IDC MarketScape

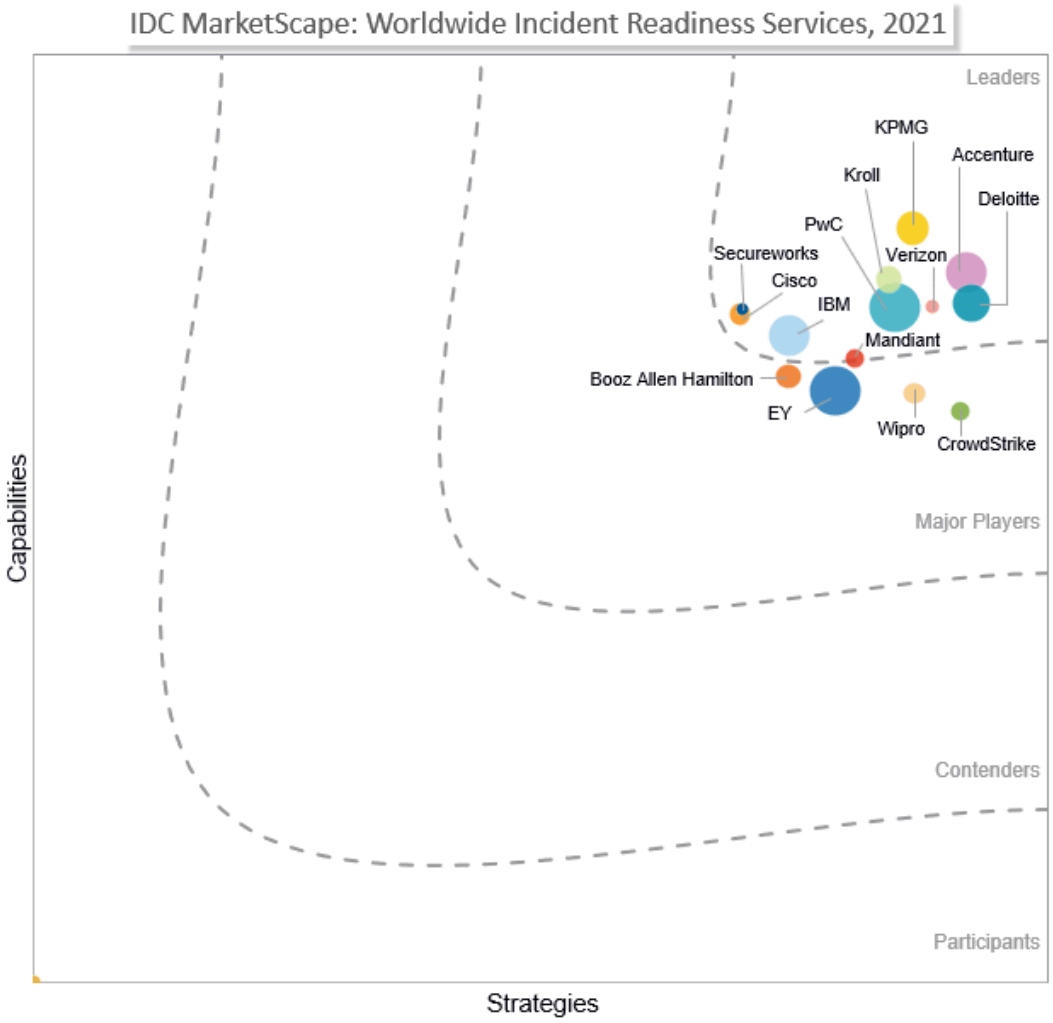
IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment

Craig Robinson Christina Richmond

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Incident Readiness Services Vendor Assessment



Source: IDC, 2021

November 2021, IDC #US46741420

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

News coverage related to the latest cybersecurity attacks is no longer restricted to the technology-related channels that IT and cybersecurity practitioners peruse. The costs to a business' bottom line, to a country's critical infrastructure, or to an individual's ability to obtain life-saving treatment in a hospital due to the proliferation of ransomware and other cyberattacks are becoming huge wake-up calls. These calls are getting the attention of newsrooms, boardrooms, and regulatory bodies across the globe.

Cybersecurity evangelists and analysts historically have debated the merits of where to invest the monetary resources and time needed to combat threats. There are those who make the argument that preventing attacks is paramount, and to a certain extent, they are correct. No one disputes the need to invest in preventing attacks. However, despite ever-increasing amounts of time and money that have been invested in preventing attacks, the cybercriminal gangs and their nation-state supporters prove their resilience in overcoming the defenses. The vicious cycle of attacks landing and ransoms being paid has led to a realization that organizations need to diversify their cybersecurity investments by gaining expertise in responding to the sort of advanced attacks like ransomware that they are likely to see in their environment.

Now it is time to diversify and channel investments into being prepared to respond when attacks land. Organizations need to work with providers that understand the value proposition of shifting to a proactive mindset from a reactive one. The launch or expansion of incident readiness programs symbolizes the logical next step required to elevate a cybersecurity program. The underlying theme for all incident readiness programs is the ability to prepare – and this is the key phrase here – in advance – to make intelligent decisions in a crisis situation to minimize the damage and duration of a cyberattack.

Arguably one of the top tools in a CISO's toolbox is the use of an incident response retainer. The primary use of a retainer is to give security leaders peace of mind. They know that if they have an incident response situation, they do not go to the back of the line. Conversely, they can engage with an incident response provider on an expedited basis to handle the situation.

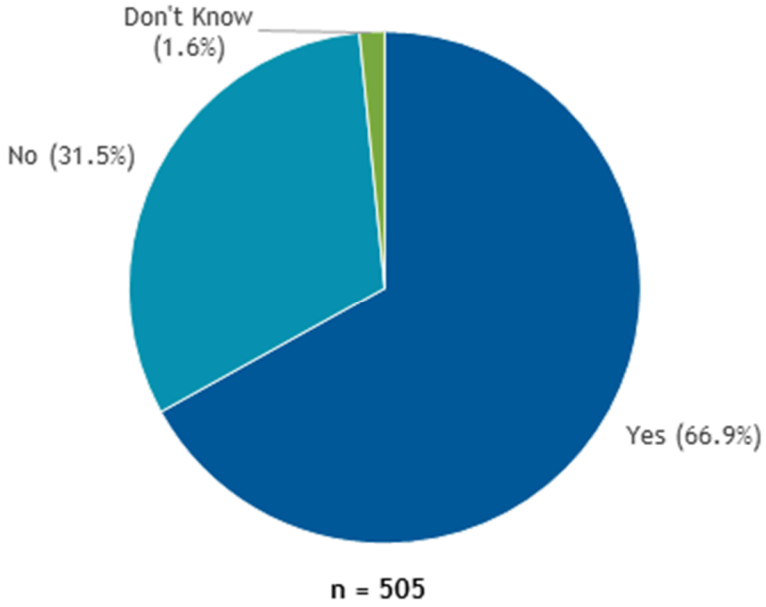
IDC has noted that incident response providers are formalizing the use of these funds to serve dual purposes. One is providing access to the exact types of services that can help minimize the need for or duration of future incident response engagements. The second is funding anticipated incident response engagements.

IDC conducted a survey in June 2021 to survey the customers of the providers that are part of this study. Respondents were surveyed on a variety of topics relating to their consumption of incident readiness services. One of the questions asked in this study is shown in Figure 2. Approximately two-thirds of the respondents who were already utilizing one of the providers in this study for incident readiness services were utilizing an incident response retainer.

FIGURE 2

Incident Readiness Provider Utilizing Firms' Incident Response Retainer Utilization

Q. Do you have an incident response retainer?



Base = respondents who worked with a security services provider in this study

Note: Data is managed by IDC's Quantitative Research Group.

Source: IDC's *Global Incident Readiness Survey,* June 2021

Recognizing that there will be a day when a full-blown incident response team will be required to respond to a ransomware or similar devastating sort of attack, CISOs are starting to make the monetary and time investments in a variety of incident readiness capabilities. In this worldwide IDC MarketScape, IDC researched the various incident readiness services that can enable organizations to be proactive in their capabilities to detect, respond to, and limit the damage from the advanced cyberattacks that too often are making the news headlines.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied 14 organizations that offer incident readiness services across the globe. Evaluated vendors provide global capabilities, and while there are many service providers providing incident readiness services globally, specific services and criteria were required to qualify for this vendor assessment:

- **Revenue:** Vendors with minimum of $25 million in a combination of incident readiness and incident response revenue for 2020 were considered.
- **Geographic presence:** Each vendor was required to have incident readiness capabilities in the North America (NA), EMEA, and APAC regions.

- **Time frame:** The time period studied was 2020–2021 with research ending toward the middle of 2021. It is possible that service providers have enhanced services since that time.
- **Current capabilities include:**
  - Tabletop exercises
  - Cyber-range
  - Vulnerability management
  - Red/blue teams
  - Incident plan and playbook development
  - Technical runbook development
  - Incident response

ADVICE FOR TECHNOLOGY BUYERS

The meaning of *incident readiness* varies by world area, size of organization, and industry. Buyers should discuss their understanding of incident readiness with providers to be sure all parties are on the same page. IDC's *Global Incident Readiness Survey* reveals the top 8 definitions of incident readiness (see Figure 3).

