverables that provide a systematic, pragmatic, and measurable approach to designing and operating a cybersecurity function, as well as for building identification, protection, detection, and response and recovery capabilities. In addition, BCG’s Platinion subsidiary within DigitalBCG provides services in more technical areas, such as secure source code screening and data architecture design. The industry and ecosystem advisory business enables BCG to execute business strategy engagements for vendors of cybersecurity products and services and for institutional investors.

BCG manages an external ecosystem of strategic innovation partners and organizations on the front lines of regulating and researching cybersecurity. Innovation partners include QuoScient, a security operations boutique founded by former members of Deutsche Bank’s cybersecurity teams, and CAST, which offers a proprietary toolset for developing and testing source code. Research partnerships with the World Economic Forum, NIST, MIT Sloan, and The Geneva Association position BCG as a thought leader shaping cybersecurity standards and policies for governments and industries.

### Cybersecurity Services

#### Cyber Strategy
- Cyber maturity and culture assessment
- Board & C-suite workshops
- Capability gap identification
- Business-driven, risk-aligned capability roadmaps

#### Cyber Risk Analytics/Doppler
- Cyber risk exposure assessment (using Cyber Doppler tool)
- Cyber threats identification
- End-to-end cyber project portfolio optimization
- Threat intelligence (leveraging 3rd party partnerships)

#### Cyber Capability Build
- Cyber governance & associated organization design
- Crisis management, IT, business continuity management, and data recovery plans
- Vendor/provider identification and rollout oversight
- Secure product development process
- Regulatory readiness
- Cybersecurity Transformation Program (Build-Operate-Transfer)

#### Cyber Industry & Ecosystem Advisory
- Business and go-to-market strategy for cybersecurity providers
- Cyber due diligence for corporate transactions and portfolio companies
- National cybersecurity policy, strategy, and ecosystem build
- Cybersecurity standards for the public sector

### Pacesetter Impact Score

<table>
<thead>
<tr>
<th>Pacesetter Criteria</th>
<th>Pacesetter Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Model</td>
<td>Moderate</td>
</tr>
<tr>
<td>Value Proposition</td>
<td>High</td>
</tr>
<tr>
<td>Service Delivery</td>
<td>Very High</td>
</tr>
<tr>
<td>Client Enablement</td>
<td>Significance</td>
</tr>
<tr>
<td>Brand Eminence</td>
<td>High</td>
</tr>
</tbody>
</table>

Impact Scale: 〇 None 〇 Low 〇 Moderate 〇 Significant 〇 High 〇 Very High
Crowe seeks to elevate cybersecurity from an exercise in technology and compliance to an organizational capability for digital resilience by breaking down the internal barriers between corporate functions and the business. The firm goes to market with an enterprise approach targeted to c-level and board executives, combining strategic consulting with technical and industry expertise. This approach is backed by a comprehensive array of services, solutions, and practical experience implementing cybersecurity technologies and processes, enabling Crowe to address a broad range of stakeholders’ interests.

Services are delivered by Crowe’s Digital Security team of professionals who are trained to actively listen and engage in the scoping process to ensure clients’ unique needs are met. The priority is to align recommendations and services to the client’s operation, size, culture, and IT strategy. For clients seeking to engage in cyber-scenario planning, Digital Security hosts ideation sessions using Crowe Blue Sky, a mobile, physical laboratory hosted at the client site that is now virtual in consideration of pandemic precautions. These session may include CroweX, a team of senior experience designers who will map Digital Security's offerings to the client's journey. In addition, Crowe has a strategically constructed ecosystem of technology partners with whom it collaborates on threat detection and endpoint security (Carbon Black, Check Point, Elastic). The firm is also a Microsoft Security Partner.

Crowe commits a percentage of annual revenues to an innovation program focused on building strategic solutions that enable better decision-making and adapting new technologies to proven security practices. Crowe Cyber Aware, for example, is a recently launched solution that translates an organization’s cybersecurity program into financial metrics using X-Analytics, a patented cyber risk analytics engine. Cyber Aware bridges the communications gap between CISOs and executives with dashboards that detail specific risks, offer actionable guidance, and track the ROI of cyber investments. Another example is a penetration-testing service for pre-production IoT devices that are typically designed without endpoint security in mind.

Crowe provides platform-enabled managed services, as well, including Crowe MDR (24/7 security operations, real-time detection, proactive threat hunting); Incident Response and Recovery (response plans, resolution team, post-breach recover); Program Maturity (cyber resilience benchmark, maturity roadmap, compliance assessments); and vISO (security professional staff augmentation, cost benefit analysis, executive communications, and more).

