ALM INTELLIGENCE
PACESETTER
RESEARCH

Cybersecurity

2022- 2023

Table of Contents

Related ALM Research & Tools

- ALM Intelligence: Analyst Reports
- BenefitsPro.com: COVID-19
- Consulting Magazine
- Credit Union Times: COVID-19
- GlobeSt.com: COVID-19
- Law.com: COVID-19
- Law.com: Diversity
- Property & Casualty 360
- Real Estate Forum
- ThinkAdvisor.com: COVID-19

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

ALM INTELLIGENCE
PACESETTER
RESEARCH

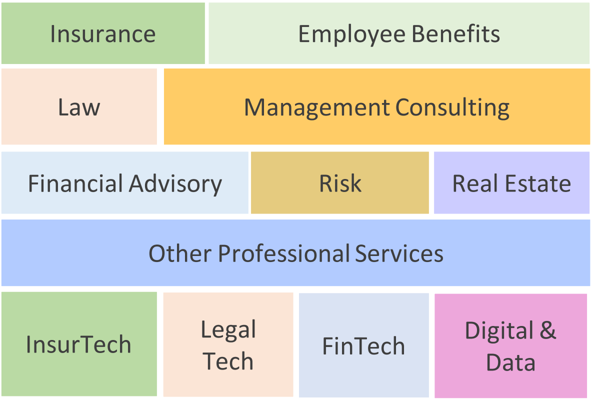
Introduction: About ALM Pacesetter Research

ALM Pacesetter Research (APR) is a market research initiative of ALM Intelligence with an inclusive perspective of the professional services landscape. Rather than traditional market research which focuses on one market segment, APR looks across a broader range that includes law, consulting, insurance, financial advisory, and other actors operating in the market defined by the research topic. ALM Intelligence started Pacesetter Research in 2020 to examine how more volatile demand dynamics are forcing market players to reevaluate their approach to ***innovation****,* ***risk****, market* ***convergence****, and ultimately,* ***opportunity****. The purpose of ALM Pacesetter Research is twofold:*

- *Deliver practical insights into the buying and selling of professional services in an increasingly converging marketplace*
- *Help buyers evaluate their sourcing options with objective assessments of providers' services and capabilities*

Pacesetter Advisory Council (PAC)

Market Leaders are selected by a panel of experts comprised of ALM editors, journalists, market intelligence analysts, and external professionals and academics who have experience working with professional services providers.



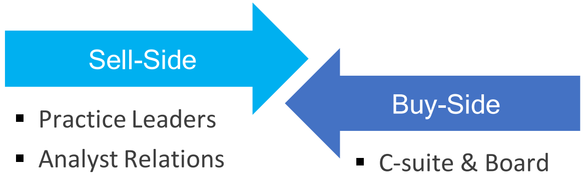
Research Methodology

APR analysts combine qualitative and quantitative research methods to profile Market Leaders in each market. These providers are evaluated and scored against five core criteria to determine Pacesetter status.

1. Business model
2. Value proposition
3. Service delivery
4. Client enablement
5. Brand eminence

Audience

APR provides independent and objective analyses 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:

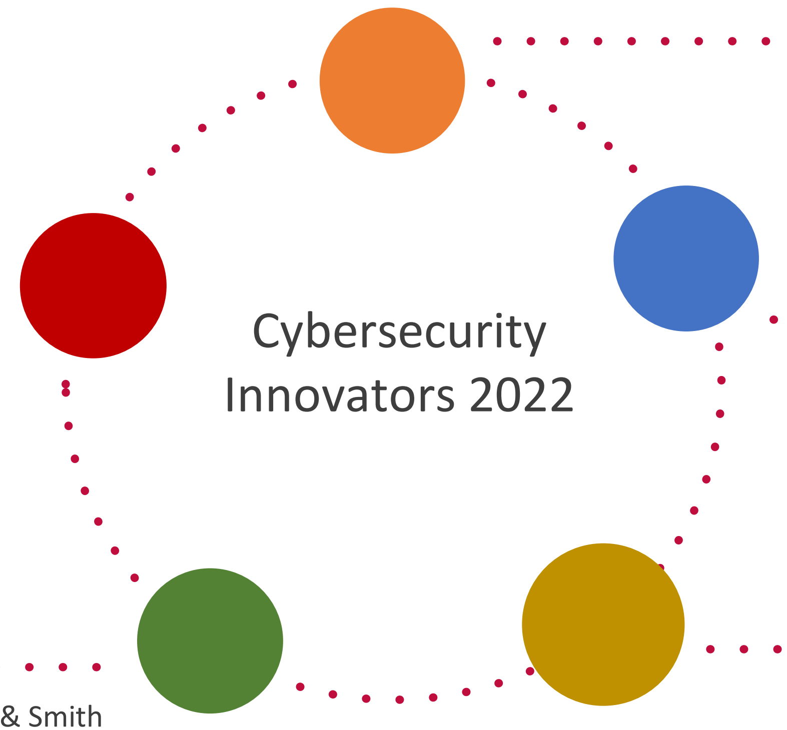
- Practice Leaders
- Analyst Relations
- Sales, Marketing & Public Relations
- Investor Relations
- Ecosystem Partners

Buy-Side:

- C-suite & Board
- Business Unit Leaders
- Procurement
- Supply Chain & Ecosystem Partners
- Shareholders

Introduction: Report Scope

After evaluating a wide field of providers, ALM Intelligence settled on 21 Innovators across five market segments for **Cybersecurity 2022***. Three providers were identified as ALM Pacesetters: KPMG, Nishimura & Asahi, and PwC (*)*



MANAGEMENT CONSULTING

- Alvarez & Marsal
- Booz Allen Hamilton
- Capco
- FTI Consulting
- Kroll
- PA Consulting

INSURANCE & BENEFITS

- AXA XL
- Berkshire Hathaway Insurance Group
- Vouch

MULTISERVICES

- Crowe
- Deloitte
- EY
- KPMG*
- PwC*

LEGAL

- Lewis Brisbois Bisgaard & Smith
- Nishimura & Asahi*
- Redgrave

TECHNOLOGY

- Accenture
- Capgemini
- Tata Consultancy Services (TCS)
- West Monroe Partners

Market Overview

ALM INTELLIGENCE
PACESETTER
RESEARCH

April 2022

Cybersecurity – technology, the sophistication of cyber criminals, what and who is targeted – continues to evolve rapidly, but the big shifts in cybersecurity services have more to do with catching up to what exactly "cyber" means for an organization in 2022. The most important of these realizations is that technology enables organizations and as such permeates everything they do. This, in turn, means that cybersecurity must do the same. A cybersecurity strategy must be more than an endpoint security solution; it must be embedded in operational procedures, employee training, management decisions and form a definitive thread in all external relationships including vendors, suppliers, logistics partners and customers.

Furthermore, cyber criminals in 2022 have moved from targeting data (usually for ransom) to disrupting operations – in effect, holding key organizational functions hostage. They have become more adept at probing an organization's entire value chain for weaknesses and entry points, then exploiting those weaknesses to threaten or inflict damage. This is reflected in recent surveys where CEOs voice fears of cyber threats less for any data loss or ransom payouts, and more as an instrument of business interruption.[1]

This means that cybersecurity in 2022 is more than a technology problem; it is also an operational, financial, human capital, value chain, product management, regulatory, and ultimately, a strategic problem. This implies, of course, that a well-crafted cybersecurity strategy can also be a differentiator and competitive advantage. Indeed, management consultants and multiservice providers have incorporated their cybersecurity offerings into their broader business transformation and long-term resiliency solutions.

The array of providers competing in the cybersecurity space remains massive, spanning mobile phone service providers to technology firms, endpoint solution software firms, security boutiques, retired IT specialists, as well as law firms, insurance companies (both carriers and brokers), management consulting providers and multiservice firms. What distinguishes Innovators from this large crowd of professional services providers is the recognition that any approach to cybersecurity requires a holistic solution incorporating the whole organization, as well as the client need for long-term engagement. On the farther end of the scale, this translates into managed services and Cyber-as-a-Service solutions, but other providers also recognize the importance of embedded solutions integrated with a client's broader risk management strategy.

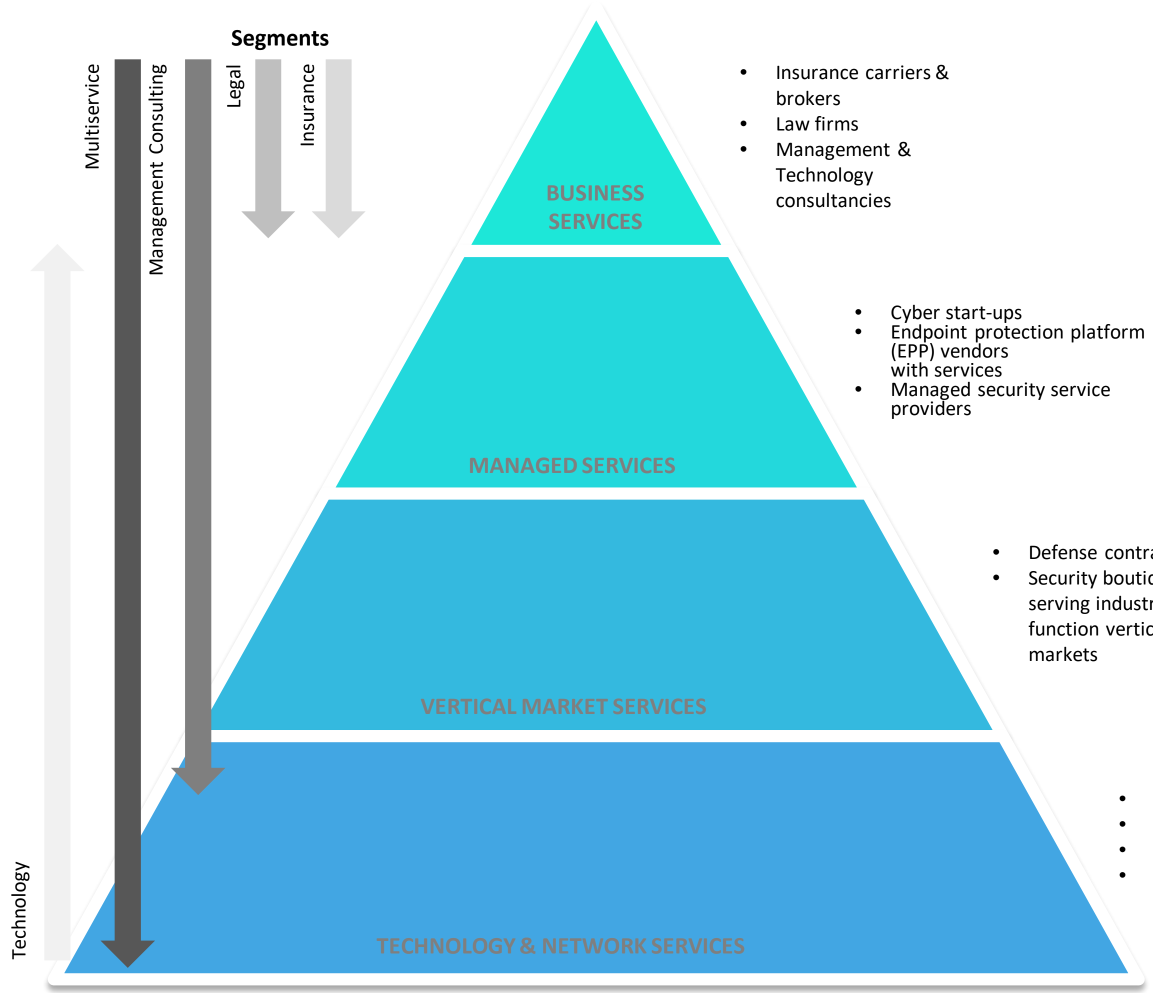
The Cybersecurity 2022 report explores how the Pacesetters in 2022 are those providers who have moved beyond stand-alone, "check-the-box" cybersecurity services to integrate cybersecurity into their approach to broader client business functions, so that their cybersecurity offering is as at home in risk management or supply chain management as technology. It is not that every provider offers a full, end-to-end cybersecurity suite of services, but that their solutions seamlessly integrate with client business functions. This includes law firms, which embed cybersecurity in their digital transformation advisory offering, as well as insurance carriers bundling broader business insurance offerings to include a comprehensive cybersecurity risk transfer offering for cost-challenged middle-tier clients. Cybersecurity is a fast-moving target, and innovators and Pacesetters alike recognize that clients do not need boxed software but long-term partners to manage cyber risk in the flow of their other business risks.

Tomek Jankowski
Director, ALM Intelligence Pacesetter Research
ALM Intelligence
T: +1.212.457.9175
Email: tjankowski@alm.com

[1] Steve Hallo. (2022, January 31). Fear & liability on a global scale: Allianz highlights 2022's top risks. PropertyCasualty360°. https://www.propertycasualty360.com/2022/01/31/fear-liability-on-a-global-scale-allianz-highlights-2022s-top-risks/?kw=Fear%20%26%20liability%20on%20a%20global%20scale:%20Allianz%20highlights%202022%27s%20top%20risks&utm_campaign=newsroomupdate&utm_content=20220131&utm_medium=enl&utm_source=email&utm_term=pc360

Cybersecurity 2022: Market Landscape

The cybersecurity services market is still dominated by technology and multiservice giants, but while the market outside of these players remains fragmented, advances in both technology and approaches to cybersecurity, as well as cost sensitivity, continue to open doors for innovators



Segments

Multiservice

Management Consulting

Legal

Insurance

Technology

BUSINESS SERVICES

- Insurance carriers & brokers
- Law firms
- Management & Technology consultancies

MANAGED SERVICES

- Cyber start-ups
- Endpoint protection platform (EPP) vendors with services
- Managed security service providers

VERTICAL MARKET SERVICES

- Defense contractors
- Security boutiques serving industry & function vertical markets

TECHNOLOGY & NETWORK SERVICES

- Cloud service providers
- IT generalists
- Network service providers
- Telecommunications service providers/ Communications Service Providers (CSPs)

Demand Drivers

The pandemic is still not over and its impact on driving digitalization and remote- or hybrid-work models is still being felt. Meanwhile, cybersecurity has moved from being seen as a technology problem to a core business challenge.

Key demand drivers include:

- The increasing sophistication and organization of bad cyber players, including the launch of ransomware-as-a-service offerings on the dark web
- The targeting of supply chains and third-party vendors/partners as the weak links in clients' cyber armor, particularly for under-resourced, mid-sized clients
- The shortening and disruption of global supply chains by geopolitical events
- The spread of new regulations with more stringent enforcement

Sources of Competitive Advantage

Constant change is the reality in cybersecurity, so rapidly adaptive solutions hold the most credibility.