FIGURE 3

Incident Readiness Understanding by Region, Employee Size, and Industry Type

Q. What does "incident readiness" mean to you? (Top 8 mentions)

		Region			Employee Size		Industry			
	Total n = 512	Amer-icas n = 153	EMEA n = 204	APAC n = 155	1,000–4,999 n = 265	5,000+ n = 247	Finance n = 99	Healthcare and life science n = 91	Mfg. n = 76	Services n = 70
We test security policies and controls frequently	**24%**	**22%**	20%	**30%**	**25%**	**22%**	20%	**22%**	**28%**	**23%**
We are fully compliant against all the cybersecurity-related regulations	**22%**	**23%**	**22%**	21%	21%	**23%**	20%	20%	14%	**26%**
We conduct periodic self-assessments to identify and prioritize critical vulnerabilities and risks	21%	**22%**	**21%**	21%	20%	**22%**	**23%**	15%	24%	21%
We subscribe to a threat intelligence platform or threat intelligence data feeds to stay on top of adversary movement	20%	**22%**	20%	18%	**22%**	18%	19%	**26%**	**25%**	17%
We have cyberinsurance or sufficient funds set aside in case of a ransomware attack	19%	**22%**	16%	21%	18%	20%	**21%**	21%	17%	16%
We utilize expert managed security services to keep us from being breached	19%	**22%**	15%	21%	19%	19%	9%	23%	21%	20%
We have developed an incident response playbook	18%	19%	14%	**22%**	20%	15%	12%	18%	22%	20%
We implement security controls and policies across our entire infrastructure	18%	19%	16%	21%	17%	20%	13%	23%	16%	17%

n = 512

Base = all respondents

Notes:

Top 2 mentions in each column are in boldface and underlined.

Multiple responses were allowed.

Source: IDC's *Global Incident Readiness Survey,* June 2021

Further, when asked what incident readiness means to survey participants, the responses make it clear that simply having an incident response retainer in place, having a CISO, or employing security by design is not enough for an organization to consider itself incident ready. Before buyers evaluate providers and services, they should clarify internally what incident readiness means to their organizations. A clear picture of expectations and requirements will help buyers ask the right questions and speed understanding of provider capabilities.

Areas of Incident Readiness in Which Spending Has Increased

Organizations continue to ramp up spending on a variety of incident readiness activities. Some clear choices are emerging: 2 of the top 3 and 3 of the top 5 categories that are forecast to see increases in IDC's *Incident Readiness Survey* include assessments, while the second most likely category to see a boost in spending is security and strategy consulting (see Figure 4).

What do all three categories share?

- They reflect the rapid changes in the use of data and applications, as well as an expanded total attack risk surface that needs to be defended. A common misconception is that data and

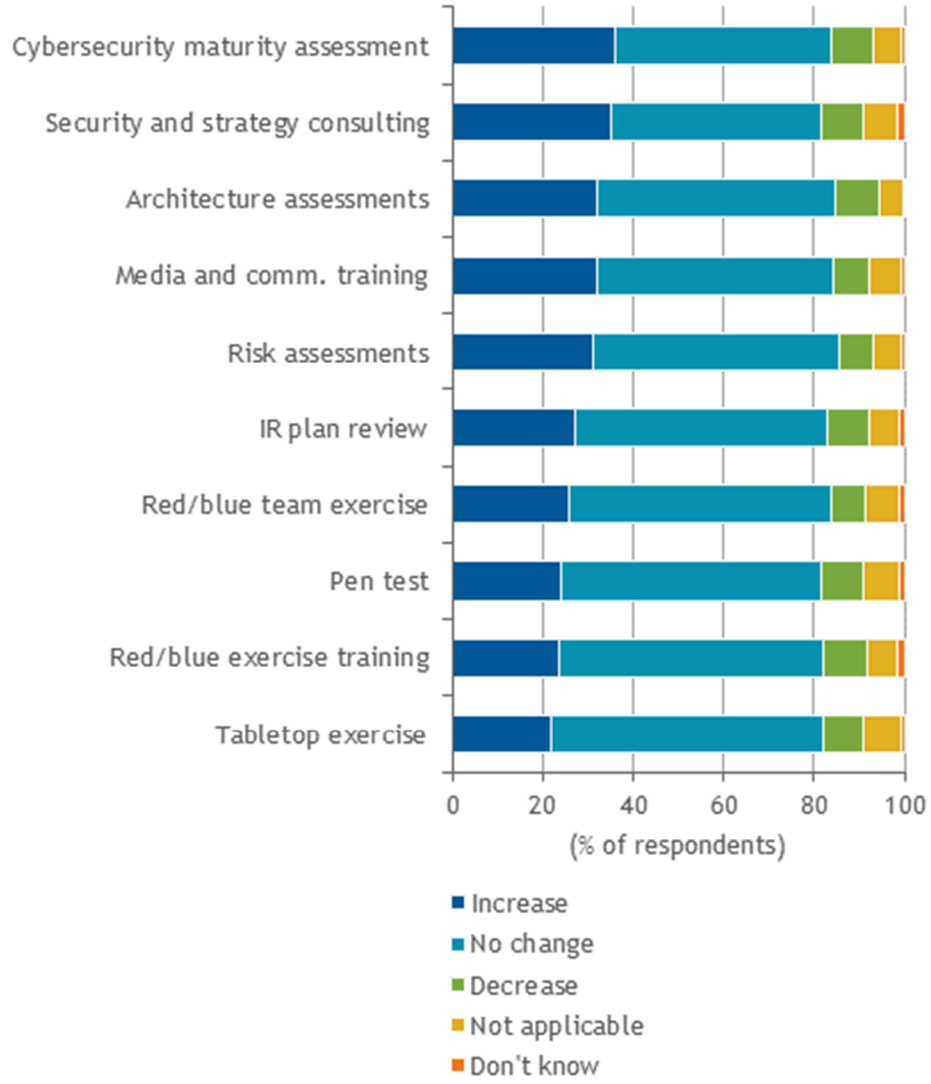
applications have shifted to the cloud. While this is true for many organizations, there still are a lot of legacy data and applications that reside in "classic" on-premises networks. As a result, the total risk attack surface for which CISOs need to prepare response has grown, not shrunk. CISOs recognize they need to realign their security posture to handle the expanded number of vectors where a zero-day attack could land and spread. They are engaging in the appropriate assessments and consulting to be resilient in the face of the expanded risk surface.

A special call out needs to be made to firms that recognize the need for media and communications training. Increased regulatory requirements related to what can and should be shared versus kept in-house are raising awareness of the need to train the voices that share crucial information during crises. Attacks such as the Kaseya ransomware attacks in July 2021 impact not only the original company that was attacked but also companies that are users of its software. Miscommunication or a lack of transparency during an attack can result in delayed reactions and increased costs not only for the "patient-zero" company but also for customers and vendors.

FIGURE 4

Incident Readiness Spending Change Over the Next 12 Months by Categories

Q. *For the following categories, how will your organizations spending change over the next 12 months?*



n = 512

Base = all respondents

Note: Data is managed by IDC's Quantitative Research Group.

Source: IDC's *Global Incident Readiness Survey,* June 2021

In addition, the sections that follow present insights into aspects of incident readiness – tabletop exercises, consulting services, assessments, exercises and testing services, training services, and complementary services – that provide a valuable decision-making context.

Tabletop Exercises

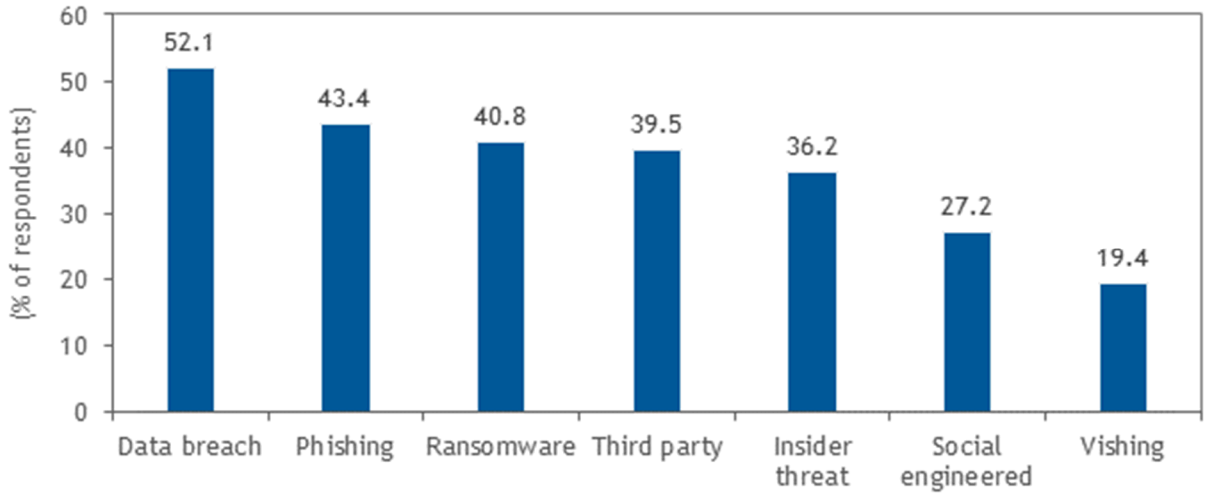
Tabletop exercises are deserving of special attention by buyers of incident readiness services. While Figure 4 does not indicate a spike in increased spending for tabletop exercises, the reader should not misconstrue this to mean they are any less as effective or that they are declining in usage. Tabletop exercises are of value to organizations with relatively low cybersecurity maturity, and they continue to see usage for organizations at the top of the cybersecurity maturity rankings.