### Pacesetter Criteria

<table>
<thead>
<tr>
<th>Pacesetter Criteria</th>
<th>Pacesetter Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Model</td>
<td>Value Proposition</td>
</tr>
<tr>
<td>Impact Scale:</td>
<td>None</td>
</tr>
</tbody>
</table>

Cybersecurity Services

- **Strategic Advisory & Risk quantification**
  - Executive cyber strategy
  - Risk appetite and quantification
  - Board and executive reporting

- **Assessment & Roadmap Development**
  - Cybersecurity risk and maturity assessments
  - IT governance, risk and compliance
  - Privacy compliance assessments
  - IT audit/PCI/SOC

- **Prevention and Detection**
  - Crowe Security Insights (CSI)
  - Technology/solutions implementation
  - Security awareness program
  - Third party risk management

- **Network, Applications & Cloud Security**
  - External and internal penetration testing
  - Web application testing
  - Creative social engineering
  - Cloud security assessment

- **Virtual Information Security Office (vISO)**
  - Outsource/co-source cybersecurity professionals

- **Monitoring and Incident Response**
  - Managed detection and response (MDR)
  - Incident response planning
  - External breach simulation
  - Internal purple teaming exercise
  - Tabletop incident response testing

Program Management Office (PMO)
FTI Consulting believes that cybersecurity should be part of every company's strategic growth strategy for two reasons. The first is to ensure the safety of the organization's assets that fuel growth, and the second is to assure corporate leaders and investors that their interest in the company is protected. This belief underscores FTI's overall purpose to help organizations protect and enhance enterprise value in an increasingly complex legal, regulatory, and economic environment.

To deliver on this commitment, FTI Cybersecurity goes to market with an expert-led approach to service delivery. The global practice is comprised of incident response consultants, developers, and data analysts with extensive investigative backgrounds, led by cybersecurity experts who have decades of experience at the highest levels of law enforcement, intelligence agencies, and global private sector institutions. Service delivery is also intelligence-led, meaning FTI infuses traditional consulting methodologies with forensic techniques to support clients in the prevention, response, and investigation of cyber threats and incidents.

FTI Cybersecurity’s professionals combine end-to-end capabilities when clients face high stakes litigation, arbitration, and compliance investigations and regulatory scrutiny. The firm's core offering focuses on cyber readiness, incident response, and complex investigations. The Cybersecurity practice integrates capabilities from across the firm, as well, leveraging the global investigations, damages estimation, regulatory management, and crisis communications teams. FTI serves clients of all sizes and across all sectors and is particularly noted for the breadth and depth of services it provides to law firms.

In terms of technology solutions, FTI is agnostic and partners with specialists to provide endpoint detection and monitoring and managed services, including security operations center (SOC) services. The real strength of its ecosystem is in the relationships it maintains with the world’s leading global intelligence agencies, regulatory authorities, and law enforcement agencies that are the alma maters for members of its global cybersecurity team.

Cybersecurity is a target of corporate development for FTI. Over the past 18 months, FTI has recruited senior talent to lead its growing cybersecurity practices in Asia Pacific and EMEA, who, in turn, recruited seven professionals in London and Seoul. Last year, Crowe recruited two high-ranking professionals from the FBI. Ronald Yearwood, the FBI’s Chief Hacker joined the San Francisco office, and Jordan Rae Kelly, former Director for Cyber Incident Response at the U.S. National Security Council and Chief of Staff for the FBI’s Cyber Division joined FTI’s Washington, DC office.

**Cybersecurity Services**

**Assess**
- Cybersecurity risk profiles
- Security data collection and correlation
- Threat analytics
- Insider threat and workplace misconduct analysis

**Defend**
- Cybersecurity compliance preparedness
- Implementation of network defense tools
- Vulnerability assessments
- Penetration testing
- Employee training

**Identify**
- Threat alerting and reporting
- Continuous risk monitoring

**Recover**
- Post-incident activity reporting
- Risk mitigation
- Cyber insurance advisory

**Respond**
- Incident response program development
- Containment, eradication and recovery
McKinsey views cybersecurity as a business enabler and accelerator that is critical to driving growth in the digital economy, from product development through supply chain operations. Cybersecurity is positioned as a key component of the corporate strategy and business model to ensure it is built into the design of products, processes, and digital technology platforms. McKinsey’s analytics-driven, risk-focused approach to cybersecurity strengthens the foundational protections of the enterprise in an ever-expanding digital ecosystem.