Key sources of competitive advantage include:

- The ability to integrate solutions within the broader context of client cybersecurity strategy and needs
- Universal GRC models that link governance with risk and compliance frameworks
- Ability to help clients utilize AI and advanced technology for continuous monitoring
- Continuous engagement models (e.g., managed service, Cyber-as-a-Service, etc.)
- Advanced change management and human capital management capabilities to help clients address the human component of cybersecurity

ALM INTELLIGENCE
PACESETTER
RESEARCH

Cybersecurity 2022-2023: Stakeholder Access Map

Cybersecurity has been broadening in client organizations as a responsibility, spreading from the CTO to the CRO and GC/CLOs, to now include even unit-level managers while leading to the creation of the CISO – and all of this with the CEO's full attention, and carefully monitored by the board

Stakeholder Impact on Decision-making

- ■ Directly involved in scoping and purchasing services
- ▩ Key influencer; accountable/ responsible for executing strategy
- ░ Some influence on purchasing decision
- □ Not involved in purchasing decision

Segment relationship intensity

- ● Strong relationship
- ◑ Moderate relationship
- ○ Weak relationship
- □ No relationship

Stakeholders	Segments					Stakeholder roles and interests
	Insurance	Legal	Management Consulting	Multiservice	Technology	
■ CEO	○	◑	●	●	◑	The CEO has long been part of cybersecurity strategy development, but more recently has been called upon to manage and foster a wider array of skills
■ CRO	●	○	●	●	●	CROs are expected to be able to integrate and weave cybersecurity into a larger risk management framework, embedding cyber risk into all operations
■ CFO	○	○	●	●	●	The CFO has all the usual financial reporting duties but the trickiest part of their role in 2022 is to define and monitor the ROI of cyber investments
■ CISO	◑	◑	◑	●	●	CISOs in 2022 are less technical experts and more project managers, able to span production, supply chains, ecosystem partners and regulations
▩ CTO	□	□	●	●	●	The CTO is primarily responsible for the underlying technology of cybersecurity solutions (e.g., endpoint security solutions), while contributing to strategy
■ GC/CLO	○	●	◑	◑	○	GCs and CLOs were once only called upon for regulatory compliance and governance but now are expected to have a stronger voice in risk strategy
▩ CHRO	□	□	●	●	◑	CHROs have become important in the intersection of workforce management, cyber policy development, training, data management and talent recruiting
▩ Unit-level managers	□	□	◑	◑	◑	Unit-level managers are a key line of defense in cybersecurity, requiring enhanced leadership development for advanced culture management skills
░ External Stakeholders	□	○	◑	◑	○	Regulators, shareholders, ecosystem partners, industry associations and customers all play a role in influencing "cyber hygiene"
▩ Employees	□	□	○	◑	□	Employee behavior has come to be recognized as crucial for cybersecurity

Acronyms: CEO – chief executive officer; CFO – chief financial officer; CRO – chief risk officer; CHRO – chief HR officer; GC – general counsel; CLO – chief legal officer; CTO – chief technology officer, CISO - chief information security officer

Cybersecurity 2022: Demand Drivers

Trends

It would be legitimate for a section on trends in cybersecurity to lead with, "Same as last year, only now to the nth degree." What is different about cybersecurity in 2022 is the concern around serious business disruption. A year ago, cyber-criminals' primary target was data, but in 2022 it is processes and operations – particularly in third-party (e.g., supply chain) relationships. Trends include:

- Cyber incidents spiraled upwards in 2021, with social engineering the fastest growing threat, particularly targeting third-party relationships
- Cyber criminals are targeting under-resourced SMEs (small-to-medium-sized enterprises) and third-(and fourth) party value chain partners more
- Cybersecurity insurance coverage is under pressure
- The rapid spread of IoT also creates vulnerabilities
- Post-pandemic end-user customer expectations of more services delivered through internet-based products has increased cloud reliance, and therefore cyber risk
- Killware is a big concern, illustrated dramatically in January 2021 when a threat actor used remote access tools to increase the amount of sodium hydroxide in a public water treatment plant in Oldsmar, Florida to lethal levels – caught in time but showcasing the danger
- Cybercriminals are better organized than ever, including the development of ransomware-as-a-service (RaaS) third party services, opening cybercrime to anyone
- However, most cyber incidents still occur because of human error rather than technology failure, which is underscored by the rise of shadow IT
- One of the biggest areas of focus in cybersecurity are providing continuous training and upskilling
- Cybersecurity in 2022 is less a technology problem, and more a risk and operational problem: a business problem where risk-informed decision-making is the crux
- AI and continuous management of cybersecurity are filling some of the talent gaps while addressing the need to bake cybersecurity into all business functions
- With the sudden shift to remote and hybrid work models, demand for cyber talent has far outstripped supply, leading to a talent crunch across all industries
- Slashed T&E budgets since 2020 led to more funds being slated for risk management
- Most anticipate new data and cyber regulations
- Geopolitical instability is driving increased demand in software supply chain risk

Implications for Buyers

- Though utility varies by industry, the benefits of Public Private Partnerships are usually pegged (inaccurately) to cost, but the real value lies in risk and information sharing and should be explored as an option for a more effective long-term cybersecurity strategy
- Your organization's weakest links may not be internal but through your third-party relationships, particularly your supply chain, which necessitates greater scrutiny of third-party partners' cybersecurity regimes including contracts, fourth-party exposure, etc.
- There is a talent crunch for skilled cybersecurity specialists now, so hiring is less of an option to fill your organization's needs, requiring robust and continuous internal training programs for both cyber roles and cultural "human firewalling"
- Managed services and Cyber-as-a-Service are increasingly common and (depending on the provider) are looked on favorably by regulators

Convergence

As ransomware attack payouts skyrocket in 2022, convergence is happening at an accelerated rate in cybersecurity:

Incident response: This was the primary entry point for many providers in the cybersecurity space, driven by the skyrocketing number of data breaches and the spread and increasing sophistication of ransomware. Incident response is a whole package of services in 2022, however, and different providers have specialized – in part because some services are protected by licensing or regulations (e.g., legal or insurance). However, some of the approaches to these services (and who provides them) derives more from tradition than regulatory sanction, providing a ripe opportunity for disruption. Multiservice and management consulting crisis management services, for instance, are being adapted to cyber incident response demand in ways that could unpack much of what law firms do for insurance providers in breach coaching.

Security-as-a-service: Few organizations can keep up with the hypersonic rate of evolution in cyber crimes, opening the door for providers able to provide any number of continuous engagement "security as a service" offerings. Technology providers got the ball rolling but multiservice providers have stepped into the breach to the extent that these now comprise a significant portion of their cybersecurity revenues. A key value both global technology and multiservice providers bring is their "follow-the-sun" global capabilities (meaning, presence and integrated technology platforms) that allow truly global, truly 24/7 monitoring services. Management consulting firms have offered more targeted offerings, being wary of the investments required for managed service-type offerings. They prefer to build their consulting offerings in cyber around complementary relationships with technology providers. However, that cooperation is important and bolsters their attractiveness to clients as an alternative to multiservice "one-stop cyber shops."

Regulations: The threat of a new tide of regulations addressing cybersecurity has nearly all providers seeking to create client-facing information and alert-based solutions to inform client strategies.

Data privacy: Most law firm cybersecurity practices are bifurcated between data privacy and incident response services. It has taken some time for professional services to connect these two demand areas, but multiservice and management consulting providers are putting a lot of resources behind both the compliance and incident response side of data privacy, and baking it into their end-to-end cybersecurity solutions, while technology providers are attempting to automate the compliance side in their client-facing platforms.

Risk transfer: Insurance providers have no competition for insurance products (as mandated by regulations), but multiservice and management consulting providers have been embedding cybersecurity within larger risk management frameworks, and within that context they advise clients on risk transfer strategy. This includes helping them develop effective cyber risk management practices (in competition with innovative efforts by leading insurers to develop upstream advisory services) as well as with cost management in risk mitigation and developing an optimal vendor (i.e., insurer) selection process. In this way multiservice providers and consultants capture as much of that risk transfer part of the puzzle as they can,. Short of actually selling insurance products themselves and insert themselves into that relationship between a client and their broker or agent.

Implications for Providers

- Providers that can demonstrate to their clients their own effective internal cybersecurity strategy will gain the most credibility with clients
- With a focus on client outcomes, innovative providers should recognize the need for a holistic approach to cybersecurity by building the internal "muscle memory" of being able to manage external market ecosystem relationships (e.g., partnerships, alliances, etc.) to both extend their own capabilities and provide a seamless an experience for clients
- One of the areas victims (and potential victims) in cybersecurity are most vulnerable is in their isolation; providers should seek to form information-sharing communities in industries, and where possible, utilizing public sector data and resources to help collect data on events as well as better understand the effectiveness of policies
- At a time when cybersecurity costs are skyrocketing, providers should be able to utilize technology and ecosystem relationships to keep costs manageable
- Insurance panels have become popular but may be of limited efficacy in cybersecurity for some service providers as they tend to be tied exclusively to remediation projects, and some clients have come to view providers on insurance panels as "ambulance chasers" – undermining efforts at building longer-term relationships with clients

ALM Intelligence Pacesetters

What makes a Pacesetter in COVID-era cybersecurity strategy?

Upstream: Professional services providers broadly recognize that an effective cybersecurity strategy cannot rely on barriers and remediation plans. Servicing client cybersecurity needs in 2022 requires proactively understanding the client cybersecurity risk profile – and managing that profile. This has prompted innovators to move their service focus upstream to help clients maintain solid "cyber hygiene." This is an area where management consulting firms, multiservice providers, and insurers in particular have reconfigured their approach to help clients understand the day-to-day, hour-to-hour nuts and bolts of an effective cybersecurity management strategy to take the onus off defensive controls and downstream remediation/crisis management plans. An ounce of prevention….

AI/Advanced technology & continuous management: As cybersecurity (as a service) has moved from stagnant software barriers and controls to more proactive, continuous management, the recognition that humans cannot possibly monitor and manage the massive flow of data, processes and events that flow through any organization on a daily basis has given rise to the deployment of advanced technology AI, machine learning and blockchain. Technology firms, consulting and multiservice providers have been the first to utilize these technology tools, but innovators among insurers are also learning to use them to keep up with on-going cycles of technical innovation, as well as the highly organized and increasingly sophisticated cybercriminal community that cooperates far more readily than cyber victims do. AI can adapt to an ever-changing threat environment, and innovative providers have incorporated it into a long-term, managed services or Cyber-as-a-Service offering.

Integrated strategy: Another key element to cybersecurity services in 2022 is the recognition that cybersecurity is also a business problem. This translates into the need to address other business components to cyber risk, including operations, human behavior, third-party relationships, contracts, communication channels, and marketing & sales. Innovative providers have broadened their approach to cybersecurity to help clients create a holistic cybersecurity profile and actively manage that profile. Multiservice and management consulting providers have led the way with seamless, integrated offerings spanning their practice domains (and sometimes anchored in their M&A, restructuring or digital transformation practices), but insurance and some legal innovators have also taken up the challenge with expanded advisory offerings that include employee training and active strategy development support.

Skills: All organizations, both providers and clients, are struggling to acquire and keep skilled talent in cyber risk management and strategy development. As one professional put it, the unemployment rate in cyber talent markets is currently zero. This is forcing organizations to become creative. Innovators recognize that cyber talent cannot be simply acquired or recruited, but must also be developed and fostered over time. This meshes with the recognition that the human dimension of cybersecurity requires that all employees must acquire and develop over time a certain level of cyber literacy and awareness. Innovators are creating continuous education and training programs, while working with institutions to build out the cyber management portion of university programs

Cybersecurity 2022

Market Segment	Provider
Multiservice	KPMG
Legal	Nishimura & Asahi
Multiservice	PwC

Methodology Notes

The ALM Pacesetter Research methodology evaluates Innovators 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% or above qualify as an ALM Pacesetter.

In some instances the scoring may be weighted due to their importance in achieving competitive differentiation in this report's topic. For details, weighting in this particular report are addressed in the Methodology section.

See Appendix for detailed definitions of the five core criteria

The ALM Intelligence Pacesetters

ALM INTELLIGENCE PACESETTER

CYBERSECURITY 2022–2023

ALM INTELLIGENCE PACESETTER RESEARCH

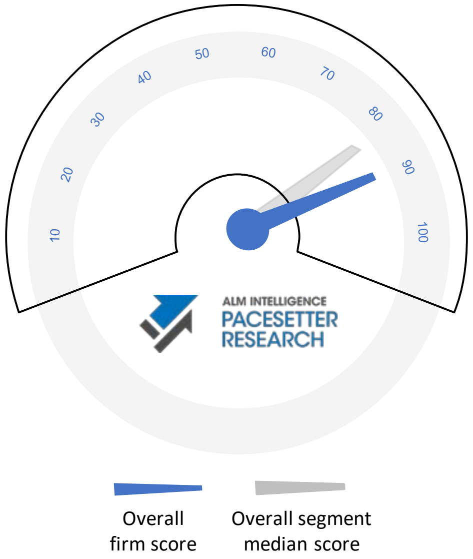
Cybersecurity 2022: Categories

The five highest scorers in each category reflect both where providers focus their investments and service focus, as well as the degree to which a full, end-to-end, integrated and business-focused offering is having the most impact on cybersecurity

Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence
Accenture	AXA XL	KPMG	EY	Accenture
Deloitte	KPMG	Kroll	KPMG	Deloitte
EY	Nishimura & Asahi	Lewis Brisbois	Nishimura & Asahi	EY
PwC	PwC	Nishimura & Asahi	PwC	KPMG
Vouch	Redgrave	PwC	Redgrave	PwC
(Alphabetical order)	(Alphabetical order)	(Alphabetical order)	(Alphabetical order)	(Alphabetical order)

KPMG

ALM Intelligence Pacesetter Overall Score: Cybersecurity



Business Model	◕
Value Proposition	◕
Service Delivery	◕
Client Enablement	◕
Brand Eminence	◕

Impact Scale: ○ None ◑ Moderate ◕ Significant ● Very High

> *KPMG's "golden thread" approach to cybersecurity brings together the business, technology and cyber elements of a comprehensive cybersecurity strategy that focus on enterprise risk and longer-term resiliency for clients.*

Profile:

A global multiservice company and one of the Big Four, KPMG (headquartered in the Netherlands) offers services across four basic practice areas: Audit Assurance, Tax & Legal, Advisory, and Private Enterprise. KPMG has focused in recent years on business transformation, with a strong emphasis on the digital component. KPMG's approach to technology-enabled transformation, dubbed the KPMG Powered Enterprise, is about organizations not undergoing a single transformation event but internalizing the ability to drive continuous change, using advanced technologies, including strong elements of agile and resilient functions and processes.

For KPMG, cybersecurity is a "golden thread" that runs through every client function, and as such enables growth, requiring a full, comprehensive approach that fuses cybersecurity into broader business and technology offerings. The main thrust for KPMG is what it calls the "Trusted Imperative." KPMG believes that when organizations earn and deserve the trust of all their stakeholders, they create a solid platform for responsible growth, confident decision-making, bolder innovation and sustainable advances in performance and efficiency. Cybersecurity is at the center of the Trusted Imperative. KPMG's cybersecurity offering combines the use of technology, business, and human capital resources across an integrated, cross-competency solution. Accelerated by COVID-19, KPMG's delivery model involves hybrid (remote/on-site) working models, virtual overlays (utilizing global specialist resources), digital service delivery & automation, and effective use of near-and off-shore resources. KPMG works closely with ecosystem partners for solutions, utilizing co-sourcing models for specialist skills and agile surge capacity. Clients have been increasingly willing to utilize managed services and Security as a Service models with risk transfer integrated into the client control environment. KPMG also makes use of its industry centers of excellence, Insights and Ignition centers as well as KPMG Lighthouse, the firm's CoE for advanced analytics.