Numerous potential attack scenarios can be walked through in a tabletop exercise, as shown in Figure 5. Figure 5 illustrates the attack scenarios that the customers of providers in this IDC MarketScape utilized in their most recent tabletop exercises. While all of these scenarios are worthy of attention, the elephant in the room that is grabbing attention is ransomware. The providers in this study were quick to highlight their capabilities in preparing their clients for the possibility of this nightmare situation.

FIGURE 5

Attack Scenarios Utilized in the Most Recent Tabletop Exercises

Q. Which of the following attack scenarios did you run in your last tabletop exercise?



n = 309

Base = respondents who indicated organization has done tabletop exercises incident readiness activity since beginning of pandemic/next 12-18 months

Notes:

Data is managed by IDC's Quantitative Research Group.

Multiple responses were allowed.

Source: IDC's *Global Incident Readiness Survey,* June 2021

The potential damage that a ransomware attack can inflict is deep and severe. Because of the potential ramifications of any response to a ransomware situation, a large number of departments need to be brought into some of the exercises that an incident readiness provider facilitates. Tabletop exercises are one of the most common incident readiness exercises in which organizations participate. They typically range from one half day to a full day, and participants can be technical, nontechnical, or a mix. The goal is to walk through a scenario, such as a ransomware situation, and simulate the sort of activities, discussions, and decisions that likely would occur. Consider the range of voices that might need to be represented in a ransomware tabletop exercise:

- Chief legal counsel and/or other legal counselors are often engaged in ransomware situations. While not low-cost participants, legal counselors can offer advice in many areas related to the decisions and implications surrounding payment of a ransom. They also may assist with notifications to legal and regulatory bodies.
- Human resources plays a role in employee communications. Internal communication systems could be impaired during a ransomware situation, and human resources representatives need to be prepared to communicate issues to employees using different communication methods than those they might normally use.
- Line-of-business department heads, depending on the industry, need to think about what processes might need to be put into play during a ransomware situation. Think about situations that are in the news (e.g., hospitals trying to track down patient information when they do not have access to electronic patient records). Consider how warehouses can receive shipments when they do not have access to electronic manifests.
- The impact of good corporate public relations on a public ransomware situation cannot be overstated. A company's high-profile situation can have an impact on a local or national economy, and a tabletop exercise is the perfect time to think about the materials that should be prepared in advance of a crisis situation.
- IT teams often are the first human line of defense to be deployed. Their roles need to be properly defined to make sure that forensic evidence is not accidentally destroyed. They are also key players in response and remediation efforts needed to bring systems back to a normal status.
- The C-suite and the board are involved in ransomware situations. While their participation may be difficult to obtain on a regular basis, their roles need to be defined and represented. When possible, these stakeholders need to be encouraged to participate in at least one tabletop exercise annually to stay current on their roles and responsibilities.

Consulting Services

The strategies and tactics that organizations utilize to increase their incident readiness maturity often require the use of providers that can give them the guidance and knowledge that they may not readily possess:

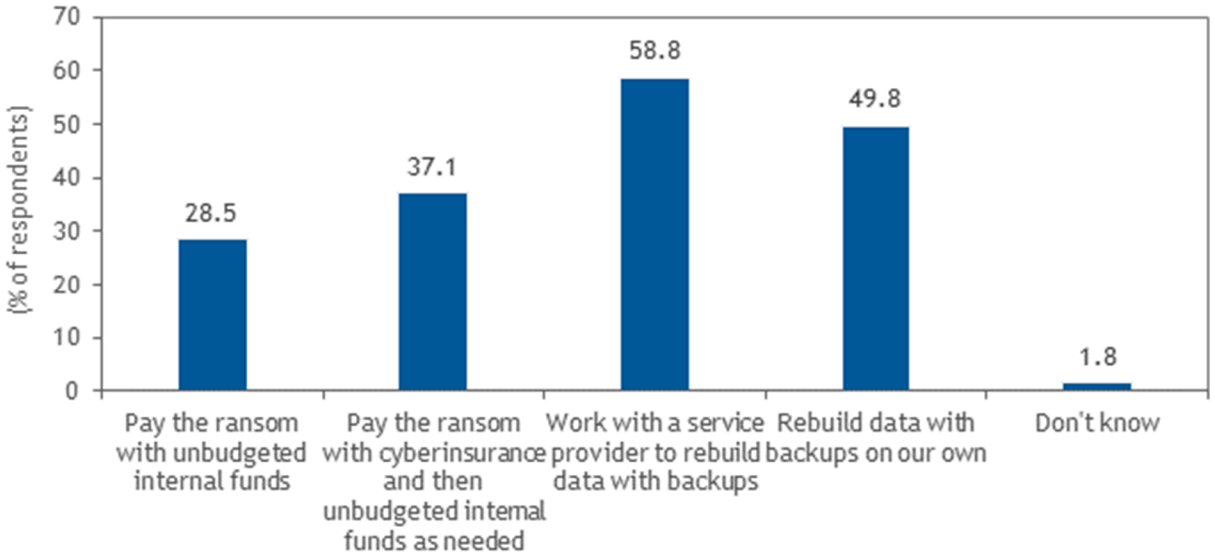
- When the topic of ransomware is raised, a common follow-up topic is the possibility of transferring some of this risk through the purchase of cyberinsurance. The rise of the cyberinsurance market is certainly getting a boost by CISOs, chief risk officers, and other C-suite members who wish to mitigate the cost of a potential ransomware situation. Figure 6 shows that many organizations see a role for cyberinsurance to pay either all or part of the cost of a ransom, and/or forensic, remediation, and potential regulatory costs associated with the incident.

- Data may be recovered through the payment of a ransom or through the use of backups. Regardless, it's a wise decision to use an incident readiness provider to assist in the planning of a wholesale backup recovery option or to gauge the amount of coverage required in a cyberinsurance policy.
- Assistance in the creation and ongoing testing and updating of incident response playbooks and runbooks is a widely used service. Changing business conditions and strategies, as well as ever-evolving IT architectures, require regular document review and updating. Incident readiness providers can help organizations apply best practices to these important documents. In "live-fire" situations, organizations can feel more confident that the planning that went into these scenario-based documents involved multiple sets of eyes. Consider using incident readiness providers that can take already-developed industry-specific playbooks and tailor them to other organizations' unique needs.

FIGURE 6

Potential Ransomware Situation Dealing Preferences

Q. If dealing with a widespread ransomware attack that significantly hampers our operations, our firm would most likely:



n = 512

Base = all respondents

Notes:

Data is managed by IDC's Quantitative Research Group.

Multiple responses were allowed.

Source: IDC's *Global Incident Readiness Survey,* June 2021

Assessments

Assessments are a way of sizing up the risks, threats, and capabilities that an organization faces. When incident readiness providers conduct assessments, the providers gain greater insider knowledge of an organization's cybersecurity posture. This helps give their guidance contextual perspective as incident readiness plans are developed and matured:

- The common theme of being prepared to tackle a potential ransomware situation continues, as providers recognize the need for organizations to walk through the steps needed to prevent and, as needed, limit the size and scope of a potential ransomware situation. Buyers should look for prepackaged ransomware readiness assessments and consider acquiring the valuable guidance that providers can add to their institutional knowledge.
- Cybersecurity maturity assessments are often a first step in establishing a cybersecurity program. Potential gaps are identified, and realistic road maps are designed that are appropriate for an organization based on its size, industry, and risk tolerance. A maturity assessment is a great document to keep around for presentations to the board and other C-suite members to highlight a CISO's long-term strategy for maturing a cybersecurity program.
- A compromise assessment is a good introduction to a relationship with an incident readiness provider. The holistic view of an organization's current and historic incident history is invaluable. Consider looking for providers that combine this assessment with a review of current security controls, security architecture, and vulnerabilities.