While much of its work is standalone, McKinsey has increasingly focused on embedding cybersecurity into digital transformations to enable the adoption of agile, cloud, and DevOps operating models. The recent investment in Praetorian strengthens this capability with security solutions for IoT, SaaS, and mobile applications that connect across cloud and on-premise networks, as well as the critical infrastructure of public utilities. By pursuing digital and security transformations in parallel, McKinsey helps its clients reduce time to market for new applications, unlock innovation, and drive efficiency and effectiveness while also maintaining security requirements.

Services are delivered through consulting service lines by the firm’s Cybersecurity practice, which is a joint venture between Digital McKinsey and McKinsey’s Risk management consulting practice. Security practice professionals include human-centered design specialists, data scientists, software specialists, and agile engineers and coaches who work alongside traditional management consultants on multidisciplinary engagements. McKinsey manages internal and external ecosystems of skilled talent, as well, including a CISO network of industry professionals who provide advisory services to McKinsey clients. The practice is extending its global reach by building up regional hubs in Latin America, France, Iberia, Japan, and the UK, as well as fostering more interaction with Asia.

McKinsey has developed a robust portfolio of intellectual property to accelerate diagnostics, design, and implementation. A sampling includes the Digital Resilience Assessment (DRA) methodology for benchmarking cyber maturity against peers using the NIST Cybersecurity Framework; Cyber Risk Insights (co-created with MetricStream), a tool for identifying cyber risk across the business value chain by using NIST 800-53 and ISO27001 to assess Crown Jewel system control maturity; a Cyber Threat Snapshot (CTS) tool to provide a rapid perspective into vulnerabilities and exposures on the Dark Web, and the Cyber Market Map, which identifies trends in the cybersecurity market across today’s and tomorrow’s security tools. In terms of thought leadership, McKinsey consultants regularly generate research and insights that reinforce how cybersecurity is an enabler of value to organizations, including publications and presentations for national level organizations and journals.

### Cybersecurity Services

- **Cybersecurity markets**
  - Product strategy
  - Go-to-market support
  - Transaction support
- **Digital security transformation**
  - Digital strategy and compliance
  - Privacy assessment, tracking, and compliance
  - Information security
  - Operational security
  - Business continuity strategy and crisis management
  - Risk analytics/Agile/cloud/DevOps technology model design
  - Cyber talent management and learning
  - Cyber leadership development
- **Crisis preparedness and response**
  - Cybersecurity breach simulation/wargaming
  - Incident response planning
  - Crisis management

### Pacesetter Criteria

<table>
<thead>
<tr>
<th>Business Model</th>
<th>Value Proposition</th>
<th>Service Delivery</th>
<th>Client Enablement</th>
<th>Brand Eminence</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Low</td>
<td>Moderate</td>
<td>Significant</td>
<td>High</td>
</tr>
</tbody>
</table>

Impact Scale: None | Low | Moderate | Significant | High | Very High

---

McKinsey & Company

**Primary Practice:** Cybersecurity

---

**Cybersecurity Services**

- **Cybersecurity markets**
  - Product strategy
  - Go-to-market support
  - Transaction support
- **Digital security transformation**
  - Digital strategy and compliance
  - Privacy assessment, tracking, and compliance
  - Information security
  - Operational security
  - Business continuity strategy and crisis management
  - Risk analytics/Agile/cloud/DevOps technology model design
  - Cyber talent management and learning
  - Cyber leadership development
- **Crisis preparedness and response**
  - Cybersecurity breach simulation/wargaming
  - Incident response planning
  - Crisis management
**Demand Drivers**

Perhaps no other segment has had to pivot so quickly to respond to the abrupt shift in client needs provoked by the COVID-19 crisis. Almost immediately, organizations realized their computer systems were not designed to manage a large, remote workforce or interact with vendors outside of a secure, on-premises network. As they adjusted, many sidestepped normal security processes to quickly get people working and supply chains flowing. Such compromises not only increased their exposure to cyber attacks, but also to significant financial damage in the event of an attack should they have invalidated the terms of their cyber insurance policies. Against this backdrop, technology providers are rethinking their strategies and offerings to accommodate a new security landscape.