Cybersecurity Service Focus

■ Data, technology tools & solutions	■ Accounting & auditing
■ Consulting services	■ Forensic investigations
■ Function-focused advisory services	■ Interim, managed & outsourcing services
■ Legal services	■ Stakeholder Management
■ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- ■ Manage/Monitor
- ■ Anticipate
- ■ Remediate

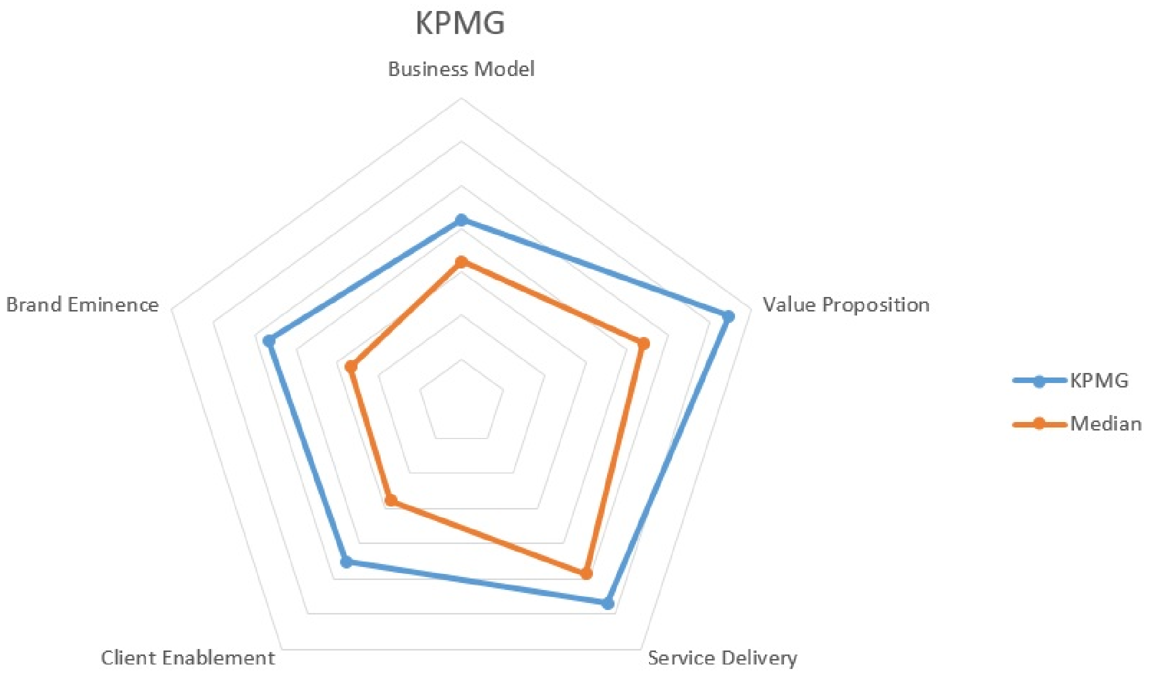
■ Services offered
□ Services not offered

Cybersecurity: KPMG

KPMG

How KPMG is moving the needle

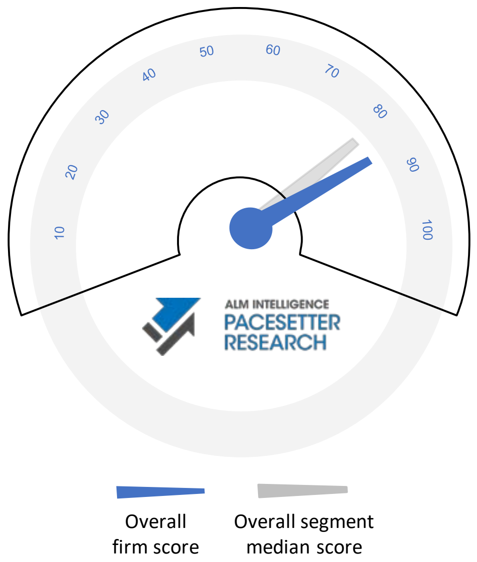
Pacesetter Criteria	Qualitative Assessment
Value Proposition	KPMG's cybersecurity offering is embedded across its Audit, Tax and Advisory solution areas, reflecting the firm's multidisciplinary approach and view of cybersecurity as ultimately a growth enabler for clients
Service Delivery	KPMG's responsiveness to rapidly evolving client needs have led the firm to address key client needs through a multidisciplinary approach, willingness to cosource solutions with external partners, offering managed and security-as-a-service solutions, flexibility in helping clients adapt complex solutions, and its focus in cybersecurity to longer-term client business resiliency goals



ALM INTELLIGENCE PACESETTER
CYBERSECURITY 2022–2023

Nishimura & Asahi

ALM Intelligence Pacesetter Overall Score: Cybersecurity



Business Model	◑
Value Proposition	◕
Service Delivery	◕
Client Enablement	◕
Brand Eminence	◕

Impact Scale: ○ None ◑ Moderate ◕ Significant ● Very High

> *Nishimura & Asahi's unique (in Japanese markets) pairing of risk, compliance and digital transformation strategy with an embedded cybersecurity component make this law firm a key partner for clients struggling to comply with Japans' digital push.*

Profile:

One of Japan's Big Four domestic law firms, Nishimura & Asahi is a full-service law firm with particular strengths in M&A and financial restructuring. The firm has a global presence, following Japanese corporate clients into the markets they serve. The firm has also invested in advanced technologies in recent years to support its legal practices. The firm has a demonstrated competency in all things digital transformation, ranging from drones and IoT to digital strategy and digital health.

In response to the Japanese government's series of laws enacted in 2021 designed to hasten the adoption of digital technologies among both local governments and businesses across Japan, Nishimura & Asahi created its digital transformation group designed to support practices (including industry practices) to manage legislative, regulatory and commercial rules and standards. This practice is not just a compliance center but helps clients formulate a digital transformation strategy, including providing some non-legal support. The firm's Digital Operations group focuses on broader social and economic digital challenges, such as autonomous vehicles, digital strategy, smart & intelligent cities, and IoT. Its Digital Innovation group in turn focuses on operational and business efficiency, including AI & robotics, blockchain, drones, digital health, and digital trust & cybersecurity. Cybersecurity is seen by Nishimura & Asahi as a regulatory compliance problem but one that is fused into its digital transformation and innovation offerings.

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	■ Forensic investigations
■ Function-focused advisory services	□ Interim, managed & outsourcing services
■ Legal services	□ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- □ Manage/Monitor
- □ Anticipate
- ■ Remediate

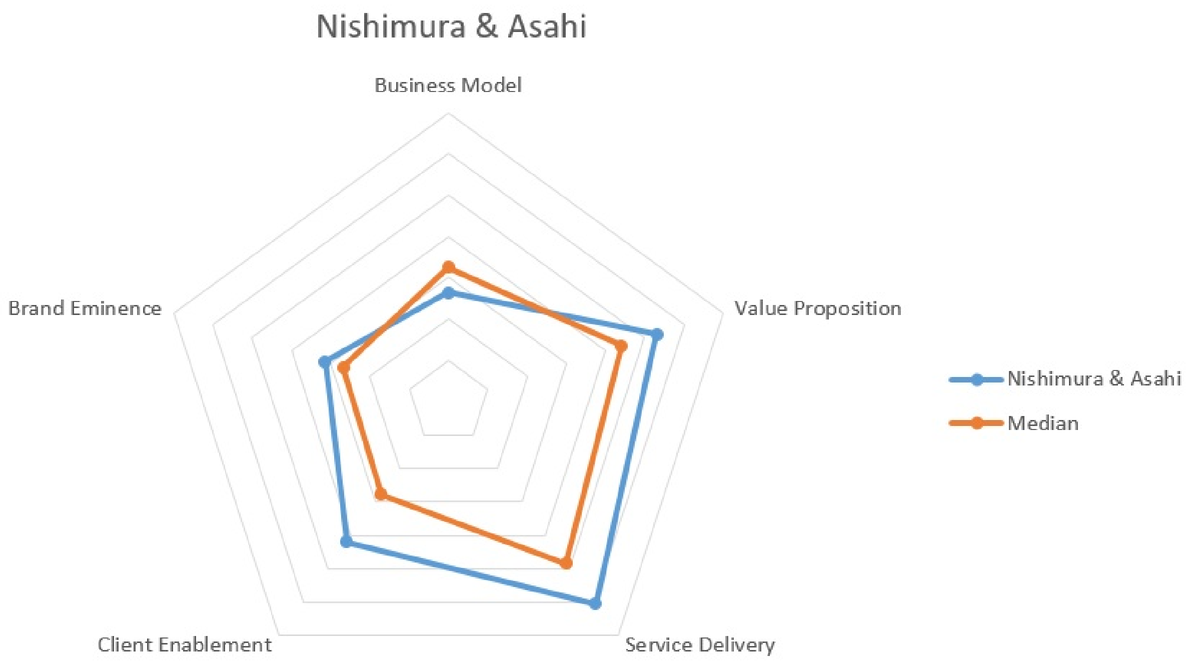
■ Services offered
□ Services not offered

Cybersecurity: Nishimura & Asahi

NISHIMURA & ASAHI

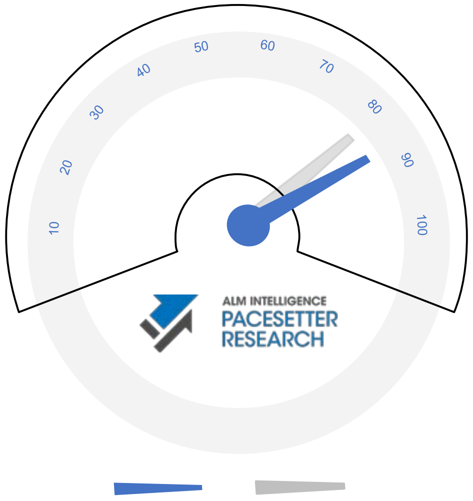
How Nishimura & Asahi is moving the needle

Pacesetter Criteria	Qualitative Assessment
Value Proposition	Nishimura & Asahi's key value proposition lies in its multidisciplinary and cross-sectional approach to cybersecurity, recognizing that client risk and compliance needs in cybersecurity are interwoven with operational and technology challenges that are inseparable from the typical legal offering when formulating a cybersecurity and cyber risk strategy
Service Delivery	In creating its digital transformation unit, the firm recruited non-lawyer specialists across a wide range of newly emerging technologies (e.g., drones, IoT, driverless vehicles, etc.) to be able to directly address client risk and cybersecurity concerns



PwC

ALM Intelligence Pacesetter Overall Score: Cybersecurity



Overall firm score

Overall segment median score

Business Model	◕
Value Proposition	◕
Service Delivery	◕
Client Enablement	◕
Brand Eminence	◕

Impact Scale: ○ None ◑ Moderate ◕ Significant ● Very High

> *“PwC’s journey with its New Equation framework, which focuses on building trust and achieving client outcomes, feeds into its approach to cybersecurity where the firm positions cybersecurity as a path to resilience, enablement and trust for clients.*

Profile:

PwC has undergone a significant transformation in the past year with the introduction of The New Equation initiative, a restatement of the firm’s commitment to a relentless focus on client challenges. The New Equation commits PwC to building trust in many forms and delivering highly sustainable outcomes, which in turn generates more client value. With The New Equation, PwC positions its people and technology as client enablers through services organized into two basic service lines: Trust Solutions, which include traditional Assurance, and Tax & Legal, and Consulting Solutions, where most of the firm’s cybersecurity services reside.

Cybersecurity is a cross-domain competency for PwC, but service delivery begins with the Cybersecurity, Risk and Regulation practice in Consulting Solutions. Cybersecurity capabilities, alongside Digital, are embedded in PwC’s global Risk and Regulatory, Transformation, Sustainability/ESG, and Deals/M&A “platforms.” PwC’s cyber consulting strategy is focused on helping clients build trust, resilience and sustained outcomes, with IP & Intelligence-led services powered by technology and people. This informs all investments and R&D priorities. Cybersecurity engagements for PwC typically take the form of cyber strategy, and GRC integration, front office transformation, security engineering, metrics and reporting, identity management, threat intelligence-led cyber defense, cloud security and zero trust engineering, and incident response. One of the central themes for PwC cybersecurity service strategy is simplifying cybersecurity strategy and operations, with the underlying tenet being that cybersecurity is as much a governance, organizational strategy and operational challenge as a technology one. PwC also runs its annual Global Digital Trust Insights Survey as well as a Cybersecurity Forum, while maintaining its Digital Cyber Academy for employee (and future client) skill development. PwC also builds relationships with key technology and academic partners for advanced and distinct business solutions.

Cybersecurity Service Focus

■ Data, technology tools & solutions	■ Accounting & auditing
■ Consulting services	■ Forensic investigations
■ Function-focused advisory services	■ Interim, managed & outsourcing services
■ Legal services	■ Stakeholder Management
■ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- ■ Manage/Monitor
- ■ Anticipate
- ■ Remediate

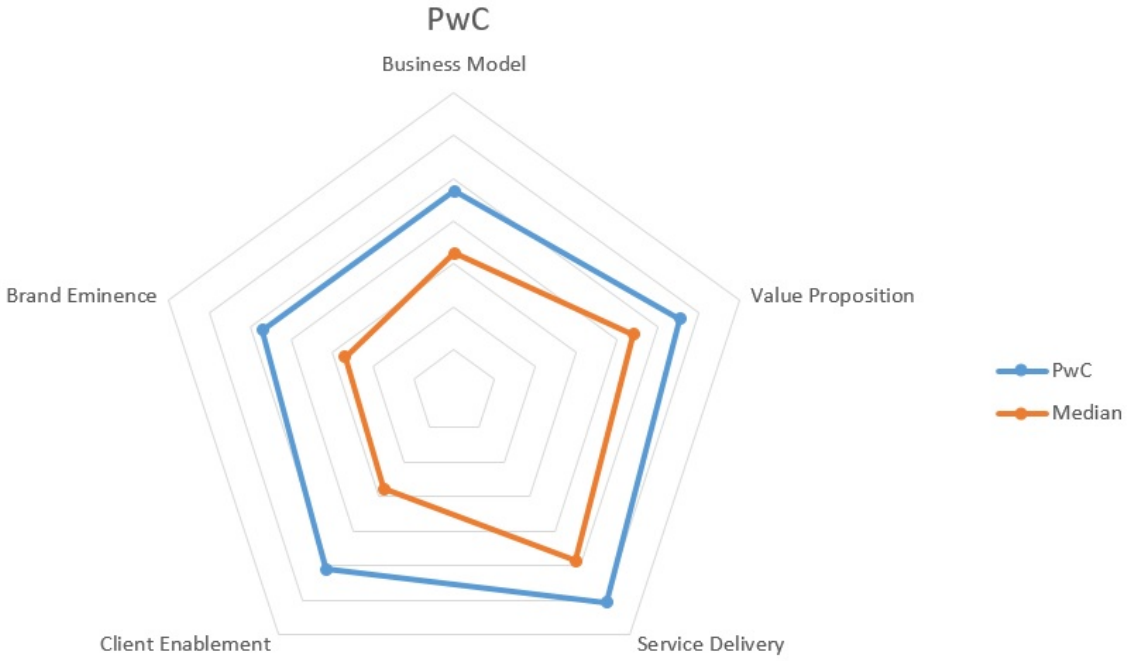
■ Services offered
□ Services not offered

Cybersecurity: PwC

pwc

How PwC is moving the needle

Pacesetter Criteria	Qualitative Assessment
Value Proposition	PwC's approach to cybersecurity is risk-led, organized through its BXT (business-experience-technology) framework, and brings together innovation, investment in IP, delivery accelerators, and the use of external partnerships and alliances to deliver an integrated, cross-platform and intelligence-led approach that, by demonstrating trustworthiness, seeks to help clients instill the same in their own cybersecurity strategies
Service Delivery	While PwC has been investing in its cybersecurity IP for years, there is powerful value in its internal-facing digital upskilling and training programs, best illustrated by its global cyber academy which utilizes internal and external vendor-created content to ensure PwC employees are skilled in the latest digital and cyber trends