Exercise and Testing Services

Testing activities offered by incident readiness providers help gauge the capabilities of an organization's systems, processes, and people to withstand attacks from various potential vectors. Just as important, these exercises can put technical and line-of-business associates in a frame of mind that allows them to immerse themselves in simulations. They can play out the activities they might need to carry out during an incident response situation:

- **Red/blue/purple team exercises.** Differing opinions surround the order of these exercises in an organization's cybersecurity maturity journey. Some argue that having the purple team exercise first is more like an open book exam, with both red and blue teams providing visibility into the opposition's tactics. Others argue that a classic red/blue team exercise(s) should be run before diving into a purple team exercise. IDC doesn't state a preference for the order but instead argues that all of these exercises are valuable.
- **Cyber-range.** A misperception exists that a cyber-range exercise is the exclusive domain of the uber technical cybersecurity practitioners that inhabit security operations centers (SOCs). This is not necessarily true. Many incident readiness providers now incorporate scenarios into cyber-range exercises that help legal, communications, and other executive team members gain valuable insights and knowledge from these immersive exercises. The collaborative capabilities of an organization's leadership team can also be observed and enhanced so that when and if a true crisis situation gets played out, the personas involved will demonstrate greater confidence in critical decisions because they have previously been tested. Buyers will want to make sure that providers include all relevant personnel in their cyber-range exercises.
- **Breach and attack.** The use of point-in-time tests such as penetration testing or red team exercises to gauge an organization's ability to detect and stop attacks is valuable. Unfortunately, these tests suffer from gaps in time between their use. Organizations that are looking for continuous testing capabilities to assess the efficacy of their security controls are increasingly utilizing breach and attack simulation tools. These tools are gaining traction with

incident readiness providers as another service that can on a more regular basis quickly identify issues with their clients' security capabilities.

Incident Readiness Training Services

For well over a decade, the common theme of security evangelists has been the lack of trained bodies to fill roles. One of the antidotes to this issue is the need for current cybersecurity practitioners to gain deeper, best practices knowledge of their craft while enticing other industry domains to widen their scope of knowledge to include cybersecurity capabilities.

Figure 7 illustrates the training services and future planned training needs that incident readiness firms are likely to fill. The rising importance of clear communications to internal and external stakeholders and the media highlights the top tier that media and communications training has entered.

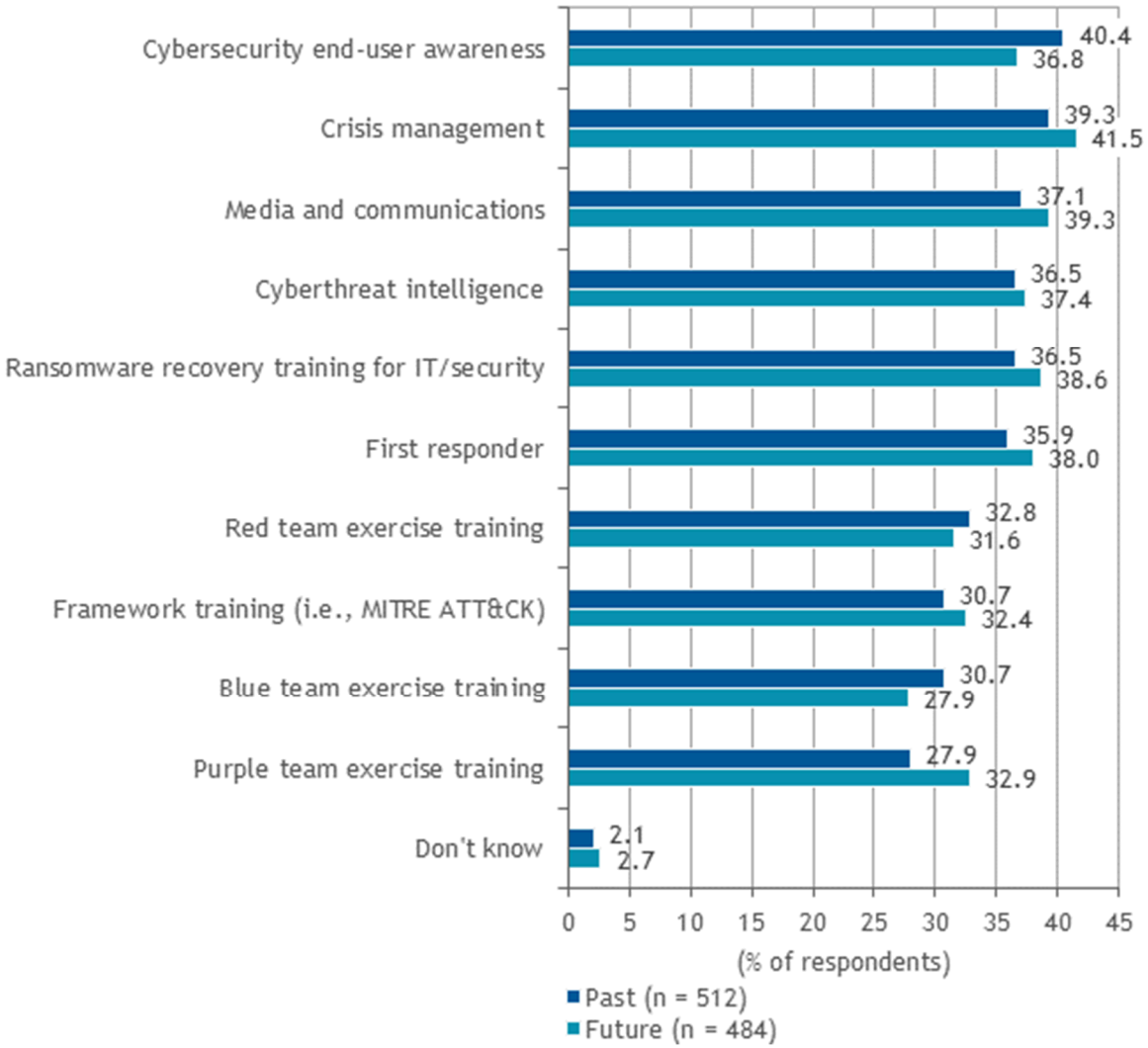
Plans to gain training in crisis management are due in part to the high stress levels endured by organizations during a ransomware situation. It is imperative that key employees develop the soft skills that crisis management training can provide during a ransomware or other high-stress cyberevent prior to these skills actually being used during a live-fire incident.

Buyers should look for incident readiness providers that have off-the-shelf training that can be tailored to their unique needs. IDC noted during this study that ad hoc training occurs while consuming incident readiness services, but a formal training program for the personas involved in incident response situations is a logical next step in elevating an organization's overall incident readiness capabilities.

FIGURE 7

Top of Mind Training Services and Future Planned Training Needs

Q. In the past 12-18 months, has your organization trained, or in the next 12 months, does it plan to train internal incident responders in any of the following areas?



Base = all respondents

Notes:

Data is managed by IDC's Quantitative Research Group.

Multiple responses were allowed.

Source: IDC's *Global Incident Readiness Survey,* June 2021

Complementary Services

Other capabilities that incident readiness providers are likely to deliver can raise the overall incident readiness capabilities of organizations:

- Asset discovery capabilities for IT, OT, IoT, and other devices help increase awareness of the actual assets that are potentially at risk of damage or destruction during an attack. Knowledge of what needs to be protected should precede the strategies to protect them.
- Use of threat intelligence to match up the threat actors and the techniques, tactics, and procedures (TTPs) they use to attack organizations can be a game-changing capability. Knowledge of how threat actors act normally can give CISOs the visibility and road map to deploy defensive capabilities that raise their overall incident readiness maturity.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Accenture

Accenture is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide incident readiness services.

Accenture states that it helps its clients answer three core incident readiness questions: "Are you prepared to respond? Are your defenses effective? Is your business resilient?"

Accenture's incident readiness capabilities include incident response planning and playbook development, as well as tailored tabletop exercises to test the capabilities of a client's security, crisis management, and resilience capabilities. Cyber-range exercises are used to train Accenture's internal team as well as clients' teams.

Accenture's Ransomware Readiness service assesses the potential impact of a ransomware attack and identifies opportunities to bolster detection, prevention, response, and recovery. Conducted via interactive discovery workshops and simulation exercises, the service helps identify how an organization restores and recovers from a ransomware attack and provides recommendations to mitigate risks.

Threat and vulnerability management, vulnerability scanning, penetration testing, and advanced adversary simulation services, as well as red, blue, and purple team exercises are all key features of Accenture's incident readiness portfolio. These services all focus on the capabilities and potential weaknesses of clients' security postures and in particular on the objectives that are the most important to each business.

An example of an Accenture investment in incident readiness is the development of the CyTwin cyber digital twin platform by Accenture Labs. The platform gathers information from a client network and builds a virtual "twin" of the environment. Information about potential attackers and the tactics that they utilize as ascertained from the MITRE ATT&CK framework are used to predict possible paths that an attacker might take through the network. CyTwin enables clients to see what an attacker might do and

consider the weighted probabilities of different paths to determine where to most effectively apply security investments.

In addition, Accenture offers focused readiness assessments for cloud, operational technology (OT) and industrial control system (ICS) environments, mergers and acquisition targets, and insider threat.

Strengths

Accenture differentiates itself with investments that added human capital and intellectual property (IP). Acquisitions of FusionX, Maglan, iDefense, Deja vu Security, Revolutionary Security, Context IS, and Symantec CSS exemplify how Accenture Security has acquired capabilities, brands, solutions, and experienced practitioners.

The company's experience in complex and business-critical investigations and exposure to intelligence and threats across critical infrastructure inform readiness services. Technical expertise and in-depth knowledge help clients understand the adversary and assess their capability to prepare and respond to cyberincidents.

One customer noted the longevity of the Accenture team that interacts with the customer and described the relationship as more partner than a vendor.

Challenges

Accenture should consider offering additional pricing options such as an outcome-based price for incident readiness offerings.