Providers in this segment tend to be either pure pure-play cybersecurity technology firms or firms with established technology security practices that are, to some degree, supported by a management and/or cybersecurity consulting capability. They share an objective to assess, design, and build every aspect of an IT security program with an emphasis on integrating threat intelligence.

- **Managed security services (MSS)** are evolving to offer IT teams the expertise and depth of functionality needed to protect data and systems in the remote working environment. Technology providers had already established themselves as MSS powerhouses, whether they focus on one security function, typically managed detection and response, or multiple security functions, e.g., cloud infrastructure, data, identity management, and overall platform security. Areas of investment include acquisitions that expand the global reach for managed services in cyber threat intelligence, threat hunting, vulnerability management, and endpoint security.

- **Additional strategies to expand global reach** include white-label and reseller agreements where the provider’s managed services are offered to pure-play Managed Security Services Providers (MSSPs) and their clients.

- **Building consulting capabilities** is another area of focused investment, particularly among the pure-play technology providers. They are investing in talent to strengthen their assessment and governance consulting capabilities, and cloud advisory expertise to help clients implement secure cloud platforms.

**Procurement Priorities**

- **Request security audit report** for vendor and vendor’s third-party partners, paying special attention to compliance with international laws related to data privacy and security
- **Perform needs analysis** to develop selection criteria focused on your organization’s system requirements; document those requirements
- **Establish evaluation criteria** for security technologies to ensure systems integrity, for example, ask vendor whether new functionality is merged into core products or offered on a standalone basis to augment existing systems
- **Analyze total cost of ownership** for security solutions recommended by providers, including expenditures for implementing, training, testing, consulting, compliance, upgrades, and additional staff needed throughout its expected life cycle
STRENGTHS

- Unparalleled expertise in legacy, current, and emerging cybersecurity technologies and capabilities for assessing, designing, and building every aspect of an IT security program with an emphasis on integrating threat intelligence.
- Able to reshape the role of the modern CIO and CISO from technology guardians to orchestrators of enterprise programs that involve all business leaders in the design and execution of cybersecurity strategies.
- Sophisticated toolkit for service delivery includes data visualization/analytics, managed services, and techniques drawn from hands-on solutions execution experience focused on creating efficiencies.

OPPORTUNITIES

- Strengthen support for client response to pandemic with scenario planning exercises and use cases that illustrate the value of implementing zero trust security systems on their networks.
- Expand assessments and frameworks to identify opportunities for integrating cybersecurity optimization and efficiency techniques into enterprise risk operations and training programs.
- Develop diagnostic tools to identify the emergence of shadow IT systems that can develop in the virtual office business model.

WEAKNESSES

- Inconsistent performance integrating acquisitions of cybersecurity companies, especially start-ups and younger peers with different cultures and approaches to client service.
- Preference for bringing numerous people representing multiple cybersecurity technologies to client meetings increases cost of sales and dilutes strategic messaging.
- Complaints of constant upselling to address threat trends take toll on relationship trust.

THREATS

- Competition from consulting providers whose agnostic approach to cybersecurity technology, ability to write application interfaces, and ecosystem management capabilities enable best-of-breed solutions design, precluding the need for technology providers’ end-to-end services.
- Overcrowded cyber technology landscape creates confusion among buyers, fragmenting mindshare for established brands competing on innovation.
- Threat from counterfeit and low quality product imitations from emerging markets.

Note: SWOT analysis is generalized to the market segment; strengths and weaknesses vary between providers.
Accenture Security’s business spans a range of professional services across all industries, from strategic consulting and proactive risk management to digital identity, cyber defense, response and remediation services, and managed security services. The firm continues to strengthen its market position through an aggressive program of acquisitions, innovation, talent management, and brand eminence. In its fiscal 2020 third quarter earnings call, Accenture CFO KC McClur commented that 70% of new bookings (~$8 billion) were for digital, cloud, and security services, proof that the strategy is translating into substantial market demand.¹ This is no small feat considering the COVID-19 pandemic globalized in March, the first month of Accenture’s fiscal third quarter.

Accenture Security targets the market for large-scale security transformations. Its comprehensive portfolio of services is organized to deliver business resilience and brand protection, the latter a source of economic value that can be quantified using Accenture Strategy’s Competitive Agility Index. The firm seeks to secure the physical, digital, and virtual assets of the client’s extended enterprise, and has evolved its approach to the demands of Industry 4.0 modernization in a framework that adds a third dimension of interoperability to value chain models. The firm scales service delivery using automation and artificial intelligence that also enhances the CISO’s ability to drive better business outcomes.