The ALM Intelligence Innovators

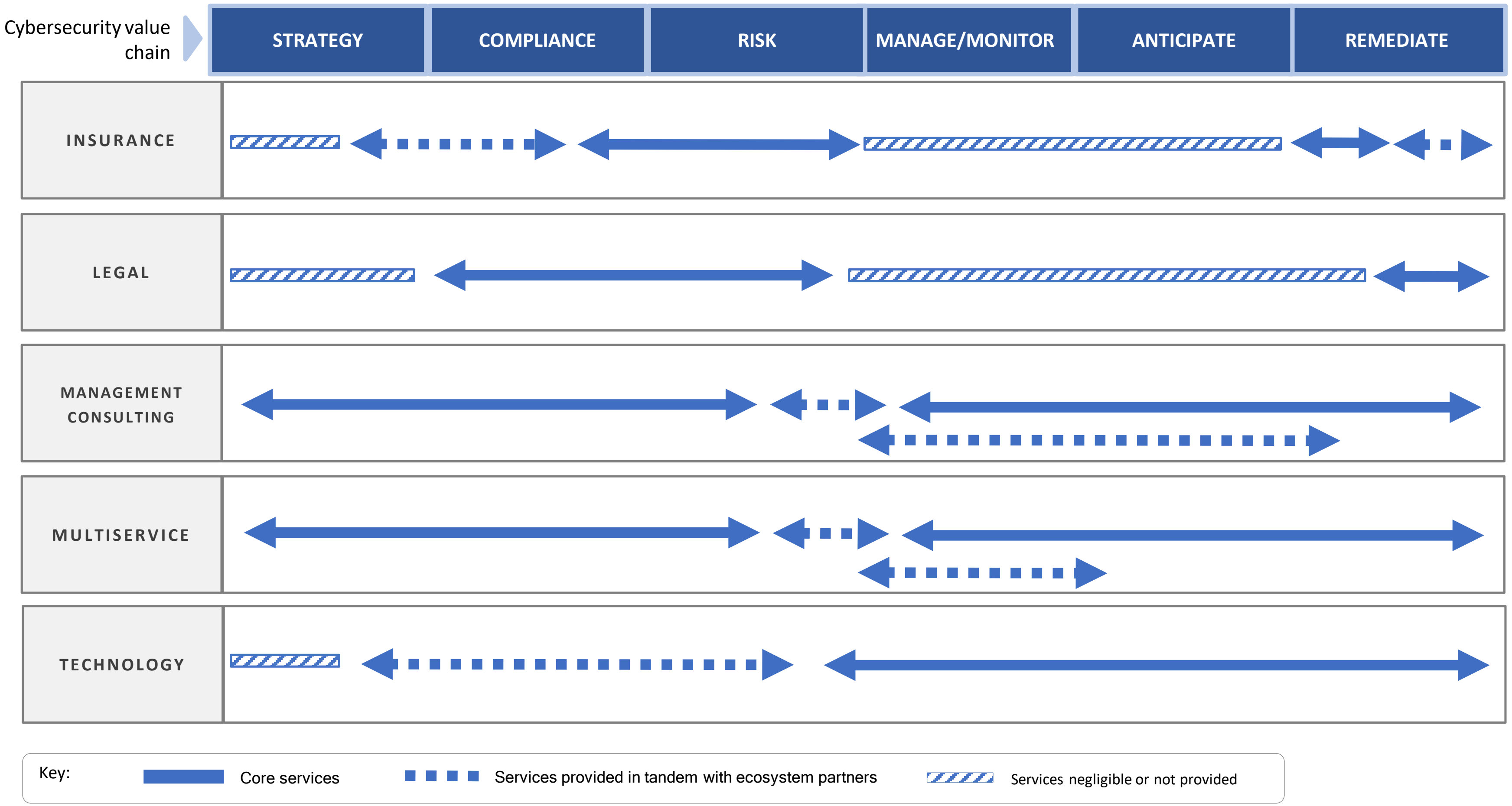
ALM INTELLIGENCE
INNOVATOR
CYBERSECURITY 2022 – 2023

Cybersecurity 2022: Market Segments Map

Cybersecurity has moved from being a linear technology and compliance defensive exercise to a pan-organization way of doing business, and while the giant technology and multiservice providers continue to dominate, innovators across the spectrum are changing how they engage clients

Notes on market convergence:

- Innovative **Insurance** providers have been building out their cyber advisory business lines in recent years, paying more attention to upstream “cyber hygiene,” but some also have been including regulatory compliance information and an advisory function in their cyber offerings, while encouraging cyber claims managers to take on more project management responsibility
- **Law firms** have moved the least, with some tying cybersecurity to digital offerings or data
- **Management consulting** firms and **multiservice** providers have broadened their offering the most, some even including legal services; their only constraint is insurance products
- **Technology** providers are all about capacity and managed services



Cybersecurity value chain: STRATEGY | COMPLIANCE | RISK | MANAGE/MONITOR | ANTICIPATE | REMEDIATE

INSURANCE

LEGAL

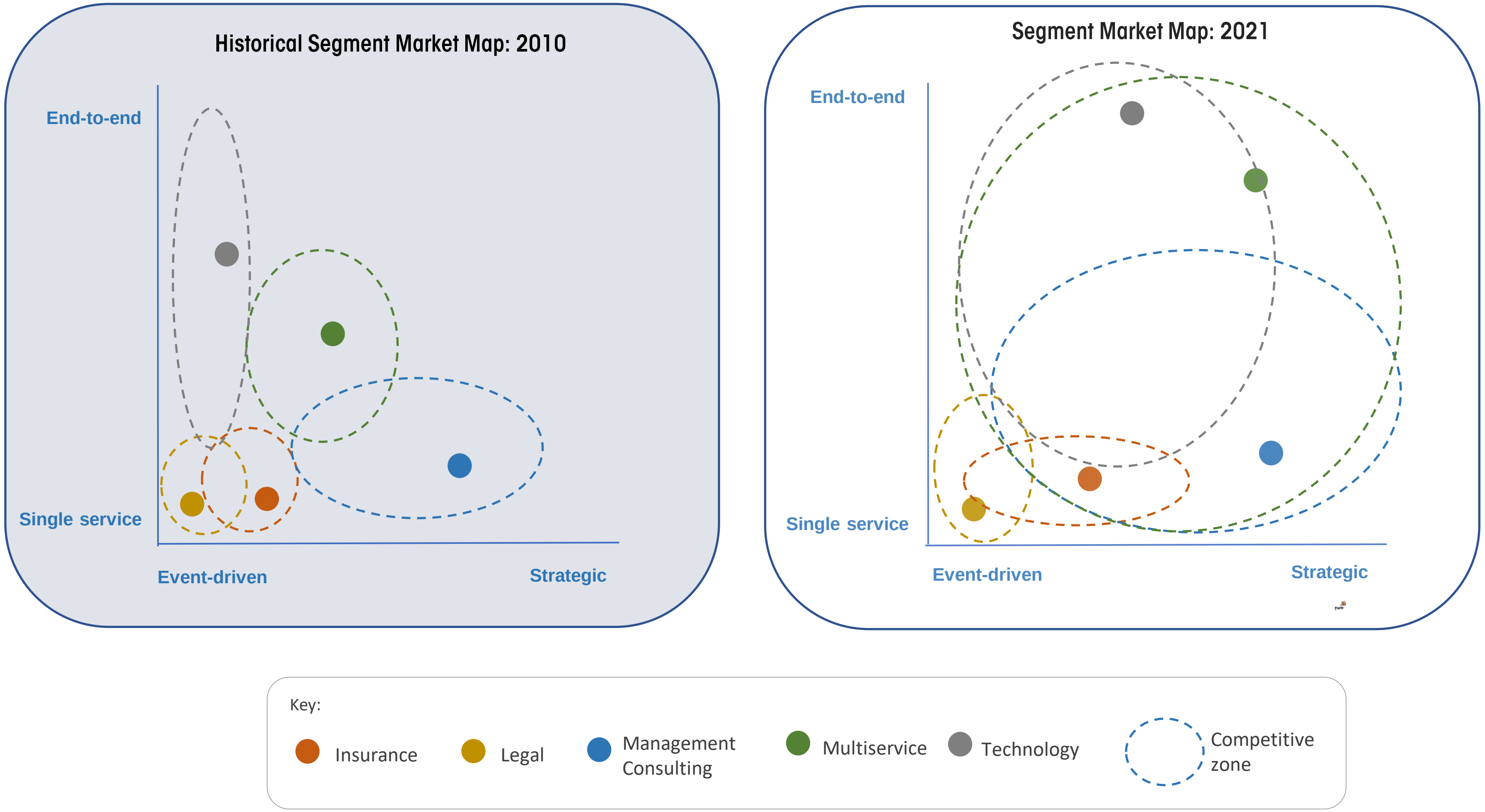
MANAGEMENT CONSULTING

MULTISERVICE

TECHNOLOGY

Key: ▬ Core services ▪ ▪ ▪ ▪ Services provided in tandem with ecosystem partners ▨ Services negligible or not provided

Cybersecurity 2022: Competitive Landscape



Notes on the competitive landscape:

- **Insurance** providers focus overwhelmingly on risk mitigation, but innovators have begun to connect that risk with upstream "cyber hygiene" improvement in clients, as well as linking cyber risk with broader data and digital risk management
- **Law firms** have been more incremental with their innovation, focusing on risk strategy advisory services and client-facing data dashboards, while honing in on compliance and remediation
- **Management consulting** firms and **multiservice** providers have embraced cybersecurity as a part of business transformation and focus on the notion of digital trust: (the idea that well-organized and effective cybersecurity strategies lead stakeholders to trust an organization), while also offering managed solutions to help clients address capability and capacity gaps
- **Technology** providers focus on cost and bundling to offer end-to-end solutions to underserved markets, but with out-of-the-box solutions and managed services

The Insurance Segment Role in the Ecosystem

The insurance world has been struggling with cybersecurity. Every year over the past decade, accelerated dramatically by the pandemic, has seen higher numbers of cybersecurity insurance claims accompanied by skyrocketing payouts. Insurers have responded by focusing on the products: on limiting coverage, raising rates and changing underwriting standards. Aggregations have been imposed, while policies are scrutinized to weed out “silent cyber” coverage.

Innovators have recognized the importance of helping clients understand the magnitude of the cyber challenge they face, and fitting them with the best possible coverage. Innovator responses have included the development of upstream cyber preparedness advisory services as well as product focus on smaller-scale clients. Though scant for the moment, some innovators have called for greater collaboration and information sharing between insurers, industry associations, the insured, governments and regulators.

One area that remains under-addressed in insurance is the claims management process, which the insurance industry has largely outsourced to law firms in the form of “breach coach” incident response services. This has led to a certain amount of cost creep as law firms typically treat these services like any other legal offering, without distinguishing between what amounts to advisory services versus legal advice. A further dimension to this problem, as noted in a recent study[1], is that using law firm “hotlines” for incident response services creates an intermediary between insurer and insured, one who brings their own peculiar lens to incidents: “…the claims process is controlled by lawyers who prioritise [sic] preventing litigation risk, which often means investigative findings are not written down or shared. Over time, this impedes the ability of insurers and policyholders to extract lessons from cyber incidents, which in turn undermines the evolutionary promise of cyber insurance.”[2] Insurers can better manage long-term cost creep by assuming more of the role of project management in claims in incident response.

Characteristics:

- Innovators recognize that cybersecurity permeates insured operations and structure their products in an integrated fashion to help clients (of all sizes) incorporate the most effective risk mitigation strategies for cybersecurity
- Some innovators have taken full charge of helping their clients proactively develop effective cybersecurity strategies

Cybersecurity Innovators in Insurance & Benefits
AXA XL
Berkshire Hathaway Insurance Group
Vouch

Procurement Priorities

- As insurers seek to more clearly define coverage (risk) and eliminate silent cyber, it is important that insureds go against the traditional grain (whereby insureds tend to prefer insurers that ask the fewest questions) and spend time – possibly with external advisors – to understand in detail their own cyber risk (especially third and fourth-party risk) to optimize their risk mitigation
- An important element absent from cyber risk mitigation is information; consider creating information-sharing networks in/with industry associations, business communities, and with the public sector
- Innovators in the insurance world have been developing employee training programs and culture-defense training; make use of these resources

* ALM Pacesetter; see profile in Pacesetter section

[1] Daniel Schwarcz, Josephine Wolff, Daniel Woods. (2022 January 5). Do the Legal Rules Governing the Confidentiality of Cyber Incident Response Undermine Cybersecurity? (Blog post). Lawfare. Retrieved from: https://www.lawfareblog.com/do-legal-rules-governing-confidentiality-cyber-incident-response-undermine-cybersecurity

[2] Daniel Woods. (2022 February 1). The Evolutionary Promise of Cyber Insurance (Blog post). The FinReg Blog. Retrieved from: https://sites.law.duke.edu/thefinregblog/2022/02/01/the-evolutionary-promise-of-cyber-insurance%EF%BF%BC/

Employee Cybersecurity SWOT: Insurance

Internal Factors

STRENGTHS

- The insurance segment is the one segment examined in this report that has an exclusive role in cybersecurity
- Insurers are competitive with law firms in accumulating knowledge of cyber regulations in regional jurisdictions, and some have been productizing that knowledge
- Though cyber insurance is relatively new, by now three decades of data has been compiled and insurance carriers own the bulk of that data
- Pricing models provide insurers with a detailed and complex understanding of the impact of cyber events, and as the runway lengthens, that understanding includes the impact over time

WEAKNESSES

- Outside a handful of innovators, insurers' focus on product (versus client engagement, cyber hygiene, etc.) has led to a more passive relationship between insurers and clients
- Traditional approaches to P&C claims events have translated into insurers handing off important portions of cybersecurity product and service delivery (e.g., incident response) to law firms and other parties, leading to cost creep over time and posing the long-term danger that insurers may be relegated to invisible, behind-the-scenes product providers in cyber remediation services
- Reliance on external partners for cyber expertise weakens brand, cedes relationship initiative to external partners

Insurance providers have a carefully ringfenced slice of cybersecurity spend, but further opportunities await in data, cyber hygiene advisory and integrating cyber risk with operational risk

OPPORTUNITIES

- Insurers are uniquely placed to build information coalitions of clients, insurers, brokers, technology firms and public sector players for data-sharing to better understand cyber events as well as the impact of good cybersecurity planning and strategy
- While there is a certain amount of panic in cybersecurity insurance markets, some view the current pricing and coverage challenges as a market shakeout of inexperienced insurers who treated cybersecurity as just another P&C line, providing an opportunity for those willing to commit and invest in the necessary expertise and resources to specialize

THREATS

External Factors

- As cybersecurity strategy moves towards an integrated service approach, other providers – particularly management consulting and multiservice – offer clients a comprehensive, bundled offering that, while not able to offer insurance products, increasingly incorporates risk transfer advisory services coupled with regulatory compliance and risk management services
- While growing slower than other fintech areas, insurtech is developing and cybersecurity is a prime area of focus

AXA XL

AXA XL	Primary Practice	Risk Consulting

Aon is a firm that has been undergoing profound change in recent years, both through its own internal realignment efforts through its Aon United Blueprint strategy and through its failed merger with Willis Towers Watson (which entailed extensive divestitures to persuade skeptical regulators). In the wake of all this change, Aon is refocusing itself to address the following client risk-related concerns: navigating new forms of volatility, building a resilient workforce, rethinking access to capital, and addressing the underserved. These are achieved through advanced data sourcing and analytics, consulting, and seeking innovative solutions to client challenges via the firm's Innovation at Scale strategy. Technology plays an important role for Aon, for instance in the form of its Aon Business Services platform (as part of its United Blueprint strategy), which supports back- and middle-office services across the firm, and Aon's People Analytics service, which provides business intelligence capabilities integrating HR, finance and other operational data to compare human capital strategies with operating costs.