One client reported confusion related to Accenture's long-term strategy in the incident readiness space.

Consider Accenture When

Large multinational organizations looking for an incident readiness provider with strong industry knowledge in multiple disciplines and a global presence should consider Accenture.

Booz Allen Hamilton

Booz Allen Hamilton is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide incident readiness services.

Booz Allen Hamilton's proactive incident response capabilities include breach readiness assessment, compromise assessment, technical war gaming, executive tabletop exercises, incident response plan development, incident response playbook/runbook development, and incident management plan development.

The breach readiness assessment kicks off Booz Allen Hamilton's prepaid retainers. This assessment measures how well a client can detect and respond to a major breach. Two versions of a custom framework, which go beyond the NIST CSF framework, look at a client's technology, expertise, associations, and mechanics:

- An initial two-week fixed fee "light" engagement generates a view of a client's current strengths and challenges after which a client receives prioritized, sequenced recommendations.
- A "full" version typically takes 8–10 weeks and layers on review of vendor agreements, technology stack recommendations, and staff training agreements.

Booz Allen Hamilton's cyber war game, BREACHED!, includes traditional players and the C-suite in the simulation. Participants in the half-day engagement are focused on developing a strategic understanding of response considerations and the operational trade-offs of managing an enterprisewide cyberattack. Issues and decisions that impact strategic communications, regulatory compliance, external engagements, third-party risks and liabilities, and other considerations are fleshed out and provide participants with an expanded perspective on areas that could and likely will be touched upon during an incident response situation.

Strengths

Booz Allen Hamilton's exercise and testing capabilities (red/blue team exercises, tabletop exercises, cyber-range, etc.) compared favorably with other firms in the market.

Organizations that are prone to nation-state sponsored attacks may appreciate Booz Allen Hamilton's accreditation by the NSA and the company's ability to be a life-cycle provider of incident readiness capabilities and incident response capabilities in crisis situations.

Booz Allen possesses deep expertise in ransomware including threat intelligence, digital forensics, breach coaching, and negotiations services to better enable organizations to effectively minimize data loss and business impact.

Challenges

Booz Allen Hamilton's historic strengths are associated with governmental bodies. Comparable success in its commercial practice may require escalation, investment, and the right marketing mix.

Booz Allen Hamilton currently does not have a formal way to measure customer satisfaction, although there are plans in the road map to do this.

Consider Booz Allen Hamilton When

Organizations with critical infrastructure, governmental bodies, and firms that need broad resilience capabilities should consider Booz Allen Hamilton.

Cisco

Cisco is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide incident readiness services.

Cisco offers tabletop exercises in three ways. The Traditional tabletop exercise provides a baseline performance of new incident readiness plans, and it is also beneficial for teams that are new to incident response. The Simulated tabletop exercise is more technical, and it involves either paper-based or electronic-based evidence created to test the technical team in its simulated investigation. The Gamification tabletop exercises is similar to the Traditional version, but it differs by adding an element of chance.

Cisco's Talos incident response retainer offers 10 services that help prepare clients to detect and respond to cybercrises. These services assist with the creation and updating of incident response plans and playbooks. Readiness assessments and tabletop exercises gauge how well prepared a client is to respond to an incident. Compromise assessments determine if a client is compromised, and/or they conduct proactive threat hunts to detect potential compromises.

The Cisco Talos Incident Response (CTIR) Intel on Demand service offers clients insights into specific tactics, techniques, and procedures of common attacks that a firm might face based on its specific industry and geographical location. Purple team engagements validate the detection capabilities of the defending blue teams that face a simulated cyberassault from a red team.

Cyber-range training helps build skills needed to defend against advanced cyberthreats. A standard three-day program created by incident response professionals follows a crawl-walk-run methodology that begins with student instruction on the first day. Students progress by the last day to a full cyber-range experience.

Strengths

Cisco provides estimates of the per-engagement work hours required from Cisco and from a client to achieve a desired outcome.

The recent integration of Cisco's incident readiness and response capabilities into the Cisco Talos offering augments the portfolio with offerings such as the virtual cyber-range, Intel on Demand, and the deep and dark web scanning.

One client noted the speed of response to a ransomware incident on a weekend after multinational Cisco professionals arrived onsite within 24 hours.

Challenges

Backup-as-a-service (BaaS) and/or disaster recovery-as-a-service (DRaaS) capability could round out Cisco's portfolio.

Cisco would benefit by fine-tuning its marketing messages for its top industry verticals.

Consider Cisco When

Organizations that seek to have a strong threat intelligence capability and a flexible incident retainer portfolio of services should consider Cisco.

CrowdStrike

CrowdStrike is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide incident readiness services.

CrowdStrike's incident readiness program helps organizations answer two core questions: Am I mature, and am I ready? Maturity is assessed by offerings that gauge the processes, procedures, and capabilities of clients' security programs including a cybersecurity maturity assessment, cloud security assessment, Active Directory security assessment, SOC assessment, IT hygiene assessment, security program in-depth assessment, and a cybersecurity enhancement program.

Readiness is addressed by testing services that gauge clients' ability to prevent, detect, and respond to attacks through tabletop exercises, live-fire exercises, adversary emulation exercises (similar to a black box penetration test), red/blue team exercises, and penetration testing. The red/blue team exercises were expanded recently to include cloud-based attack scenarios.

While most engagements are delivered entirely through CrowdStrike resources, CrowdStrike also leverages a network of trusted partners to offer customers unique offerings that can be delivered off the CrowdStrike catalog or directly with the partner. One such partner program is the Active Directory

(cloud and Office 365) security assessment that provides a prescriptive assessment of a customer's environment.

The firm's incident readiness professionals leverage the CrowdStrike Falcon platform across several offerings to get the latest threat data and insights to pinpoint what threats may be already present in a client environment at the start of an engagement. Falcon also allows CrowdStrike to pull hygiene and other supplemental information to inform the assessments and tests, augmenting traditional documentation and interview-based inputs.

Two half-day onboarding sessions are offered for new retainer clients. The personnel assigned to these sessions include incident response experts who provide recommendations, a customer experience/project manager, and a technology deployment expert. The output of the sessions proactively gives a client and the CrowdStrike team the information that is needed in the event of an incident response engagement.

CrowdStrike's CrowdExchange is a customer-to-customer program that allows customers to exchange relevant information, experiences, and insights, and it presents reward and recognition opportunities.

Strengths

The joint retainer between Dragos and CrowdStrike for IoT/OT incident readiness and response is a unique offering that allows CrowdStrike's customers to gain access to expertise in hard-to-find domains. In addition, CrowdStrike maintains a dedicated cloud-focused incident response team, which continues to be a primary attack landscape for many of the most recent cyberattacks seen.

One client noted a good feeling because the CrowdStrike people working on the account have the client's best interests in mind from sales through post-sales.

Challenges

CrowdStrike has focused its in-house services on larger and more strategic offerings in North America while only offering more tactical offerings like playbook development in other geographies. It augments this more narrowly focused scope of services in North America through its aforementioned partnership program.

CrowdStrike recognizes that some of its back-end processes will require more automation to allow them to continue to grow at the scale that it has previously shown.

Consider CrowdStrike When

Organizations of all sizes looking to partner with an incident readiness provider with a variety of managed and professional service capabilities and a range of technology partners should consider CrowdStrike.

Deloitte

Deloitte is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide incident readiness services.

Deloitte's approach to improving client preparedness to respond to and recover from a major cyberevent is a tailored program focused on the five areas of strategy, governance, technology, training, and exercising and testing. The preferred engagement begins with strategy that encompasses

incident readiness capability and maturity assessments, incident response strategy and transformation, and cybersecurity strategy.

Deloitte invests significantly in its own technology and IP. Crisis Hub is an example. It is an out-of-band network tool that is licensed to clients whose primary network is unavailable due to a ransomware event or other incident. The tool allows secure user communications and access to playbooks, runbooks, and incident response processes.

The ransomware readiness program encompasses steps of assess, plan, and prepare to help clients manage high-severity ransomware incidents by focusing on people, processes, and technology. Examples of people-focused questions include: Are roles and responsibilities of the cyberincident response team defined, documented, and understood? Are people trained and tested to perform during a ransomware incident? Process components include documentation, review, and approval of incident response procedures and playbooks, as well as clear escalation pathways and a defined and documented procedure to handle post-incident investigations. Technology components include the procurement of digital forensic technology and a secure backup solution deployed for business continuity and recovery purposes.

Deloitte also developed an online virtual lab environment, Hackazon, that offers challenge-based learning activities. This gamified learning experience enables security professionals to improve their technical cyberskills based on the latest cyberdevelopments and recent attacks. The environment is delivered as a service, which enables Deloitte to provide incident readiness training services at scale, with scenarios customized by client and industry.

Deloitte has programs for training media and communications associates to be able to communicate proper messages during an incident response situation with all relevant stakeholders.

Strengths

Deloitte's global network of responders allows the company to deliver end-to-end response services to its clients, and then seamlessly integrate its experiences into readiness services using those very same responders to add much needed realism.

Deloitte has flexible, innovative pricing models that go beyond hourly pricing models and often can be tailored to meet clients' needs.