Accenture Security shares a P&L and resources with Accenture Federal Services LLC (AFS), a subsidiary that provides managed cybersecurity services to U.S. federal agencies. Applying best practices from private to public sector clients and offering end-to-end solutions is key to Accenture’s growth in this space. On its own, AFS has been awarded contracts by several agencies, including the U.S. Department of Defense. To facilitate this engagement, AFS opened the Federal Cyber Center in San Antonio, Texas, staffed by an interdisciplinary team of advanced cyber defense experts providing services for managing, detecting, and responding to cyber threats.

Accenture Security works with law enforcement, regulators, and a large ecosystem of specialists who provide cyber defense support, trend analysis, threat hunting, advanced threat analytics, and more. The practice has formed alliances and partnerships with Endgame, IronNet, Microsoft, Palo Alto Networks, Ripjar, ServiceNow, and Splunk. The underlying goal is to industrialize security systems by embedding artificial intelligence, analytics, big data, and machine learning into their design.

¹ Accenture 3rd Quarter Fiscal 2020 Conference Call Transcript (Accenture, 25 June 2020, pg. 5)
FireEye, Inc. is a provider of cybersecurity solutions that uses a mix of security software products, threat intelligence research, and hands-on services to help clients protect their networks against attacks and malicious software. The company was founded in 2004, went public in 2013, and currently serves more than 9,300 customers across 103 countries and protects more than 1,000 government and law enforcement agencies worldwide. Through a series of strategic acquisitions, FireEye has strengthened its bench of 700+ highly experienced threat researchers, platform engineers, malware analysts, intelligence analysts, and investigators, and diversified its platform beyond protection and detection to include investigation processes.

FireEye organizes its business around security solutions and professional services. The company operates as an extension of its customer’s security operations, going to market with FireEye Helix Security Operations, a single platform that blends security technologies, nation-state level threat intelligence, and Mandiant® consulting. The solutions suite includes on-premise and cloud-based endpoint technology, network sensors and analytics, and managed detection and response (MDR) platforms. Technology is deployed according to the threat environment profiled by Mandiant’s Framework for Security Needs, which is structured around five security functions: respond, assess, transform, train, and defend.

FireEye is investing in Mandiant Consulting with new services and additional capacity to deliver in Mandiant Advantage, an offering that brings Mandiant’s consulting services, threat intelligence, managed defense, and Helix and Verodin solutions into a unified platform. The offering includes related open source information, enabling clients to embed FireEye’s threat intelligence and validation capabilities into all security operations, whether they leverage FireEye control products or not. Mandiant Advantage is a critical step in FireEye’s transformation to a vendor-agnostic service provider.

FireEye manages an extensive ecosystem of technology solutions providers (e.g., AWS, Microsoft, Oracle), global law firms (e.g., Baker & Hostetter, Ropes & Gray), and insurance brokers and underwriters (e.g., AXA, Beazely, Marsh). For the latter, Mandiant offers a Cyber Insurance Risk Assessment service targeted to C-suite executives that proposes strategic recommendations for improving an organization’s overall cyber risk posture. FireEye also sponsors a reseller program for MSSPs that provides a combination of technology platforms, cyber intelligence, and professional services. There are currently 26 partners, including BT, GuidePoint, and IBM. Select services, such as incident response services, are offered on a retainer basis.

### Pacesetter Criteria

<table>
<thead>
<tr>
<th>Business Model</th>
<th>Value Proposition</th>
<th>Service Delivery</th>
<th>Client Enablement</th>
<th>Brand Eminence</th>
<th>Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Low</td>
<td>Moderate</td>
<td>Significant</td>
<td>High</td>
<td>Very High</td>
</tr>
</tbody>
</table>

Source: ALM Intelligence, 2020
The Herjavec Group is a managed security services provider (MSSP) founded by Canadian entrepreneur and angel investor Robert Herjavec in 2003 as a vendor of CheckPoint firewall technology. The firm has grown along with the cybersecurity industry, expanding its managed services offering to include security operations center (SOC) services, threat detection, and security technology engineering. Herjavec also offers a mix of advisory and consulting services specific to cybersecurity, including, but not limited to governance, risk, and compliance; data privacy assessments, including GDPR and payment card industry (PCI) compliance; identity and access management (IAM); and technology and architecture implementation.