For Aon, employee well-being is firmly embedded in the benefits experience, which for Aon translates into crafting the optimal benefits package for clients. The firm's Five Pillars of Benefits Strategy covers the employer view, the employee view, the competitive view, the financial view, and the environmental landscape view. Aon's approach to benefits is end-to-end and spans compliance, budgeting and ROI, the employee experience, benchmarking, vendor selection, incentivization, and health & wellness program design. Consulting services span health and benefits consulting services solutions. Aon also developed its Well One app, which uses data analytics to help clients (both individual employees and management) track physical, emotional, social and financial well-being across the client organization, helping them continuously reassess their employee and team well-being strategy. With the onset of the pandemic, Aon began producing survey-driven thought leadership targeting employee mental health as well.

Impact Scale:
- ● Very High
- ◕ High
- ◑ Moderate
- ◔ Low
- ○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence	🟥	🟨	⬜	🟩
◕	◕	◕	◑	◑				◑

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	□ Forensic investigations
□ Function-focused advisory services	□ Interim, managed & outsourcing services
□ Legal services	□ Stakeholder Management
□ Risk assurance services	■ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- □ Manage/Monitor
- □ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

Berkshire Hathaway Insurance Group

Berkshire Hathaway Insurance Group	Primary Practice	THREE

Legendary investor Warren Buffett's insurance group has been on a quest to craft an insurance offering targeting small- to mid-sized business (SME) clients. Berkshire Hathaway Insurance Group owns several well-known insurance brands – most famously GEICO – as well as two reinsurance brands and is an important global competitor.

In 2019 the firm launched its THREE insurance line, which tries to simultaneously reduce the financial and time cost of business insurance for SMEs. The name derives from the number of pages of each insurance application in stark contrast to typical insurance product applications for businesses, which are often a dozen or more pages long for each product line. THREE combines business liability, business interruption, cybersecurity, worker's compensation, business auto, and property & assets insurance into a single product package. The cyber portion covers data breaches and cyber liability. THREE is controversial in the insurance world and some wonder whether clients are trading simplicity and affordability for weaker or less clear coverage, and if claims challenges would hold up in court. Still, while basic, THREE does offer for particularly smaller resource-challenged SMEs a chance for even some limited coverage in cybersecurity, which many argue is the fastest growing area of coverage in business insurance.

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◑	◕	◕	◑	◑	🟥	🟨	⬜	🟩 ◑

Impact Scale:

- ● Very High
- ◕ High
- ◑ Moderate
- ◔ Low
- ○ None

Cybersecurity Service Focus

□ Data, technology tools & solutions	□ Accounting & auditing
□ Consulting services	□ Forensic investigations
□ Function-focused advisory services	□ Interim, managed & outsourcing services
□ Legal services	□ Stakeholder Management
□ Risk assurance services	■ Risk transfer services

- □ Strategy
- ■ Compliance
- ■ Risk
- □ Manage/Monitor
- □ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

Vouch

Vouch	Primary Practice	Business Insurance

Vouch is a cloud-based insurance platform (with its own insurance carrier) focused on helping start-ups and high growth companies get the personalized insurance they need quicker and more affordably, or as co-founder Greg Becker describes Vouch's mission, to "empower the innovation economy." One of the drivers behind the firm's founding was the recognition that start-ups (especially early-stage start-ups) struggle with getting adequate insurance coverage, and the process of acquiring that coverage can be as expensive as the insurance itself, absorbing a lot of the start-up's resources while undermining the new company's speed-to-market. Vouch is also backed by Silicon Valley investors, further linking the firm to its client base.

As part of its comprehensive business coverage for start-ups, Vouch includes first- and third-party cyber breach insurance, covering costs for forensic analysis, ransomware payments, customer notification, settlements, and credit monitoring. Vouch's cyber package also covers social engineering and electronic funds mis-transfers. Claims also receive litigation support. Vouch's coverage is personalized for each client, scaling cyber coverage up (or down) based on the degree to which clients manage customer data, for instance. This cyber coverage was expanded during the pandemic to recognize new remote work models and now includes work from anywhere coverage, broader cyber coverages and embedded insurance.

Impact Scale:

- ● Very High
- ◕ High
- ◑ Moderate
- ◔ Low
- ○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◕	◕	◕	◑	◑	🟥	🟨	⬜	🟩 ◑

Cybersecurity Service Focus

□ Data, technology tools & solutions	□ Accounting & auditing
□ Consulting services	□ Forensic investigations
□ Function-focused advisory services	□ Interim, managed & outsourcing services
□ Legal services	□ Stakeholder Management
□ Risk assurance services	■ Risk transfer services

- □ Strategy
- ■ Compliance
- ■ Risk
- □ Manage/Monitor
- □ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

The Legal Service Provider Segment Role in the Ecosystem

For law firms, cybersecurity is a mixed bag. On the one hand, it is a big compliance exercise with strong emphasis on data privacy and, increasingly, data risk management. These services are in high demand, though as cybersecurity shifts gears from a focus on data protection to operations protection in 2022, rote data compliance is devolving from a stand-alone cyber solution to just another puzzle piece in a larger, managed solution picture. Some law firms focus on the micro, like the importance of standardizing cyber risk assessment surveys. Others have sought to augment their technology capabilities through external market relationships with specialized technology players.

One area law firms have excelled in cybersecurity is in hotline-style breach coaching incident response services, positioning themselves as the project managers for insurers covering client incident response events with services spanning first notice of loss calls, discovery, forensic investigations, local jurisdictional notification regulations, and stakeholder communications. Law firms inherited these duties through older insurance models in P&C lines involving client crisis events (triggering claims), which dictated seeking external expert help with crisis management. This has become an important revenue leader for law firms, and as such insurers consider law firms a key part of the insurer cybersecurity response ecosystem. However, the value law firms bring is in part driven by insurers' own reluctance to bring cybersecurity expertise in-house. This value may be eroding as insurers grapple with spiraling costs in their cybersecurity lines, and some focus particularly on not just the payouts, but the cost of the claims process itself in cybersecurity. Law firms can solidify their value proposition by separating the "practice of law" legal advice portion of what they provide in breach coaching from the quasi-legal, lower value fact-finding and informational, as well as administrative value services. Finding ways to maintain or lower costs for insurers by automating, as some innovators have done, the regulatory and compliance informational elements can be helpful. Some law firms have maintained that the forensic investigations part of breach coaching is subject to client privilege and is therefore treated as standard billable hours; this view is controversial among insurers. Taken as a whole, breach coaching is a valuable service for insurers and, unusually, law firms have carved out a unique service niche in what is easily the fastest growing service area in professional services. However, without some level of acknowledgment of clients' (i.e., insurers') growing cost concerns, law firms may find themselves losing ground to competitors with expertise in specialized crisis management. Some insurers are already insisting that their own internal cyber claims professionals take on a bigger role in project management for cybersecurity claims precisely because of cost concerns.

Characteristics:

- Innovators step out of the traditional bounds of how law firms approach cybersecurity, understanding that the compliance and incident response elements are too reactive, that clients need a more integrated approach that meshes with a more managed cybersecurity strategy
- Innovators also recognize that more than anything else, the biggest challenge for clients in cybersecurity in 2022 is cost: cost of management as much as cost of incidents. Consequently, they are utilizing the opportunities presented by AI and automation to keep costs manageable

Cybersecurity Innovators in Legal
Lewis Brisbois
Nishimura & Asahi*
Redgrave

Procurement Priorities

- Be sure to understand a law firm's level of internal technological expertise, and the degree to which they are willing to extend those capabilities through external partnerships
- Request a security audit report for the law firm, paying special attention to data privacy practices and security certifications
- Form an internal team which includes your own in-house legal department (as well as IT, HR, production, etc.) to define cyber risks while formulating a cybersecurity strategy
- Push back on breach coaching services that do not segment quasi-legal, less competitive more "portable" services better addressed through technology as opposed to actual, billable legal advice

* ALM Pacesetter; see profile in Pacesetter section

Cybersecurity SWOT: Legal

Internal Factors

STRENGTHS

- Some law firms have developed detailed specializations in breach coaching services, making them invaluable partners for insurers
- Law firms bring particular expertise around data privacy and governance laws, especially across regional jurisdictions
- The growing importance of GCs in framing client cybersecurity strategies gives law firms a natural conduit for both understanding and shaping client thinking in cybersecurity

WEAKNESSES

- Law firms are struggling to bring technology expertise in-house, and find it difficult to compete with technology and other providers that are better able to integrate deep technology expertise into their cybersecurity offerings
- Most breach coaching offerings still operate on a traditional billing model that does not distinguish between "practice-of-law" services and other, lower value work – saddling clients with high costs at a time when cost containment is a key demand driver in cybersecurity
- Without some level of automation, breach coaching and other incident response services may find themselves constrained soon by capacity issues

Legal providers have traditionally focused on the data compliance and data governance risk component of cybersecurity, but innovators are taking a broader risk approach and becoming more client-centric

OPPORTUNITIES

- As consulting and multiservice providers grow the managed services and Cyber-as-a-Service part of their offerings, law firms can develop parallel services in data privacy and cybersecurity regulatory compliance
- Breach coaching services provide the opportunity for law firms to build and deepen relationships across insurer client organizations, and develop advisory services for cyber strategy
- Cybersecurity also provides an opportunity for law firms to develop cross-domain capabilities by linking broader organizational risk management needs with cybersecurity for clients
- Technology capabilities in particular do not need to be built in-house; cybersecurity presents opportunities for collaboration

THREATS

- The multiservice firms and consulting firms already encroach on legal services through events (e.g., M&A, restructuring), and are applying that same strategy to cybersecurity – with their managed services offerings serving as a Trojan horse
- Data privacy regulations and varying jurisdictional compliance enforcement are areas for which other providers (from consulting and multiservice providers to insurance companies) are developing client-facing databases and automated tools to help clients plan and navigate
- The door is open for ALSPs and others to automate aspects of data privacy and breach coaching services

External Factors

Lewis Brisbois Bisgaard & Smith

Lewis Brisbois	Primary Practice	Data Privacy & Cybersecurity

Los Angeles-based Lewis Brisbois Bisgaard & Smith started out focused on insurance litigation, but has since expanded to become a general practice though still with strong weighting in insurance and Business, Finance & Transactions. Lew Brisbois has fifty-four offices in the US and international affiliates in China, Italy, Japan, South Korea and the UK.

As part of its active Data Privacy & Cybersecurity practice, Lew Brisbois' incident (breach) response services span forensics services (with outside partners), consumer and regulatory notifications, facilitation of consumer remediation services, regulatory investigation guidance & defense, and third party defense. There are two areas, however, where Lewis Brisbois differs in its approach to cybersecurity. One is in the development of cybersecurity and data privacy compliance advisory services which provide proactive "cyber hygiene"-related advisory services around data privacy assessments and strategy planning, training, data retention policies, data transfer agreements, HIPAA security risk assessments, information security assessments & policy development, incident response planning, tabletop exercises, information security awareness training, third party contract review and management, and M&A information security due diligence. The other is that the firm helps manage costs (as well as allowing lawyers to focus on higher value work) through the Lewis Brisbois Data Privacy & Cybersecurity Team's client-facing database of summaries of data breach notification statutes and information security standards throughout the United States (to be extended globally).

Impact Scale:

- ● Very High
- ◕ High
- ◑ Moderate
- ◔ Low
- ○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◑	◕	◕	◕	◑	🟥	🟧	⬜	🟩 ◑

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	■ Forensic investigations
■ Function-focused advisory services	□ Interim, managed & outsourcing services
■ Legal services	□ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- □ Manage/Monitor
- □ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

Redgrave

Redgrave	Primary Practice	Redgrave Data

Since the Firm's founding in 2010, Redgrave LLP ("Redgrave") has been unique in both focus and approach. Created to address the legal challenges that arise at the intersection of the law and technology, Redgrave's sole focus is on Information Law, a practice spanning the fields of eDiscovery, information governance, and data privacy and cybersecurity. Redgrave integrates business and technology acumen with legal advice to help clients understand and address issues from a holistic viewpoint of the business and not just from the angle of legal risk. To this end, Redgrave's client teams are interdisciplinary, with attorneys, MBAs, software developers, and eDiscovery consultants working together. Redgrave recognizes the multi-layered value in its service approach and works with clients to determine mutually acceptable alternative fee arrangements to ensure successful engagements.

In 2022, Redgrave launched an independent affiliate, Redgrave Strategic Data Solutions LLC ("Redgrave Data"), which takes on its own clients and partners with Redgrave to address a wide range of clients' Information Law needs, including vendor management, technology development and deployment, robotic process automation, analytics, artificial intelligence, and data visualization. The new affiliate is more than a traditional law firm LPO in that it looks beyond automation or outsourcing services. Rather than relying on a "one size fits all" approach to software and processes, the Redgrave Data team combines the best commercial offerings with custom development and process engineering to craft tailored solutions for clients.

This level of customization allows for Redgrave Data to enhance and add value to the data privacy and cybersecurity bench that Redgrave has been building out in recent years. Together, the team provides clients with a full spectrum of support, with Redgrave handling strategy and cyber hygiene assessments and partnering with Redgrave Data to focus on solving the data challenges inherent in remediation and incident response. Both entities are thought leaders in their respective spaces and have generated impactful content around eDiscovery, information governance, data privacy and cybersecurity.

Impact Scale:

● Very High
◕ High
◑ Moderate
◔ Low
○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence	🟥	🟨	⬜	🟩
◑	◕	◕	◕	◑				◑

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	■ Forensic investigations
■ Function-focused advisory services	□ Interim, managed & outsourcing services
■ Legal services	□ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

■ Strategy
■ Compliance
■ Risk
□ Manage/Monitor
□ Anticipate
■ Remediate

■ Services offered
□ Services not offered

Cybersecurity 2022: Management Consulting Market

The Management Consulting Segment Role in the Ecosystem

Management consulting providers are on a similar path as multiservice providers – in fact, often emulating their successes – in that they view cybersecurity as a long-term business issue. However, where these providers differ is in their starting point, often bringing very specific technical expertise to bear from their consulting heritage. Legacy financial restructuring & turnaround providers such as Alvarez & Marsal or FTI Consulting bring an important financial, forensic investigations and stakeholder management lens, while traditional strategy consulting firms often focus on cybersecurity from a digital transformation perspective. As private equity clients have become increasingly important for many providers, these providers have shifted focus towards cybersecurity across portfolios, rather than single client organizations, with attention on standardization and simplification. Others bring an important industry focus, with particular expertise around cybersecurity in the light of industry regulations, resource deployment or logistical realities. Many have very powerful brands in specific fields or competencies, though by now their offerings have long since expanded to focus on transformation. Still, in this way these providers are able to compete with the huge technology resources of the multiservice providers, though less so with the giant technology providers.

While less able to compete on scale with multiservice providers and technology giants, management consulting providers have been making substantial investments in technology, to the extent that some offer managed detection & response (MDR) services competitively. These providers are also more likely to partner with technology firms, as well as insurance and law firms in remediation events. Like multiservice providers, these firms often enter cybersecurity projects through adjacent events like M&A or litigation, then approach cybersecurity in an integrated business fashion like multiservice providers do. Another area where management consulting providers have a larger impact than multiservice providers is in tailoring their offering to specific clients (e.g., an industry), or offering solutions more amenable to clients below the Fortune 1000, helping them address some of the unique challenges of more resource-starved clients.