One client noted that a ransomware-focused tabletop exercise "hit it out of the park" with realistic videos showing what the media coverage might look like during a ransomware incident.

Challenges

Clients looking for low-cost, small-scale incident readiness services would not be best suited for Deloitte.

In addition, some clients may not be able to engage Deloitte due to the firm's audit independence restrictions.

Consider Deloitte When

Midsize to large global enterprises looking for incident readiness capabilities that can be tailored to their specific needs should consider Deloitte.

EY

EY is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide incident readiness services.

The firm takes a holistic approach to developing incident response plans that are designed to increase the collaboration among security, IT, line-of-business groups, and executive teams.

EY states that its roots in business consulting influence its incident readiness engagements. A typical engagement might start with a kickoff meeting to review existing incident response materials, interviews with key business personnel to identify key business processes and high-value assets, and scoping an appropriate incident response simulation exercise based on a specific scenario such as ransomware, data exfiltration, or social engineering threat.

Three levels of an incident response retainer (silver, gold, and platinum) offer options such as remote or onsite SLA response times, playbook maintenance and testing, and access to client-specific situational awareness updates. Additional incident response services can be purchased individually or utilized via unused incident retainer hours. Tabletop exercises, first responder training, red and purple team exercises, and other services are available.

EY's partnership with AttackIQ, a breach and attack simulation (BAS) vendor, enables a threat-informed defense across a client's organization. AttackIQ leverages the MITRE ATT&CK framework and emulates tactics, techniques, and procedures to exercise host-based security controls in the same way an adversary does.

The Ransomware Readiness and Resilience service deliverables include a report that describes several findings. These include the results of a ransomware simulation, optimized tool configuration, enhanced endpoint detection and response (EDR) rules, updated firewall and network configuration, an inventory of priority assets for backup and protection including specific IT recovery actions and updated standard operating procedures (SOPs), and playbooks focused on ransomware threats.

Strengths

EY's proficiency in providing cybersimulations that engage board members of the company's clients is a compelling offer.

Multiple clients noted the ability of EY to help them with crisis communications plans. One client commented on EY's ability to change assessments and simulations to match the particular geographic needs of a large multinational firm.

Challenges

EY should consider adding a formal training program to upskill clients' personnel, rather than relying on ad hoc training.

Consider EY When

Large global organizations looking for a firm to elevate an existing incident readiness program to prepare for current or future advanced threats should consider utilizing EY.

IBM

IBM is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide incident readiness services.

IBM's X-Force incident response team provides a suite of incident readiness services that can be consumed on a standalone basis or through an incident response retainer. Core capabilities center on consulting and assessments, testing, exercise engagements, and training.

IBM states that its cybersecurity incident response planning services help its clients better respond to cyberincidents and cyberattacks. IBM's planning services can be tailored to meet clients' specific needs such as by providing incident response program assessments, ransomware readiness assessments, incident response, and crisis management playbooks that define the roles and responsibilities in an organization that have to be applied during a cyberincident. IBM provides immersive attack simulation exercises that allow organizations to test and improve on their plans/playbooks.

First responder training focuses on the critical data that is needed to determine the root cause of an incident — data that could be lost or destroyed prior to the arrival of the forensic incident response team. A two-day workshop covers topics such as collecting images of live systems that cannot be shut down, creating a proper chain of custody, and collecting volatile data such as memory, network connections, and system settings.

IBM's active threat assessment services review a client's current defenses and seek undetected threats. This involves a potential combination of an analysis of historical network logs, network traffic, threat intelligence–led threat hunting, and endpoint metadata.

IBM has three different levels of application penetration testing for testing web, mobile, terminal, client-server, mainframe, and middleware platforms. Additional network penetration testing services are available that focus on exploiting identified vulnerabilities on both internal and externally facing systems.

Strengths

Training and preparedness are led by a team of responders, backed by years of research and consultancy. IBM plans to have at least two associates per region who are specialists in the nuances of incident response for OT.

Security Command Centers in Cambridge, Massachusetts, and Atlanta, Georgia, and in Europe use the latest threat intelligence to simulate cyberattacks for clients based on industry and needs. Participating security personnel test how well participants work together to respond in a simulated crisis situation.

Challenges

Currently, client satisfaction is measured using only NPS scores.

IBM's strategy to remain competitive from a pricing perspective is not clear.

Consider IBM When

Large firms that prefer to work with a global partner that offers a suite of security testing, training, and incident readiness consulting should consider IBM.

KPMG

KPMG is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide incident readiness services.

KPMG takes a comprehensive approach to cyberincidents through its integrated cyberpractice. Incident readiness services include cyberstrategy and planning, security configuration and monitoring, security controls testing, and business and technical simulations. KPMG Incident Response includes digital forensics, case and incident tracking, data analytics and source log analysis, disaster recovery, remediation, and business improvement.

KPMG also acts as a cyberinsurance coordinator. Participation in cyberinsurance carrier panels helps the incident readiness team walk their clients through the process of figuring out what they have at risk and how they can procure the proper amount of cyberinsurance. KPMG also works with carriers to determine risk for individual policy holders as well as monitoring dark web activity for indications of pre-ransomware activity.

The company's cyber-ranges provide exercises for clients to train and test their response capabilities — from the executive team to technical, security, and incident response teams. For example, basic tabletop exercises can focus on a single scenario. Time-sliced tabletop exercises involve separate meetings of the crisis/incident management teams to simulate extended crisis periods. Live exercises can play out with actors standing in for external stakeholders that often are engaged in crisis situations.

Globally available, cloud-enabled digital twin platforms provide virtual OT, IoT, and IIoT environments that can mimic 17 industry-specific processes suitable for client environments such as oil and gas refineries, cities, airports, and trains. Physical labs in Germany, Argentina, Abu Dhabi, United Kingdom, and India and soon to be opened in the United States can physically replicate portions of environments to give clients an immersive opportunity to walk through, test, and refine incident response playbooks.

Strengths

KPMG invests significant nonchargeable amounts of its own time in onboarding new incident retainer clients and zero-dollar retainer clients (basically a time and material agreement). This approach aligns KPMG and new clients on the client's environment and SOC, includes a review of the existing incident response plan, identifies augmentation requirements, and explores other needs.

If a company decides to put in a retainer and those funds that are not used during a contract period, those funds can be used for the next contract period for a variety of advisory and training services. Client terms are flexible, but typical arrangements are for clients to use the funds within the first 60 days of the next contract period.

Challenges

One client noted a lot of turnover on the KPMG team assigned to the client organization.

At the time of this study, while KPMG does provide red/blue/purple testing/teaming exercises and industry accreditation testing (TIER, CBEST, etc.), it does not provide breach and attack simulation capabilities directly (as defined by IDC) but would work with partners to deliver and are investing to expand these capabilities in specific geographies like the United Kingdom and China.

Consider KPMG When

Firms of all sizes that desire to work with a global incident readiness provider with strong digital forensic capabilities should consider KPMG.

Kroll

Kroll is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide incident readiness services.

Kroll's portfolio of incident readiness testing and assessment capabilities include risk assessments and analysis, network and cloud security assessments, penetration testing, physical security assessments, vulnerability assessments, web application testing, and policy assessment and design. More recent assessments include a ransomware preparedness assessment and a remote work security assessment.

Kroll's historic investigatory and forensic capabilities that benefit incident response engagements have expanded by "shifting left" to include incident readiness capabilities. Notable capabilities include the Cyber Risk Retainer, which gives clients the flexibility to incorporate preparedness, response, and notification services; Kroll CyberClarity360, which assesses the cyber-risk of third-party suppliers; data-mapping and asset inventory exercises; and the Data Protection Officer consultancy service.

One way in which the company scaled up its incident readiness offerings was to develop a tool that provides real-time remote collaboration during certain aspects of assessment engagements. The tool automates, scales, and standardizes the process of ingesting information and creating reports.

Pricing models are flexible and include flat fee and phased engagement pricing. Discounts on incident readiness services are available to organizations that buy an incident response retainer and to organizations with policies underwritten by over 60 Kroll cyberinsurance partners worldwide.

Kroll conducts human-led penetration tests to examine different aspects of clients' environments and to identify legitimate activity versus cyberpredator activity. The company also delivers automated cybertesting services using the proprietary FAST Attack Simulations platform, which delivers customized simulations that mimic likely attackers.

Strengths

Kroll handles more than 2,700 incidents annually, and the related experience and insights are fed into incident readiness services.

Clients can take advantage of regulatory and legal knowledge to inform cyberdecisions.

Kroll clients praised the company's assessment capabilities in areas of risk, network architecture, and vulnerabilities.

A critical infrastructure client noted that Kroll is a "trusted advisor" for cybersecurity planning.

Challenges

Additional channel partners could support growth beyond Kroll's current inroads into the legal community and cyberinsurance providers.

Limited methods of collecting customer feedback may not provide Kroll with adequate information on customer satisfaction.

Kroll will be challenged to secure the talent that it needs to continue to grow its business. It currently has plans to hire more than 100 additional staff worldwide over the next year.

Consider Kroll When

Organizations of all sizes that value an incident readiness provider with deep forensic capabilities, and strong regulatory and legal capabilities, should consider utilizing Kroll.