Herjavec goes to market with a flexible service delivery model targeted primarily to CIOs and CISOs. The approach is to support clients with the selection and management of SOC 2 Type 2 cybersecurity technology, including the development of road maps for executing and implementing those technologies. Its technology solutions ecosystem is comprehensive and includes over 53 market leaders such as Crowdstrike, FireEye, Palo Alto Networks, and Splunk. Services are delivered by integrated teams of advisory, consulting, and managed services professionals who are committed to building clients’ capabilities through knowledge transfer.

Recent acquisitions have strengthened Herjavec Group’s capabilities in identity and access management (IAM). The acquisition of Aikya Security Solutions in 2016 expanded Herjavec’s identity and access product portfolio to include CyberArk, Lieberman Software, RSA Identify, and SailPoint technology suites. In July 2020, the firm acquired Securience, a provider of identity and access management programs for complex global enterprises.

Select services, such as incident response, are offered on a retainer basis.

### Cybersecurity Services

**Advisory & Consulting**
- Cybersecurity maturity model measurement
- Governance, risk and compliance
- Identity services
- Incident response
- Privacy/GDPT assessments
- PCI compliance
- Security assessments and testing
- Security workshops
- Technology and architecture implementation
- Third party risk
- Threat hunting and advisory services

**Managed Services**
- 24/7 threat detection
- 24/7 identity management
- Endpoint detection and response
- Incident response
- Managed phishing service
- Secure gateway (firewall, IPS, email, URL & content filtering)
- Security technology engineering
- SOC operations
- Threat management
- Vulnerability scanning
- Custom-built solutions
  - HG Threat Framework
  - HG Analytics Platform

---

**Pacesetter Criteria**

**Business Model**
- Value Proposition
- Service Delivery
- Client Enablement
- Brand Eminence

**Pacesetter Impact Score**

- Cybersecurity Services
  - Advisory & Consulting
  - Managed Services

Impact Scale: 0 None 1 Low 2 Moderate 3 Significant 4 High 5 Very High
IBM’s cybersecurity business is largely devoted to managed services and technology solutions, which account for roughly half of practice revenues for IBM Security. This suggests that IBM is pursuing a managed security services provider (MSSP) business model, which will evolve into one that is largely cloud-based as IBM advances its strategy to become a leader in the market for cloud services and solutions. IBM Security has an advantage over traditional MSSPs, however, because its business model is more expansive. It includes strategy and operations consulting, software and technology and as-a-service platform solutions. This combination more accurately reflects how today’s enterprise clients are buying cybersecurity services to enable the design, build, operation, and integration of private, public, and hybrid cloud environments.

IBM’s platforms and tools cover a range of security processes, including identity access management, application and cloud security, endpoint management, fraud protection, and data security and privacy. The practice is recruiting professionals to build out its service offerings to support organizations that lack a cybersecurity infrastructure and talent. These services are grounded in analytics, artificial intelligence, and cognitive technology. One such solution is QRadar Security Intelligence, a platform that combines advanced analytics with machine learning and the cognitive capabilities of Watson® for Cyber Security to automatically investigate security incidents in real time and provide SOC analysts with actionable insights.

Support is provided by IBM Security Expert Labs, a global network of more than 3,700 consultants and 3,300 service delivery experts trained in agile and DevOps methodologies who help clients implement and master IBM solutions. Expert Labs also offers a subscription-based bundle of services that can be customized to include direct access to specific expertise, personalized training, priority case handling, and built-in consulting hours.

IBM also partners with MSSPs in two types of arrangements. One where IBM white-labels its security managed service offerings to MSSPs and their clients. The second is IBM’s Cloud Reseller program structured to provide tiered levels of support and access to IBM’s distribution channels and innovation ecosystem.

### Cybersecurity Services

#### Consulting
- Cloud security advisory and implementation
- Identity access, governance, risk, and controls
- IT risk management
- Payment card industry (PCI) compliance
- Security information and event management (SIEM)
- Security and intelligence operations and consulting
- Security strategy, risk, and compliance

#### Technology Solutions
- IBM CloudPak for Security
- IBM Privilege Manager
- IBM QRadar Security Intelligence Platform
- IBM Secret Server (identity & access management)
- IBM Security Guardium
- IBM Security Maas360® with Watson™
- SOAR/Security orchestration, automation and response
- IBM IGI/Identity governance and intelligence