Characteristics:

- While on the same path as multiservice providers in terms of their approach to cybersecurity, their offering by necessity is often more focused and “brass tacks,” providing end-to-end solutions but utilizing external partners for lengthier engagement like managed services
- Many bring targeted expertise such as the regulatory dimension of cyber event remediation, forensic investigations and litigation support, cybersecurity in enterprise risk frameworks, or even navigating US Federal procurement while acquiring cybersecurity assets
- Less tied to end-to-end technology tools than multiservice providers, consulting firms nonetheless bring important digital and cyber capabilities in cybersecurity, both in-house and through ecosystem partnerships

Cybersecurity 2022 Innovators Management Consulting Providers
Alvarez & Marsal
Booz Allen Hamilton
Capco
FTI Consulting
Kroll
PA Consulting

Procurement Priorities

- Ask about their own cybersecurity certifications, and examine in detail how they have implemented their cybersecurity strategy in-house
- Spend time examining their ecosystem partner working relationships
- Ask about how their cybersecurity offering historically evolved, and what service area it originated from; this will provide some insights into their underlying philosophy and service approach, as well as the career trajectory of their senior partners

* ALM Pacesetter; see profile in Pacesetter section

Cybersecurity 2022 SWOT: Management Consulting

Internal Factors

STRENGTHS

- Management consulting providers bring specific competency expertise to cybersecurity: financial restructuring, digital transformation, change management, risk & regulatory strategy
- Most consulting providers have come to focus (like their multiservice peers) on broader business transformation, and incorporate cybersecurity into that service matrix
- Management consulting providers have deep relationships across the C-Suite and throughout client organizations (with variability according to each firm's service focus), providing them with the client knowledge and relationship leverage to design and implement a cybersecurity strategy

WEAKNESSES

- While consulting providers have been developing a wider array of capabilities in recent years, they still tend to be fairly focused (e.g., finance, strategy, an industry, etc.) and will often have weaker service areas (e.g., change management remains an under-developed and resourced offering in some consulting providers) outside of their core competencies that may need bolstering through alliance partnerships
- Management consulting providers face intense competition on the incident response side of cybersecurity, and so seek differentiation on the strategy side leaving them vulnerable to market cycles as spending dries up for strategy projects in economic downturns

For management consulting providers, cybersecurity is a longer-term resiliency play though often tied to events like M&A, and anchored in operational performance as much as technology.

OPPORTUNITIES

- Some management consulting providers have been developing in recent years legal services-focused offerings to support their business transformation business lines – usually centered on forensic investigations (usually event-focused), discovery/ ediscovery, contract management, litigation support, regulatory compliance enforcement action support, legal operations optimization, etc. – and these services can be turned to better capture more of the incident response "breach coach" work currently deployed by law firms for insurance carriers
- Depending on the provider, some have top-tier human capital consulting capabilities and can utilize those for the area clients need most help with: training and creating a cyber-aware culture

THREATS

External Factors

- Cybersecurity talent is scarce, and the multiservice and technology providers appear more attractive from a career standpoint to a lot of candidates
- Cybersecurity as a service area is crowded and the market (outside the largest multiservice and technology firms) is highly fragmented, with technology providers usually first in clients' minds when cybersecurity arises as an issue

Alvarez & Marsal

Alvarez & Marsal	Primary Practice	Regulatory & Risk Advisory

Alvarez & Marsal is a client lifecycle management consulting firm, helping organizations with corporate performance improvement, private equity services, restructuring & turnaround, tax, disputes & investigations, and valuation. The firm has leveraged its turnaround & restructuring consulting heritage with a business model that focuses on the cyclicality of the client company and asset performance, with particular emphasis on M&A. Long known for its financial and tax restructuring strengths, in recent years Alvarez & Marsal has also developed its operational and technology capabilities, furthering the firm's ability solve for complex client problems.

As technology has come to play an increasing role in the firm's offering over the past decade, cybersecurity has also risen in prominence. Alvarez & Marsal approaches cybersecurity from an embedded perspective; since connectivity and technology permeate everything in the modern organization, so too must cybersecurity. Alvarez & Marsal's services span cyber risk advisory, cyber resilience and IR readiness, and incident response and forensics investigations. This includes training and managing the human dimension of cybersecurity, as well as proactive threat hunting, scenario war-gaming and regulatory and litigation support. Managed services are also a growing part of the firm's offering.

Impact Scale:

● Very High
◕ High
◑ Moderate
◔ Low
○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◕	◕	◕	◕	◑	🟥	🟨	⬜	🟩 ◑

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	■ Forensic investigations
■ Function-focused advisory services	■ Interim, managed & outsourcing services
□ Legal services	□ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

■ Strategy
■ Compliance
■ Risk
■ Manage/Monitor
■ Anticipate
■ Remediate

■ Services offered
□ Services not offered

Booz Allen Hamilton

Booz Allen Hamilton	Primary Practice	Cybersecurity

Edwin G. Booz, the founder of the first iteration of Booz Allen Hamilton in 1914, essentially invented modern management consulting, and with it the concept of the objective “trusted advisor.” McLean, Virginia-based Booz Allen Hamilton’s most recent incarnation is the result of a spin-off of its commercial-focused side of the firm to create Booz & Company, which was acquired by PwC in 2013. This means Booz Allen Hamilton today is overwhelmingly focused on US Federal government contract work, in particular its work with US intelligence agencies, and is known for recruiting extensively among intelligence alumni. Today Booz Allen Hamilton is a strategy consulting firm focused on transformation across four service pillars: data analytics, digital, engineering and cybersecurity. While heavily geared towards the US government as a client, the firm has been slowly building its corporate client portfolio as well.

Given the firm’s close business relationships with the US military and intelligence services, cybersecurity is a major competency for the firm. In response to the needs of its US Federal clients, Booz Allen Hamilton approaches cybersecurity proactively as an integrated, interdisciplinary prevention strategy rather than a reactive event remediation service. In this sense Booz Allen Hamilton represents the cutting edge of cyber risk management spanning active defense, detection and remediation, while also including a cost management dimension. It describes its approach as a full-spectrum cyber mission delivery. Cyber solutions are organized into three core service groups: Cyber Defense (Cyber Risk, Cyber Architecture and Engineering, Cyber Defense Operations), Cyber-enabled Platforms, and Cyber Warfare, where Booz Allen Hamilton helps clients actively engage cyber opponents through reverse engineering, data analytics, advanced algorithmic warfare solutions, and more. While technology-centric, the firm’s solutions also take into account the human factor in cyber defense.

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◕	◕	◕	◕	◑	🟥	🟨	⬜	🟩 ◑

Impact Scale:

- ● Very High
- ◕ High
- ◑ Moderate
- ◔ Low
- ○ None

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	■ Forensic investigations
□ Function-focused advisory services	■ Interim, managed & outsourcing services
□ Legal services	■ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- ■ Manage/Monitor
- ■ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

Capco

Capco	Primary Practice	Security services

London-based Capco was founded in 1998 under the name The Capital Markets Company NV as a consulting firm focused on capital markets and banking clients. Rebranding as Capco just a few years later, it has gained global notoriety over the following decades for its financial services expertise. Its consulting approach has always included a strong technology component but the firm expanded its investment in its technology capabilities after the 2008 economic crisis and the resulting retrenchment of regulations in financial services. Today Capco's services span financial services and include a strong risk management component with the central theme being digital transformation and has translated its technology, compliance, risk and operational expertise to the energy sector. In 2021 Capco was acquired by India-based technology firm Wipro and operates as an independent subsidiary.

Capco recognizes that cybersecurity cannot be separated from other client organization functional elements and must be baked into the larger risk management framework. In its approach to cybersecurity the firm brings together its expertise across risk management, technology and regulatory compliance in financial services with services in plan design that span crisis management, data security and protection, regulatory response, and governance and reporting functions. Other services include board-level advisory on cybersecurity strategy, and both augmented staff solutions and managed services that includes a CISO-as-a-service offering. Despite the firm's strong technology and regulatory focus, Capco's cybersecurity offering contains important human capital elements, both on the defense side – the human role in cyber vulnerability – as well as recruiting skilled talent. Another important distinguishing element for Capco's approach is a specially designed cybersecurity offering for medium-sized clients, considering their own peculiar risk and resource reality.

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◕	◕	◕	◑	◑	🟥	🟨	⬜	🟩 ◑

Impact Scale:

- ● Very High
- ◕ High
- ◑ Moderate
- ◔ Low
- ○ None

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	■ Forensic investigations
□ Function-focused advisory services	■ Interim, managed & outsourcing services
□ Legal services	■ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- ■ Manage/Monitor
- ■ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

ALM INTELLIGENCE
INNOVATOR
CYBERSECURITY **2022–2023**

FTI Consulting

FTI Consulting	Primary Practice	Cybersecurity

Washington, DC-based FTI Consulting is a global consulting firm covering a broad range of services including restructuring, M&A, change management, strategic communications, cybersecurity and technology, risk and disputes management. Their primary practices are Corporate Finance Restructuring, Forensic and Litigation Consulting, Economic Consulting, Technology, and Strategic Communications. Even before the pandemic and a looming recession, FTI's M&A and restructuring businesses were in high gear. FTI has also invested heavily in its industry expertise.

Cybersecurity for FTI is something that needs to be woven into the fabric of any growth strategy, and as such, cybersecurity is a horizontal competency that permeates all practice areas in the firm. The cybersecurity team at FTI has seen phenomenal growth in recent years in response to direct client demand and it targets former government cyber experts in its recruiting. Services are organized around three basic buckets: Cyber Readiness (program assessment, penetration testing, table-top exercises, crisis simulations, compliance, threat-hunting operations, red teaming, any steady-state condition assessment analysis tied to the formulation of a cybersecurity strategy), Incident Response (utilizing a 360° holistic approach involving a full technical response supported by a crisis manager, a strategic communicator, and other experts such as compliance specialists), and Complex Investigations & Litigation support (which utilizes FTI's forensic investigations and litigation support capabilities, including expert witness testimony, e-discovery and evidence collection, forensic analysis, data breach class action and industry-specific settlement advice). FTI offers interim CISO services, as well as human- and technical-resource managed services, and continues to aggressively expand its cybersecurity team globally. FTI also has a multidisciplinary Office of the Chief Risk Officer (OCRO) solution, which is designed to identify, assess, evaluate, and respond to key risks across the enterprise, business lines, and geographies.

Impact Scale:
● Very High
◕ High
◑ Moderate
◔ Low
○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◕	◕	◕	◕	◑	🟥	🟨	⬜	🟩 ◑

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	■ Forensic investigations
□ Function-focused advisory services	■ Interim, managed & outsourcing services
■ Legal services	■ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

■ Strategy
■ Compliance
■ Risk
■ Manage/Monitor
■ Anticipate
■ Remediate

■ Services offered
□ Services not offered

Kroll

Kroll	Primary Practice	Cyber risk

In 2018 finance and investment consulting firm Duff & Phelps acquired compliance, litigation and risk management consulting firm Kroll, and by 2022 the combined firms had rebranded as Kroll. In the last several years before the merger Kroll had developed particular expertise in cybersecurity. Services span compliance and regulation, corporate finance and restructuring, cyber risk, ESG, investigations and disputes, business services and valuation. The common thread in both Duff & Phelps' and Kroll's service focus was GRC: governance, risk and compliance with cybersecurity becoming a service spear point.

In cybersecurity, the (pre-Duff & Phelps) Kroll name had been synonymous with an elite special operations force in incident response that contained teams of experts with specialist skills in cybersecurity, intelligence and investigations. The firm has since been building out the defense and risk management (and active real-time monitoring) dimension of its offering more recently for a full-service, end-to-end cyber risk offering. Kroll's framework for building what it calls a Defensible Security Strategy is structured around five pillars: assessments, governance, notification, response and managed security. The managed services part of that offering forms a growing portion of Kroll's efforts in cybersecurity. Other services include end-to-end cyber risk management services, including breach notification and identity theft, notification call center operations, and identity monitoring and restoration solutions.

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◕	◕	◕	◕	◕	🟥	🟨	⬜	🟩 ◕

Impact Scale:

- ● Very High
- ◕ High
- ◑ Moderate
- ◔ Low
- ○ None

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	■ Forensic investigations
□ Function-focused advisory services	■ Interim, managed & outsourcing services
□ Legal services	■ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- ■ Manage/Monitor
- ■ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

PA Consulting

PA Consulting	Primary Practice	Cyber security & digital trust

UK-based PA Consulting is a legacy strategy consulting firm with strong design, technology, and human capital service components. Services span agile transformation and delivery, business design, cybersecurity and digital trust, data and analytics, design and engineering, digital transformation, IT strategy and sourcing, major program delivery, operational excellence, people and change, and strategy.

In cybersecurity, PA Consulting's approach is built around the concept of digital trust: convincing (through apt policies) customers, regulators and third-party partners that all external data is handled securely and responsibly. This requires an end-to-end approach covering cyber transformation, data privacy, operational resilience, IoT security, cloud security, risk and compliance, e-discovery, operational technology security, and incident response. Services are divided into three basic roles: prevention, recovery & remediation, and a human capital focus that includes AI-based monitoring, training, and leadership development focused on good governance models for cybersecurity. PA Consulting also helps clients prepare (operationally, strategically, compliantly) for more innovative third-party cybersecurity solutions such as Managed Detection and Response services or Security as a Service (SECaaS) offerings.

Impact Scale:
- ● Very High
- ◕ High
- ◑ Moderate
- ◔ Low
- ○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◑	◕	◕	◑	◑	🟥	🟨	⬜	🟩 ◑

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	□ Forensic investigations
□ Function-focused advisory services	□ Interim, managed & outsourcing services
□ Legal services	■ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- □ Manage/Monitor
- □ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

Cybersecurity 2022 Demand Drivers: Multiservice

The Multiservice Segment Role in the Ecosystem

The multiservice provider approach to cybersecurity has been years in the making and was born mostly of necessity. As they gravitated in recent years towards a business transformation delivery model, cybersecurity organically became intertwined in that offering. This taught multiservice providers to weave cybersecurity into client operations and functions, putting them at the forefront of thinking on what constitutes effective cybersecurity. In typical fashion they integrated their several competencies (risk assurance and compliance, technology, operations, legal, tax, human capital and change management, financial restructuring, M&A, supply chain, etc.) to create a full, end-to-end offering that treated cybersecurity as a business activity rather than a software play, helping clients make informed cyber risk decisions as they go about their business. Training and upskilling client employees is a key part of their offering, for instance.

Aside from a full, end-to-end offering fully integrated into their horizontal and vertical service domains, multiservice providers bring a few other approaches to cybersecurity that distinguish them from their competitors. The first one is that their primary point of entry for cybersecurity tends to be through an adjacent event, although they also offer remediation services in their integrated approach. M&A, restructuring, IPOs, and new product launches are all "foot-in-the-door" entry points for multiservice providers to engage their cyber teams. For them, cybersecurity is less a stand-alone problem and more a strategic challenge and their goal is to help clients build long-term business resiliency. A key term many multiservice providers use when describing their cybersecurity offering is trust, meaning building and integrating an effective, transparent cybersecurity strategy throughout a client organization so that stakeholders know they can rely on that organization to deliver.

While they lead with business transformation, multiservice providers do not eschew technology in cybersecurity. Quite the contrary, they compete head-to-head with the giant, global technology firms in terms of data analytics and advanced technologies, and also partner with the largest endpoint solution providers. One area they have particularly invested in in recent years in cybersecurity is managed services and Cyber-as-a-Service – again, in direct competition with the big tech firms – but their endgame is to develop long-term, stickier relationships with clients while engaging them at lower price points and more creative billing models.