Mandiant

Mandiant is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide incident readiness services.

The evaluation of Mandiant was done prior to the June 3, 2021, announcement of the separation of the Mandiant offerings from FireEye.

Mandiant organizes its incident readiness solutions into four pillars: assess, transform, defend, and train.

The assess pillar evaluates clients' ability to prevent, detect, and respond to cyberthreats. Services include a compromise assessment, red team, purple team, penetration testing, tabletop exercises, cloud architecture assessment, remote security assessment, ransomware defense assessment, and response readiness assessments.

Transform actions center on helping clients design, build, or improve key functions such as threat detection, containment, and remediation capabilities. The company provides hands-on support to implement critical changes and best practices for functional/staff readiness.

Mandiant's threat intelligence capabilities as well as the company's managed detection and response service are key pieces of its defend pillar.

Train pillar offerings teach clients how to execute the right processes and technologies through instructor-led learnings and hands-on scenario gameplay based on real-world investigations, not theoretical scenarios. Courses include enterprise incident response, malware analysis, network investigations, and forensic analysis. All courses can be delivered remotely.

The ThreatSpace cyber-range is an immersive, virtual environment that enables Mandiant to test a security team's ability to protect, detect, and respond. Participants are coached to apply proven capabilities, processes, and procedures to improve overall security effectiveness and capabilities.

Strengths

Mandiant Threat Intelligence provides proactive guidance that helps clients understand the current threat landscape and its potential impacts.

One client noted that after completing a tabletop exercise, it was obvious that the Mandiant team had "done the homework, was fully prepared, and understood the mission."

Challenges

A client commented that sign-in to the website brings up all Mandiant portals and navigating among them is confusing unless one spends a lot of time in the system.

Because of limited vendor agnosticism, the company works with clients by relying extensively on client tools.

Consider Mandiant When

Organizations looking for a provider with a global footprint, threat intelligence, assessment capabilities, and the ability to strengthen client capabilities through training should consider Mandiant.

PwC

PwC is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide incident readiness services.

PwC's holistic view of incident readiness recognizes that resiliency across four strategic pillars is key to elevating clients' incident readiness maturity. The four pillars are technology and operational resilience, workforce resilience, financial resilience, and data resilience.

As organizations increasingly utilize simulations to stress test different readiness scenarios, the order in which these scenarios and teams are tested matters. PwC believes that testing technical teams first allows the lessons learned to be applied to simulation exercises on crisis response, for example, with line-of-business leaders.

To help answer questions that its clients' board members might have (e.g., "How do you know we are ready" or "What is happening in our industry vertical?"), PwC provides threat intelligence, modeling, and threat profiling services. These services enable clients to understand the threats most relevant to individual clients and tailor their readiness and response plans to specific threat actors and associated TTPs.

The company's incident response, readiness, and resilience (IR3) assessment helps address a client's gap in modeling, detection, and response capabilities. Specifically, it can pinpoint why an organization may not be prepared to recover critical business services supported by databases, applications, interfaces, Active Directory, or other technology assets in the event of a ransomware event.

For its retainer services, PwC conducts a baseline capabilities assessment after a client establishes a retainer relationship. This activity supports mutual understanding of a client's people, processes, and technologies used in incident response situations. The assessment is followed by an intelligence-led risk-based threat assessment, executive/technical tabletop exercises, and a compromise assessment that gathers and analyzes evidence from log files, endpoints, and network traffic to uncover previously hidden cyberattacks.

Strengths

Cyber-readiness is at that heart of PwC's global Cyber, Risk and Regulatory practice. PwC utilizes its existing partnerships and relationships with the C-suite and the board to further the visibility and elevation of its clients' incident readiness capabilities and its global threat intelligence to target areas to improve cyber-readiness. In addition to client delivery teams, PwC operates a Cyber Innovation Center and allows clients to access these centers of excellence for hands-on knowledge that can further inform readiness assessments and testing.

Clients can also tap this expertise to support assessments and testing of industrial control systems and other operational technology.

Challenges

Although PwC does not participate in specific insurance panels currently, it should continue to evaluate the benefits of pursuing this area for development and growth.

PwC might benefit by creating formal partnerships with firms that can provide BaaS or DRaaS capabilities.

PwC should consider utilizing more ways of measuring its pricing strategies to make sure that the firm is properly pricing its incident readiness portfolio.

Consider PwC When

Large global organizations that desire to work with a firm that can provide expertise beyond incident readiness, and that has capabilities in areas of increasing importance like OT or IoT, should consider PwC.

Secureworks

Secureworks is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide incident readiness services.

Secureworks' incident readiness programs consist of a life cycle of planning and organizing, training and exercises, and evaluating and improving. The plan and organize functions are anchored by incident response documentation development, remediation road maps, and recommendations. The train and exercise area is focused on incident response training, tabletop exercises, and red and purple team testing. The evaluate and improve portion of the life cycle covers a variety of assessments, testing, and documentation reviews.

Secureworks offers purple team exercises as either a one-time functional training exercise or an ongoing scenario-based exercise. In both engagements, the goal is better incident response preparation. Key measurements include time to detect, time to respond, and time to eradicate. Information is shared between the adversary (red) team with the defensive (blue) team throughout the exercises.

The ongoing purple team exercise is similar to the one-time engagement, but it spans scenarios such as insider threats, phishing, and stolen laptops and is based on knowledge of likely threat actors. Matching tactics that these threat actors utilize based on previously acquired threat intelligence allow for the use of tailored, realistic scenarios to elevate clients' incident preparedness.

Secureworks offers a ransomware preparation assessment with four components: an Active Directory security assessment, document review and stakeholder interviews, tabletop exercises, and a ransomware simulation.

Strengths

The firm's supply chain testing program helps clients understand the abilities of supply chain vendors to perform their contractual obligations even when under sustained cyberattacks.

The recently launched Taegis VDR (vulnerability management capabilities) allows clients to view their risk and vulnerability positions and use the information to prioritize security investments.

The Remote Access Vulnerability Assessment is relevant to testing and assessing areas like remote desktop protocol (RDP), virtual private network (VPN), and password credentials that are common threat vectors in hybrid and work-from-home situations.

Challenges

Secureworks does not currently offer cyber-ranges as a form of cyberattack training and simulation.

Additional pricing options such as an outcome-based pricing model should be considered.

Consider Secureworks When

Organizations of all sizes that prefer a provider that has a range of cybersecurity software along with managed and professional services should consider utilizing Secureworks.

Verizon

Verizon is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide incident readiness services.

Proactive incident response capabilities assessments, incident response plan and playbook development, purple team exercises, and forward-deployed endpoint and network telemetry are examples of programs that Verizon offers to create, maintain, or elevate incident readiness and drive down response SLAs. Network and endpoint security health checks are available on the proactive end of the spectrum. Cyberthreat hunting, through the use of dark web hunting, enterprise threat hunts, and forensic analysts, searches for cyberthreats that have evaded cyberdefenses.

One of Verizon's incident readiness goals is to control potential incident costs. Upfront discovery of a new client's history in prior cyberattacks, along with assessing, current cybermaturity, helps Verizon come up with a road map of activities, exercises, and testing needed to elevate an incident readiness program.

Verizon's threat research contributes to the preparation of breach simulation kits that are used to facilitate tabletop exercises and other simulation workshops.

The Verizon Rapid Response Retainer (RRR) contains components such as a proactive assessment, an emergency escalation protocol, a guaranteed service-level agreement, dark web hunting, endpoint and network telemetry analysis, Verizon's Backbone Netflow Collection, and security health checks. Verizon's retainer offers buyers the flexibility to customize the retainer to accommodate their own cyber-risk profile in which they can choose add-ons beyond the Core package.

Incident response planning includes health checks and assessments. The espionage health check seeks to recognize any potential in-progress breaches, identifies systems that might be susceptible to persistent threat, and defines actionable steps to mitigate the threats. An executive breach simulation is a mock breach simulation that aims to uncover security vulnerabilities and identify process improvements to streamline incident response capabilities.

Verizon's insights gained from threat intelligence and data breach investigations offer additional information about industry-specific threats that clients can utilize to mitigate assets at risk.

Strengths

Verizon's technology stack is intertwined with a broad and deep pool of technology vendors, resulting in a vendor-agnostic portfolio of services.

Verizon can set up clients to take advantage of its 5G infrastructure by enabling forensic data that needs to be preserved and analyzed to be sent from a client's on-premises location through its 5G network. This speeds up the data transmission and reduces the stress on other networks that might still be under active cyberattacks.

One client noted the detailed nature of the free incident readiness evaluation conducted during onboarding. When an incident response situation occurred, the client was talking to an incident responder within an hour.

Challenges

Verizon needs to work on integrating its marketing strategies such that its incident readiness capabilities can also be portrayed as separate and distinct offerings.

Verizon allows limited flexibility related to incident retainer funds that are unused at the end of a contract period.

Consider Verizon When

Organizations of all sizes that wish to partner with a vendor-agnostic incident readiness firm with threat intelligence capabilities should consider utilizing Verizon.

Wipro

Wipro is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide incident readiness services.