#### Managed Security Services
- Application security services
- Firewall management
- GRC-as-a-service (governance, risk, and compliance)
- IBM Security Verify (identity-as-a-service)
- IBM X-Force cloud security services
- IBM X-Force incident response and intelligence services
- IBM X-Force red offensive security services
- IBM X-Force threat management services
- Identity and access management services
- Infrastructure and endpoint services
- Intrusion detection and prevention system management
- Managed detection and response (MDR)
- Managed identity services
- Secure SD-WAN (software-defined wide area network)
Appendix
The goal of ALM Pacesetter Research is to help buyers of professional services navigate an increasingly complex landscape with confidence. We use a multidisciplinary perspective to identify best-in-class providers of legal, consulting, financial, insurance, employee benefits, and other professional services, and analyze how they are evolving as an ecosystem of interdisciplinary service providers. Our research is grounded in over 50 years of accumulated market insights and qualitative research models that combine knowledge of management science with case studies and other sources of knowledge to understand patterns of market supply, demand, behavior, and ways of doing business.

**IDENTIFY**
- The ALM Pacesetter Advisory Council (PAC) convenes in advance of the research project kick-off; members include ALM journalists and editors, and external experts such as consultants, general counsel, and industry thought leaders
- The PAC selects the set of Market Leaders that will be covered in the research topic from a larger group of providers that members have identified in the normal course of their work
- PAC members also provide expert knowledge and insights to the ALM Pacesetter team throughout the research and analysis process

**RESEARCH**
- The ALM Pacesetter Team within ALM Intelligence conducts primary and secondary research
- Primary research includes in-depth interviews with practice leaders at the provider firms covered in the research; satisfaction interviews with clients referred by those providers; and in-depth interviews with thought leaders, recruiting professionals, and other sources
- Secondary research includes data gathered from annual reports and earnings calls, management presentations, public filings, case studies, press releases, journals and publications, online information databases and other publicly available resources

**ANALYZE**
- ALM Pacesetter analysts evaluate and score the Market Leaders against five core criteria
  1. Business model
  2. Value proposition
  3. Service delivery
  4. Client impact
  5. Brand eminence
  
  See criteria definitions on next page
- Market Leaders that achieve a Pacesetter Impact Score equal to or over 85 are designated as ALM Pacesetters
- Pacesetter analysts map markets and stakeholders and write market trends
- Market segment overviews are peer reviewed by the appropriate PAC member
### Core Criteria

<table>
<thead>
<tr>
<th>Core Criteria</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Business Model** | Provider's ability to reposition core competencies around new products, services, and business models to adapt to shifting patterns of market supply, demand, behavior, and ways of doing business   
Detailed Criteria: scope of services, supply chain, ecosystem, corporate development, innovation capability                                                                                                                                                                                                                                                                                                                                                           |
| **Value Proposition** | Provider's ability to deliver on its value proposition, i.e., the positioning statement that communicates the benefits and economic value a prospect will receive by purchasing the provider's products and services over a competitor's  
Detailed Criteria: differentiated services, risk management, measurable outcomes, evidence-based solutions, pricing options                                                                                                                                                                                                                                                                                                                      |
| **Service Delivery** | Provider's ability to mobilize resources and configure assets to serve clients  
Detailed Criteria: solutions design, engagement model, talent and culture, project management, enabling tools                                                                                                                                                                                                                                                                                                                                                           |
| **Client Enablement** | Provider's ability to help clients affect continuous, sustainable change, improve performance, and achieve growth  
Detailed Criteria: client relationship management, business case development, stakeholder conversations, change management and capability development, living laboratory                                                                                                                                                                                                                                                                            |
| **Brand Eminence** | Provider's ability to leverage brand and marketing strategies to differentiate in its marketplace as an expert practitioner and thought leader  
Detailed Criteria: thought leadership, intellectual property (IP), external research partnerships, sales and marketing, case studies                                                                                                                                                                                                                                                                                                                                                         |
**Cybersecurity Services**

ALM defines Cybersecurity Services as the body of professional services designed to help organizations manage the corporate, financial, legal, operational, regulatory, and reputational risks resulting from the deliberate and accidental cyber events which compromise their organization’s network-connected computer systems.