Characteristics:

- Cybersecurity conversations for multiservice providers begin very differently than for most other providers, and center around long-term business goals rather than software solutions
- Multiservice providers have turned towards managed services and as-a-service solutions in a big way in recent years

Cybersecurity Innovators Multiservice Providers
Crowe
Deloitte
EY
KPMG*
PwC*

Procurement Priorities

- Multiservice providers are themselves great laboratories for cybersecurity, so ask to see in detail how they themselves have implemented the kinds of systems and policies they recommend
- Typically with a multiservice provider, the billing and pricing options are a negotiable variable but before committing to any option, be sure to investigate the full impact on both your project outcome and the cost
- Many multiservice providers have been investing in recent years in scenario-planning capabilities, including "wargaming" technology that help flesh out risk models
- Cybersecurity projects – especially with multiservice providers – are large and complex, so it is more important than usual for clients to be conscious of provider resource and team composition

* ALM Pacesetter; see profile in Pacesetter section

Cybersecurity 2022 SWOT: Multiservice

Internal Factors

STRENGTHS

- More so than most other providers, multiservice providers take a long-term, enterprise perspective on cybersecurity that aligns well with enterprise risk management and strategic development goals
- Multiservice providers are experts at penetrating client organizations, learning about and building relationships at all levels, making these providers apt partners for garnering buy-in with key stakeholders for cybersecurity strategies
- Themselves global organizations, multiservice providers can bring an informed, objective eye to cyber challenges
- Multiservice providers typically also manage large, developed ecosystem partnerships to extend their own expertise

WEAKNESSES

- By their nature global, member network organizations, multiservice providers often struggle with scale and are forced to focus on the largest, most complex, global client challenges
- Though this varies from provider to provider, multiservice providers have the reputation of being less able (or willing) to customize, taking a more standardized, less flexible, best practices-driven approach to cybersecurity
- Multiservice providers tend towards the upper end of attractiveness for candidates but still struggle to staff cyber teams as the talent market is white hot

Multiservice providers view cybersecurity as a business transformation component, and as such one that can be made into a competitive advantage for clients

OPPORTUNITIES

- One of the areas clients struggle with is justifying the huge investments required for cybersecurity, which are often considered sunk costs instead of strategic or differentiating investments, and multiservice providers have the relationships across client organizations to make these ROI arguments
- Multiservice providers also have the thought leadership and economic consulting resources to produce long-term studies linking specific client outcomes to cybersecurity practices
- In an increasingly volatile world, multiservice providers can produce targeted offerings helping clients navigate the geopolitical dimensions of cybersecurity, including data privacy and cyber regulations shifts

THREATS

- Multiservice providers' approach to cybersecurity is being replicated and emulated by management consulting providers, who often bring specialist skills and talent
- Cost sensitivity is a major driver in 2022 in cybersecurity, and multiservice providers are surrounded by cheaper technology providers and boutiques whose offerings are less comprehensive, but assert that "good enough" trumps perfection
- While mechanical and reactive, law firms have cornered a sizeable audience with their breach coaching services for insurers, providing them with a platform for exploiting their remediation services should they decide to do so

External Factors

Crowe

Crowe	Primary Practice	Risk Consulting Services

Crowe is a New York-based multiservice, legacy auditing network with services spanning auditing, tax, advisory and consulting, all underscored by strong technology capabilities. Crowe's services are organized around the principle of business transformation, reflected in its Adaptive Business Framework, which puts business challenges on a value spectrum ranging from value protection through value creation, across four basic stages (remediate, maintain, optimize, innovate). In Crowe's framework, these stages are impacted by what it calls the levers of value: data-driven insight, data-powered technology, culture-supported empowerment, appetite for change, and communication and translation. Crowe focuses on helping clients build business resiliency earlier in the value protection stages to make room for innovation later in the value creation stages.

Cybersecurity has been a major area of investment for Crowe in recent years, very much in tandem with its pivot towards total business transformation, with the emphasis shifting from reactive technology services to making cybersecurity an organizational differentiator. Embedded in its risk consulting practice area, Crowe's approach to cybersecurity is a full, end-to-end solution encompassing strategy, program design and implementation, attack and penetration testing, incident response (including a managed detection and response service offering), and monitoring. Crowe's Integrated Cybersecurity Framework (CICF) evaluates client cybersecurity systems across controls and risks, including Key Risk Indicators (KRIs) to measure a client's risk management status. Crowe's ultimate goal in cybersecurity is to help clients make better risk-informed decisions. The firm also has a managed detection & response (MDR) capability. In late 2021 Crowe acquired auditing firm Briggs & Veselka which also strengthened the firm's digital forensics capabilities.

Impact Scale:

● Very High
◕ High
◑ Moderate
◔ Low
○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence	🟥	🟨	⬜	🟩
◕	◕	◕	◕	◕				◕

Cybersecurity Service Focus

■ Data, technology tools & solutions	■ Accounting & auditing
■ Consulting services	■ Forensic investigations
■ Function-focused advisory services	■ Interim, managed & outsourcing services
■ Legal services	■ Stakeholder Management
■ Risk assurance services	□ Risk transfer services

■ Strategy
■ Compliance
■ Risk
■ Manage/Monitor
■ Anticipate
■ Remediate

■ Services offered
□ Services not offered

Deloitte

Deloitte	Primary Practice	Risk Advisory

Deloitte has become a more asset- and platform-driven professional services firm, relying more on technology (and technology-driven services) to drive transformation across client organizations. Total business transformation is a central theme for Deloitte, with its approach relying on technology tools developed both in-house as well as partner technology, all closely integrated across its Tax, Consulting, Audit Assurance, Mergers Acquisitions, and Legal and Risk Advisory practice areas.

Deloitte approaches cyber from a strategic risk perspective, housing its core cybersecurity services in its Risk Advisory practice. The central theme for Deloitte is digital trust: developing an effective cybersecurity framework that convinces a client's key stakeholders that it is serious about how it manages its digital assets. This trust is achieved (according to Deloitte) through transparency and accessibility, security and reliability, privacy and control, and ethics and responsibility. Some solutions Deloitte has focused on for digital trust are cloud-enabled data trusts and AI monitoring, and using blockchain for data provenance and ownership. Deloitte's approach to cybersecurity is integrated across its practice areas, and spans strategy formulation, data & privacy, application security, infrastructure, identity, cloud, and detect & respond. In early 2022, Deloitte launched a new cybersecurity threat detection & response Software-as-a-Service (SaaS) platform called Managed Extended Detect and Response (MXDR) in conjunction with several vendors.

Impact Scale:

● Very High
◕ High
◑ Moderate
◔ Low
○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◕	◕	◕	◕	◕	🟥	🟨	⬜	🟩 ◕

Cybersecurity Service Focus

■ Data, technology tools & solutions	■ Accounting & auditing
■ Consulting services	■ Forensic investigations
■ Function-focused advisory services	■ Interim, managed & outsourcing services
■ Legal services	■ Stakeholder Management
■ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- ■ Manage/Monitor
- ■ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

EY	Primary Practice	Cybersecurity, strategy, risk, compliance and resilience

As the consulting world moves towards a business transformation focus, EY has extensively developed the human dimension of its approach in the form of its People Advisory Services (PAS) practice. PAS is closely integrated into all EY's offerings across the Consulting, Strategy Transactions, Tax, Assurance, and Legal practices, reflecting EY's strategy of putting humans at the center of change. EY sees people centricity, along with technology and innovation as being among the three drivers of long-term value creation.

For EY, cybersecurity is just one more component of business transformation, but a necessary one. Its risk-based Security by Design approach bakes cyber risk into strategic transformation. Under Cybersecurity Transformation, Security by Design is a systems engineering approach to managing cyber risk by prioritizing security features in the design of technology and data architectures. EY accomplishes this 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, called Transformation Realized™. EY further addresses CISO needs through its cybersecurity, strategy, risk, compliance and resilience services, which include cyber risk assessment, program design, compliance, stakeholder management, and training & upskilling, as well as a managed services offering.

Impact Scale:

● Very High
◕ High
◑ Moderate
◔ Low
○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◕	◕	◕	◕	◕	🟥	🟨	⬜	🟩 ◕

Cybersecurity Service Focus

■ Data, technology tools & solutions	■ Accounting & auditing
■ Consulting services	■ Forensic investigations
■ Function-focused advisory services	■ Interim, managed & outsourcing services
■ Legal services	■ Stakeholder Management
■ Risk assurance services	□ Risk transfer services

■ Strategy
■ Compliance
■ Risk
■ Manage/Monitor
■ Anticipate
■ Remediate

■ Services offered
□ Services not offered

Cybersecurity 2022 Demand Drivers: Technology

The Technology Segment Role in the Ecosystem

Technology providers in cybersecurity are Legion, and come in all shapes and sizes. For obvious reasons, technology providers are where cybersecurity was born, and continues to develop. By now there are a large group of pureplay cybersecurity technology firms, but nearly every technology provider has developed some strong suite of cybersecurity services. These services were ratcheted up significantly by the pandemic and the experience of clients having to suddenly develop remote working models en masse, prompting providers to put together end-to-end suites that included everything from shareware packages and video conferencing to cybersecurity – often on an ad hoc basis. Solutions span infrastructure, automation, the cloud, endpoint security solutions, encryption, and more recently, continuous monitoring of cyber threats (with AI-driven responses) in the form of managed services and offering such as managed detection & response (MDR) services. In fact this latter category is where the bulk of today's service investments focus, developing longer-term retainer-style service relationships while filling in client skill and capacity gaps.

Innovators have been building out consulting capabilities alongside their technology offerings, and have also been bundling different service packages to make technology-enabled business functions – including cybersecurity – available for middle-tier and smaller clients. This is where technology firms are able to have the most impact, providing service and technology suites to under-resourced clients below the radar of multiservice providers and larger consulting firms. Some of these providers such as Capgemini straddle the technology and consulting worlds so effectively it is difficult to categorize them. However, consulting capabilities are usually only support services (and rarely stand-alone), and these providers' first point of entry for clients is usually the CISO, CIO or CTO. These firms often do not have the breadth of contacts in client organizations that consulting or multiservice providers do. Their serious capabilities and bandwidth capacity (e.g., data analytics and management, service centers, etc.) puts them first in line for cyber event remediation, however, for many clients. Their global reach and ability to automate risk and compliance functions also makes them attractive in cyber.

The emphasis for technology providers tends to be on data protection, and identifying and addressing specific threats – ergo the detect and protect monitoring services and managed services offerings. Many providers also work through ecosystem partnerships to fill in the operational gaps in their services. These firms are also usually first in line for top cyber talent.

Characteristics:

- Technology providers typically build end-to-end cybersecurity suite solutions but Innovators bolster with consulting services
- Whether through managed security services (MSS) or similar offerings, technology providers seek to offer long-term partnerships to help clients manage the ever-shifting threat landscape in cybersecurity and keep abreast of latest regulations

Cybersecurity Innovators Technology Providers
Accenture
Capgemini
Tata Consultancy Services (TCS)

Procurement Priorities

- Examine whether they use their own cyber solutions and study in detail how they work, how their employees interact with them, etc.
- There are so many technology systems available to address cybersecurity that clients must prepare by creating a detailed list of their in-house technical needs (and abilities), defining carefully the criteria cyber solutions must meet
- Carefully vet any third party vendor relationships, both in their supply chain as well as in service delivery both for the impact on your risk in working with them as well as the quality of the outcome in your cyber solution
- Seek to understand their billing and exactly how they arrive at the final price, as technology providers are often able to be the most cost effective in cybersecurity

* ALM Pacesetter; see profile in Pacesetter section

ALM INTELLIGENCE
PACESETTER
RESEARCH

Cybersecurity 2022 SWOT: Technology

Internal Factors

STRENGTHS

- Massive global capacity in data analytics and management, as well as AI and advanced technology resources
- Top (and even lesser-known) brands are often first choice for scarce cybersecurity talent
- Deep expertise in legacy, current, and emerging cybersecurity technologies, systems and capabilities
- Sophisticated service delivery tools increasingly tailored for the post-pandemic, remote workforce world
- Some providers also manage detailed databases of cyber events, key players, networks, and evolving technologies

WEAKNESSES

- While many of these providers are developing consulting capabilities to support their cyber solutions, these are often fairly limited or, even when robust, often encounter difficulty in the market convincing clients of their viability – leading to difficulties building relationships outside client risk or technology leads
- As some providers develop their own proprietary in-house cyber platforms and solutions, some clients have expressed concern about objectivity in vendor/system recommendations
- Despite efforts at in-house consulting teams and partnering with external consultants, some technology providers struggle to incorporate a strong operational element into their cyber offerings

Technology providers in some respects have been eclipsed in cybersecurity by multiservice providers but still offer a significant value in terms of detect-protect-defend services

OPPORTUNITIES

- Legal departments in 2021 reported a growing willingness to "piggyback" onto existing platforms in their organization for their own operational needs, opening the door for technology providers with their own platform products to extend cybersecurity tools into new client areas
- One area multiservice providers have made much traction with is scenario-planning and "war-gaming," helping clients visualize in detail the impact of policy decisions and external factors
- As clients continue to struggle with Shadow IT in 2022, developing diagnostic tools to help them identify and address instances (and motivations) of use could be very helpful

THREATS

External Factors

- Multiservice providers in general are either almost on par with technology firms in terms of their technology capabilities, or are catching up – and are better able to wed those technology capabilities with operations, human capital etc. dimensions of cybersecurity solutions.
- Multiservice and management consulting providers stress to clients their objective assessment of cybersecurity tools
- Cost sensitivity is a major driver in 2022 in cybersecurity, and multiservice providers work with cheap technology vendors and boutiques whose offerings are less comprehensive, but assert that "good enough" trumps perfection in cybersecurity

Accenture

Accenture	Primary Practice	Security

Accenture has been gaining recognition in recent years for the increased impact of its non-consulting offering and more integrated solutions, all underlined by years of solid revenue performance. Accenture was originally the consulting wing of the fabled Arthur Andersen accounting firm, and it separated from its disintegrating parent in 2001 to become Accenture ("Accent + Future"). In recent years Accenture has developed a sophisticated long-term client onboarding strategy that builds relationships with clients in their early development stages, ultimately shepherding them to growing into what Accenture calls its Diamond Clients – organizations with annual revenues topping $100 million. In early 2020 Accenture underwent a significant reorganization into four core service areas: Strategy & Consulting, Interactive, Technology, and Operations.

Accenture's cybersecurity offering is housed in its Security practice area, and is heavily anchored in managed services. The pandemic has spurred big growth for the firm's cybersecurity services. Services span advanced attack and readiness operations, cyber operations & resilience, application security advisory services; cyber investigation, forensics & response; and cyber threat intelligence. There is a strong element of long-term business resilience and brand risk management baked into Accenture's approach. The firm created its Accenture Cyber Fusion Centers (many of which are tailored to specific industries) to allow clients to develop and test their cybersecurity strategies in a realistic environment. Accenture Security has in recent years become an important partner with the US Federal government for cybersecurity services. In 2020 Accenture acquired Symantec Cyber Security Services, enhancing the firm's managed security services offering.

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◕	◕	◕	◑	◕	🟥	🟨	⬜	🟩 ◕

Impact Scale:
- ● Very High
- ◕ High
- ◑ Moderate
- ◔ Low
- ○ None

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	■ Forensic investigations
□ Function-focused advisory services	■ Interim, managed & outsourcing services
□ Legal services	□ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- ■ Manage/Monitor
- ■ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

Capgemini	Primary Practice	Cybersecurity Services

Paris-based French technology firm Capgemini has wavered over the years between consulting and technology, but has always sought ways to combine the two to help clients achieve total business transformation. The firm was a leader in digital transformation and cloud-based solutions and has made a steady stream of global acquisitions to support these service lines.

Capgemini's approach to cybersecurity has evolved into a Cybersecurity-as-a-Service offering, strengthened by the 2019 acquisition of the cybersecurity services unit from defense and technology firm Leidos. Capgemini combines technology with people and processes in its approach to cybersecurity, with services grouped into three basic categories: Define (current-state assessment, application security, GRC), Protect (developing a strategic plan), and Defend (actively monitoring for threats and managing them). In the Define category, Capgemini has developed what it calls its Unified Enterprise Defense (UED) model, which addresses culture and organization, governance, visibility and controls, a focused defense, and intelligence operations. Its managed services and managed detection & response (MDR) services reside in its Defend category. These services are supported by a global array of connected Security Operations Centers.

Impact Scale:

- ● Very High
- ◕ High
- ◑ Moderate
- ◔ Low
- ○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence	🟥	🟨	⬜	🟩
◕	◕	◕	◑	◑				◑

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	■ Forensic investigations
□ Function-focused advisory services	■ Interim, managed & outsourcing services
□ Legal services	□ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- ■ Manage/Monitor
- ■ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

Tata Consultancy Services (TCS)

Tata Consultancy Services (TCS)	Primary Practice	Cyber Security

Mumbai-based TCS is the technology and consulting affiliate of the famed Indian Tata family of businesses and has followed its sibling business lines throughout the world. While increasingly competitive in Europe and North America, TCS has an anchor in emerging markets regions, particularly southern Asia, MENA (Middle East and North Africa), and eastern Africa. Services span the technology spectrum from infrastructure to cloud, data analytics, and advanced technology, with managed services and outsourcing playing a significant role in revenues. TCS' consulting mostly supports these services from strategy and development through implementation. A unique element to TCS' strategy is its focus on emerging markets regions and on medium-sized clients in those regions. While global consulting firms work with clients hovering near the Fortune 500 designation to get them across the finish line, TCS has developed a framework to help medium-sized clients along the organization maturity curve to achieve long-term growth goals. In the process, TCS gains a larger-sized and more sophisticated – and loyal – client base.

Given its client focus, it is not surprising that TCS is well known for its more template- (and platform-) driven solutions. TCS puts cybersecurity into a broader business transformation context, and as such weaves its solutions into its digital offerings, especially data management and governance. In early 2022, TCS introduced its Cyber Defense Suite to support clients undergoing digital transformation. TCS' Cyber Security Implementation Services offer a full, end-to-end service approach across identity & access management, enterprise vulnerability management, fraud management & digital forensics, GRC, and managed security services (which includes intelligence-led, managed detection and response (MDR) services such as TCS' Cyber Vigilance Platform). TCS has also set up eight security centers of excellence to capture success stories and help drive innovation.

Impact Scale:

● Very High
◕ High
◑ Moderate
◔ Low
○ None

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◑	◕	◕	◑	◑	🟥	🟨	⬜	🟩 ◑

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	■ Forensic investigations
□ Function-focused advisory services	■ Interim, managed & outsourcing services
□ Legal services	□ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

■ Strategy
■ Compliance
■ Risk
■ Manage/Monitor
■ Anticipate
■ Remediate

■ Services offered
□ Services not offered

West Monroe Partners	Primary Practice	Digital & Technology

Started by former Arthur Andersen consulting colleagues in Chicago in 2002, the firm is named after the address of Arthur Andersen's Chicago office. West Monroe Partners' early service focus was on the technology platforms of local Chicago financial exchanges. Today, West Monroe Partners bills itself as a digital consulting firm though with increasing strategy and operations capabilities, with services spanning analytics & AI, the corporate transformation practice, analytics-driven customer experience, cybersecurity, digital transformation, a strong M&A practice, and operations excellence. WMP has developed many proprietary technology tools for its practices over the years, and services also include interim and managed services. WMP formed a strategic alliance with the European consulting firm BearingPoint in 2010, and has a strong history of working closely with a wide array of ecosystem partners due to its specific service focus.

In recent years West Monroe Partners has come to focus strongly on private equity clients, and its approach to cybersecurity reflects this client focus (consequently, the firm's offering is heavily M&A-focused). Often leading with its industry practice areas, West Monroe's offering spans strategy development, the use of cyber mesh strategies to mingle management of individual portfolio assets with entire portfolios, active threat detection and the firm's Cybersecurity Advisory for Private Equity (CAPE) cybersecurity managed services offering. With its consulting-supported Intelllio® suite of technology tools, West Monroe Partners provides private equity clients (with ever-changing portfolios, for which they must constantly build and optimize platforms) with the ability to build platforms more quickly and manage their cybersecurity risk (including due diligence) over an M&A deal lifespan.

Pacesetter Criteria					Pacesetter Impact Score			
Business Model	Value Proposition	Service Delivery	Client Enablement	Brand Eminence				
◑	◕	◕	◑	◑	🟥	🟨	⬜	🟩 ◑

Impact Scale:
- ● Very High
- ◕ High
- ◑ Moderate
- ◔ Low
- ○ None

Cybersecurity Service Focus

■ Data, technology tools & solutions	□ Accounting & auditing
■ Consulting services	□ Forensic investigations
□ Function-focused advisory services	■ Interim, managed & outsourcing services
□ Legal services	□ Stakeholder Management
□ Risk assurance services	□ Risk transfer services

- ■ Strategy
- ■ Compliance
- ■ Risk
- ■ Manage/Monitor
- ■ Anticipate
- ■ Remediate

■ Services offered
□ Services not offered

ALM INTELLIGENCE
PACESETTER
RESEARCH

Appendix

Research Methodology: Overview

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

Research Methodology: Scoring

Impact Scale:

● Very High

◕ High

◑ Moderate

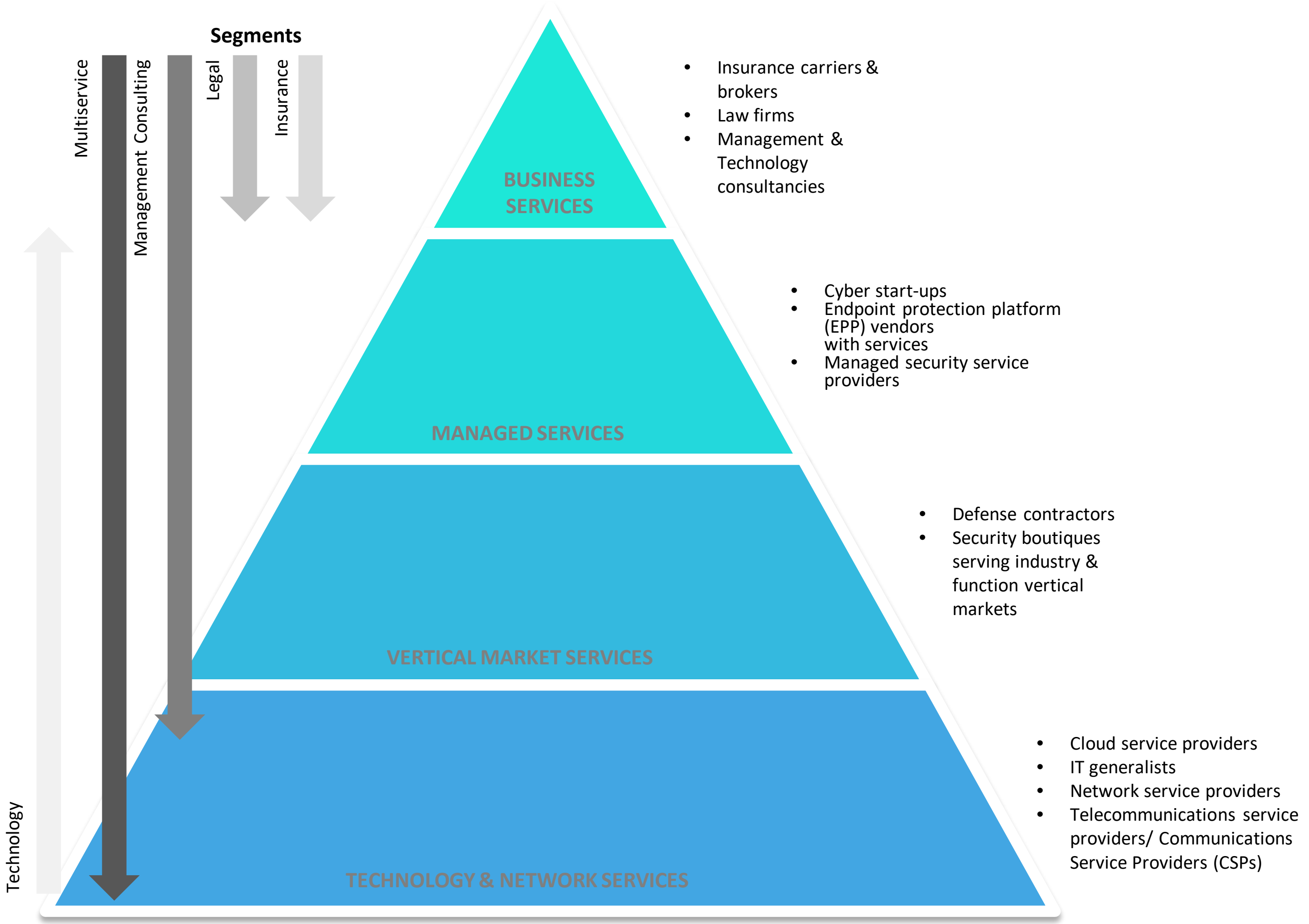
◔ Low

○ None

The goal of this research was to identify which professional services providers were having the most impact in a rapidly shifting market environment, and measure precisely what that impact was. Each provider, once identified either through the research or by the Pacesetter Advisor Council (PAC), was evaluated in five client impact categories and within each, five sub-categories (See Page 54 for category details and definitions.), using a 100-point scale for each sub-category. This means that that maximum unweighted score for each category was 500 points, all of which rolled up to a maximum (unweighted) score of 2,500 points. The scoring framework does allow for targeted weighting of subcategories, though no weighting was used for the Cybersecurity *2022* report. In order for a provider to be identified as a Market Leader – in other words, to be included in this report – they had to score a minimum overall 70%. To achieve Pacesetter status in this report, they had to score a minimum 85%. The Harvey Balls moon graphics represent the following scores:

- 85%-100%: Very High impact
- 80%-84%: High impact
- 75%-79%: Moderate impact
- 66%-74%: Low impact
- <74%: None

Definitions: Cybersecurity



- Insurance carriers & brokers
- Law firms
- Management & Technology consultancies

- Cyber start-ups
- Endpoint protection platform (EPP) vendors with services
- Managed security service providers

- Defense contractors
- Security boutiques serving industry & function vertical markets

- Cloud service providers
- IT generalists
- Network service providers
- Telecommunications service providers/ Communications Service Providers (CSPs)

Cybersecurity refers to the risk management strategy of protecting an organization's technology, data and digital assets – with the goal of reducing, if not entirely mitigating, the risk of cyber attacks and protect against the unauthorized exploitation of systems, networks and technologies – and the operations they enable.

This involves the strategy, compliance, risk, manage/ monitor, anticipation (detect), and remediation phases. While most discussions of cybersecurity focus on the technology aspects, this report focuses on the business side of cybersecurity, including the operational, financial, and human capital elements, with a long-term view towards business resiliency.

Definitions: Pacesetter Evaluation Criteria

Core Criteria	Definition
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

Definitions: Acronyms

Acronym	Definition	Line of Defense	Areas of Risk Responsibility
CCO	Chief Compliance Officer	2nd	Responsible for establishing standards and implementing procedures to ensure compliance programs effectively identify, prevent, detect and correct noncompliance with applicable laws and regulations
CEO	Chief Executive Officer	1st	Collaborates with Board in fiduciary oversight role; responsible for enterprise risk management strategy overall
CFO	Chief Financial Officer	1st	Manages funding of risk resources, programs and insurance; analyzes impact of risk events on bottom line; monitors and reports on ROI of risk investments, including insurance
CHRO	Chief Human Resources Officer	1st	Contributes to development of risk policies and procedures related to workforce and workplace matters; central source of risk training, communications, and change management for employees, managers and leaders
CIO	Chief Information Officer	1st	Responsible for monitoring and enforcing risk policies, procedures and practices related to information technology
CISO	Chief Information Security Officer	1st	Responsible for monitoring and enforcing risk policies, procedures and practices related to corporate data
CMO	Chief Marketing Officer	1st	Manages, monitors and mitigates organization's brand and reputational risk; leads external crisis communications
COO	Chief Operating Officer	1st	Assesses, controls and mitigates risks impacting day-to-day operations and business processes
CPO	Chief Procurement Officer	1st	Manages and audits third party risk; collaborates with CFO and GC on insurance procurement
CRO	Chief Risk Officer	2nd	Primary responsibility for enterprise risk management strategy and operations; leads corporate risk function; collaborates with GC and CPO to procure insurance in line with organization's risk strategy and appetite
GC	General Counsel	2nd	Advises Board and senior management on governance, compliance, risk and legal matters; responsible for developing, implementing and monitoring programs to support the business' risk owners
IA	Internal Audit	3rd	Provides independent assurance that the organization's risk management, governance and internal control processes are operating effectively

Definitions: Pacesetter Profile Service Indicator Graphic Definitions

Service(s)	Definition
Data, technology, cybersecurity tools & solutions	Any and all internal or client-facing technology assets and data management tools applied to a client solution
Accounting, auditing & risk assurance services	All accounting and auditing services requiring licensing from state and national authorities (in most jurisdictions), including services related to the controls and compliance side of auditing and risk management
Consulting services	All management consulting services which provide expert strategic and operational advice designed to drive significant change in client organizations
Forensics & Disputes	Any investigative services designed to recover evidence concerning misconduct, a crime, or operational failures; with different types of forensic investigations including financial, physical, operational, data & technological, etc., and as well the resolution (e.g., arbitration) of legal disputes
Function-focused advisory services	Non-consulting advisory services such as investment banking, transaction advisory, tax advisory, law practice (separate from legal services), asset management, etc.
Interim, managed & outsourcing services	All short and long-term services by which an external vendor takes over some degree of client functions, whether for reasons of capacity, affordability, temporary stewardship (e.g., interim CFO), monitorship, expertise, etc.
Legal services	Services provided in support of the practice of law, usually high volume, low value work (e.g., contract review), and usually dependent on advanced technology for delivery
Technical	Specialized technical services or competencies such as economic consulting, engineering, valuation, strategic communications, etc.
Brokerage services	Typically insurance brokerage, but includes real estate and etc. brokerage services
Insurance products/ services	Insurance products and services including wealth management, retirement management, etc.

Definitions: Pacesetter Profile Service Indicator Graphic Definitions

Core Criteria	Definition
Internal Living Laboratory	Living laboratory refers to a provider's own internal employee well-being efforts and programs, particularly (but not limited to) those enacted during the pandemic. Most importantly about this category, it is capturing the degree to which a provider has been able to take those lessons learned and transmit them systematically to clients.
Risk & Legal Compliance	This is the most defensive approach which merely seeks to help clients ensure that their employee well-being efforts and projects are in compliance with existing employee and labor laws. This is being applied most commonly in 2022, for instance, in helping clients determine if their efforts to bring employees back into the office are valid, as well as dealing with vaccination controversies.
HR/Rewards/Benefits	This approach can range from the reactive to the proactive depending on the provider, but it is one focused (still) primarily on the HR and benefits delivery models for employee well-being, though some providers have become sophisticated in this approach and connect these programs and efforts to client parties, KPIs and outcomes outside of HR.
Workforce Management	This approach is less concerned with the individual employee issues and more with the impact on the larger client organization, and as such tends to focus on problems (e.g., turnover, productivity, skill gaps, etc.) rather than addressing the full employee experience, taking a more tactical approach to employee well-being.
Holistic/Business Strategy	This approach can begin elsewhere but grounds its approach in the recognition that employee well-being is both influenced by and in turn, influences all value-adding activities in a client organization, requiring therefore a holistic, pan-organizational solution.

About ALM: Who we are

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.

30+	65+	250+	2.65M	2.85M	1.08M
Publications	Events hosted globally	Intelligence reports developed	website visitors per month	Newsletter subscribers	Mobile visitors per month

ALM INTELLIGENCE

PACESETTER
RESEARCH