### Risk Matrix Definitions

<table>
<thead>
<tr>
<th>Risk Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy</td>
<td>Project-based management consulting services designed to enhance business growth opportunities</td>
</tr>
<tr>
<td>Operations</td>
<td>Project-based management consulting services focused on improving the functional capabilities and resources required to operationalize the business strategy</td>
</tr>
<tr>
<td>Advisory</td>
<td>Ongoing services provided by professionals who are licensed or certified in a specific functional discipline that may be regulated by a body of law or practiced according to industry-based technical standards</td>
</tr>
<tr>
<td>Technology</td>
<td>Services designed to enhance productivity and/or business performance through the utilization of enabling technologies for strategic and operational decision support, business process automation, digital risk management, and information technology (IT) enterprise and network security</td>
</tr>
<tr>
<td>Managed/Outsourced</td>
<td>Managed and outsourced services involve the provision of technology-enabled process management services by an external provider. Managed services differentiate from outsourcing in several ways. They are provided by highly skilled talent with deep domain expertise who are capable of making risk-based decisions on behalf of the client; contracts are structured on an outcomes-based pricing model rather than hourly billing; the relationship is long-term compared to outsourcing’s typical five- to seven-year contract; and they are typically deployed using cloud technologies.</td>
</tr>
</tbody>
</table>

### Risk Strategy

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reactive</td>
<td>Actions in response to a risk occurrence, e.g., mitigating damage from risk event, implementation of business continuity plans during a risk event, and root-cause analysis of risk events</td>
</tr>
<tr>
<td>Proactive</td>
<td>Actions that address perceived risks before they occur, e.g., identification and prioritization of risks, risk monitoring, and implementation of risk controls</td>
</tr>
<tr>
<td>Predictive</td>
<td>Actions that forecast future, potential risk occurrences, e.g., risk assessments, case studies/use cases/claims scenarios, risk scenario planning, and simulated war games</td>
</tr>
</tbody>
</table>
About ALM: ALM Intelligence Pacesetter Team

- **Liz DeVito**
  Lead Analyst
  ALM Pacesetter Research
  edevito@alm.com

- **Tomek Jankowski**
  Lead Analyst
  ALM Pacesetter Research
  tjankowski@alm.com

- **Patrick Fuller**
  Vice President
  ALM Intelligence
  pfuller@alm.com

- **Jeanne Graham**
  Research Lead
  ALM Pacesetter Research
  jgraham@alm.com

- **Jim Doyle**
  Strategic Account Executive
  ALM Pacesetter Research
  jdoyle@alm.com

- **Eliza Sawyer**
  Marketing Manager
  ALM Intelligence
  esawyer@alm.com
About ALM Intelligence
ALM Intelligence provides proprietary data, analysis, tools, and knowledge that empower our clients to succeed. The product suite and vast data repository arm professionals with the critical business information required to make the most impactful and informed decisions possible. The exhaustive data repository and product functionality enable professionals to combat competitive challenges head-on with the confidence to remain ahead of the field. The depth of ALM Intelligence’s expertise across the benefits, insurance, consulting, and legal industries provide a broad spectrum of actionable intelligence to facilitate & execute strategy. Please visit www.alm.com/intelligence for more information.

About ALM
ALM, an information and intelligence company, provides customers with critical news, data, analysis, marketing solutions and events to successfully manage the business of business. ALM serves a community of over 6 million business professionals seeking to discover, connect and compete in highly complex industries. Please visit www.alm.com for more information and visit www.alm.com/events/ to learn about our upcoming events. Please follow us on Twitter at @ALMMedia.
Usage Inquiry Guidelines
This ALM Intelligence Product has been made available to Authorized Users pursuant to your organization’s agreement to the ALM Media Customer Agreement or other applicable Licensing Agreement.

Unless authorized by ALM Media, Customer may not use the Product except as permitted by U.S. copyright law and the applicable Licensing Agreement.

For details and ALM Intelligence’s full Usage Inquiry Guidelines, please contact your Client Service Leader or e-mail ConsultingResearch@alm.com.

External Usage Permission
External Usage Permissions can be obtained...
- by contacting ALM Intelligence for each usage episode (refer to Usage Inquiry Guidelines herein)
- by acquisition and purchase of a “Limited External Usage License,” which provides for usage of Research contents in the marketplace

ALM Media Properties, LLC Contact:
James Doyle – Strategic Account Manager – ALM Intelligence – ALM Media Properties, LLC
150 East 42nd Street, Mezzanine Level, New York, NY 10017 USA
Tel: +1.212.457.9171 – e-mail: jdoyle@alm.com

EY Consulting Contact: Alexia O’Sullivan, Global Analyst Relations Lead
London – Tel: +44 (0) 20 7980 0533 – email: alexia.osullivan@uk.ey.com