Wipro's IR Incident Readiness Assessment Framework focuses on the people, processes, and technology aspects of resilience. Using the framework, Wipro:

- Engages members of the incident response team, senior management including the C-suite and the board, technology teams, and external stakeholders
- Reviews processes including incident response policies, plans, and playbooks; communication of incidents; backup and restore policies; and data retention policies
- Reviews technology including network topology, logging and artifact collection capabilities, identification of key access points, and forensic analysis capabilities

Tabletop exercises, scenario-based assessments, and framework-based assessments provide inputs to elevate clients' readiness capabilities. Deliverables such as readiness and gap assessments, road

maps to elevate incident readiness, and best practices are offered as documented outputs of the firm's activities.

Wipro's global cybersecurity and risk services (CRS) practice maintains regional leadership that recognizes region-specific incident readiness needs. 16 cyberdelivery centers are located across the globe.

Wipro's simulation exercises break down into tabletop exercises, technical simulations, and breach and attack exercises. The clients' cybersecurity maturity level is taken into account to design the proper exercise(s).

Strengths

Wipro's adjacent business and technology consulting services enable an inside-out viewpoint of clients' capabilities and potential areas of improvement. Incident readiness programs can be tailored to meet each client's requirements.

The creation of incident response playbooks helps speed containment and response times during an incident. Playbook templates can be customized to industry and organizational needs.

For each step in an incident response situation — preparation, identification, containment, eradication, recovery, and lessons learned — Wipro identifies whether it is a Wipro's responsibility, client responsibility, or shared responsibility.

Challenges

Wipro should consider expanding relationships with cyberinsurance firms by being on their panels and providing guidance to clients that desire to mitigate a portion of their risk by purchasing cyberinsurance.

Wipro does not offer formal training programs, although ad hoc learning may occur during the delivery of incident readiness services.

Consider Wipro When

Organizations looking to partner with a global incident readiness firm that has IT and cybersecurity acumen and broad industry knowledge should consider Wipro.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level

decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Incident readiness services help organizations prepare to act in the case of a security breach or attack by putting in place organized procedures to manage the effect of a breach in the event of a security incident. Incident readiness services include consulting, training, assessments, exercise and testing engagements, and other complementary services.

The objective is to limit the damage of any potential security incident and to reduce recovery time and costs through the prompt identification, isolation, and eradication of the problem.

Definitions of Incident Readiness Services

IDC recognizes that there are five buckets of services of incident readiness services that providers generally offer. The following list of incident readiness services is not an exhaustive list, but it does lay out the primary list of capabilities that IDC sees in the market, and the definitions are largely based on industry standards as well as the knowledge that IDC has gained doing the research in this study:

- Consulting:
  - **Risk mitigation.** The prioritization, evaluation, and implementation of the appropriate risk-reducing controls/countermeasures recommended from the risk management process
  - **Security strategy.** A strategy that is determined after completion of activities such as asset discovery and risk classification, review of existing security controls, and evaluation of new/additional controls and security team capabilities (The strategy is a living document that describes the steps an organization should follow to identify, remediate, and manage risks while remaining compliant with applicable regulations.)
  - **Business continuity and disaster recovery.** Business continuity that focuses on what organizations need to do to keep their businesses running in case of a crisis and return to normal state; disaster recovery that focuses on restoring IT systems and operations as quickly as possible following a disaster to minimize downtime
  - **Creation of incident response playbooks.** Playbook documents that outline actionable steps an organization can follow to successfully recover from a cyberevent

    - **Creation of runbooks.** The establishment of predefined procedures to achieve a specific outcome
    - **Cyberinsurance.** Guidance and negotiation related to purchasing cyberinsurance
    - **Ransomware C-suite.** Advice and counsel given to the C-suite related to specific ramifications that a ransomware attack entails
- **Assessments:**
    - **Risk.** The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact
    - **Maturity.** A review of the existing cybersecurity program to determine preparedness for sophisticated attacks and examination of relevant internal documentation; sometimes includes in-person meetings with an organization to understand how the security program works in practice; often includes a heatmap to demonstrate gaps and road map to maturity
    - **Network architecture.** An evaluation of network architecture and network operations designed to identify vulnerabilities related to device configuration, controls, and policies; typically includes recommendations (ideally prioritized) to address vulnerabilities
    - **Cloud architecture.** An assessment of cloud service providers' security controls, policies, standards, and documentation and comparison to an organization's requirements; typically identifies gaps and provides recommendations to address security vulnerabilities
    - **Edge architecture.** An assessment of the security of physical or virtual components, software, and processes used in edge computing (When appropriate, regulatory compliance should be a consideration.)
    - **Vulnerability.** Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation
    - **Compromise.** A high-level review of an organization to determine if it has been or currently is compromised
    - **Proactive threat hunting.** The proactive and iterative search for threats that have evaded detection by automated detection systems
    - **Threat modeling.** A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment
    - **Ransomware readiness.** Checks an organization's ability to defend against an actor's techniques, detect ransomware threats, respond effectively in case of attack, and recover rapidly based on knowledge of assets, locations, and restoration procedures
- **Exercise/testing:**
    - **Penetration testing.** A form of ethical hacking that involves simulating a cyberattack on an organization's network and other systems such as web applications to discover vulnerabilities and test security controls
    - **Cyber range.** An interactive, virtual learning/training environment in which attacks on IT infrastructure, software platforms, networks, and applications can be simulated

- **Tabletop exercises.** A discussion-based exercise in which team members gather around a table to discuss their roles and responsibilities related to a cybersecurity event (Exercises, which can be customized scenarios, examine current state and identify improvements.)
- **Incident response plan testing**. Methods such as tabletop exercises, simulated attacks, and communications strategy testing that verify whether incident response playbooks and processes work as expected
- **Red team exercises.** Red teams that test the effectiveness of a security program (This is accomplished by emulating the behaviors and techniques of likely attackers in the most realistic way possible. The practice is similar, but not identical, to penetration testing, and it involves the pursuit of one or more objectives.)
- **Blue team exercises.** Blue teams that refer to the internal security teams that defend against both real attackers and red teams (Blue teams should be distinguished from standard security teams, as most security operations teams do not have a mentality of constant vigilance against attack – the mission and perspective of a true blue team.)
- **Purple team exercises**. Groups that exist to ensure and maximize the effectiveness of the red and blue teams (They do this by integrating the defensive tactics and controls from the blue team with the threats and vulnerabilities found by the red team into a single narrative that ensures the efforts of each are utilized to their maximum.)
- **Breach and attack simulation (BAS).** An evaluation of security postures in a continuous, automated, and repeatable way by simulating cyberattacks against an organization's infrastructure from within and outside (BAS is used to complement traditional red/blue or purple team exercises, or penetration testing exercises.)

- **Training:**
  - **Media and communications.** Learning activities centered on an organization's security incident communication strategy, which covers internal communications, media communications, and issues related to compliance
  - **Crisis management.** Learning activities focused on the process and steps an organization performs to respond to and manage a crisis that has the potential to harm the business or stakeholders
  - **Ransomware recovery for IT/security.** Training focused on the processes and procedures used to recover from a ransomware attack (Depending on the type of attack, adherence to digital forensics procedures may be essential.)
  - **First responder.** Education, and potential certification, of individuals who are an organization's first line of defense against cyberattacks (Topics may include how to analyze threats, how to design secure network environments, and how to investigate security incidents.)
  - **Red team.** Training sessions designed to teach an internal group to test the effectiveness of security program. (The team plays an adversarial role by running simulated cyberattacks, including penetration testing and vulnerability assessments. Attacks are designed to determine how well people, networks, applications, and physical security controls can detect, alert, and respond to an attack.)
  - **Blue team.** Education of a group that assesses network security for purposes of identifying vulnerabilities and strengthening incident response (Knowledge of tactics, techniques, and procedures is essential. A blue team defends against red team attacks and uses methods such as security audits and reverse engineering.)

- **Purple team.** The education of a "bridge" team that works between red and blue teams to facilitate information sharing and real-time collaboration to improve organizational security (The purple team can be a separate group or a methodology that red and blue teams can implement.)
- **Cybersecurity end-user awareness.** Employee education focused on identification of suspicious attachments, social engineering, and scams (In addition, employees are taught what to do when they encounter suspected malicious attacks and how to report them.)
- **Cyberthreat intelligence**. Education of individuals who are tasked with using threat intelligence to identify, analyze, block, and remediate potential and actual threats
- **Framework (e.g., MITRE ATT&CK).** Sessions designed to teach individuals about one or more security frameworks and how to use them in their cybersecurity analyst roles

- **Complementary:**
  - **Forensics imaging/analysis during red, blue, or purple team exercises or other simulation exercises.** The analysis of relevant data from digital images using the latest image analysis techniques (This may involve metadata, GPS data, and other analysis to determine image origin and content, generally undertaken in legal investigations.)
  - **Threat intelligence.** Data (and sometimes advice) about cyberattackers, including tactics, techniques, and procedures, that is supplied to experts who can enrich, correlate, and analyze it to improve an organization's cyberdefense
  - **Big data and analytics (also known as anomaly detection or user behavior analytics).** The use of machine learning to identify unusual patterns, events, and atypical behaviors that may indicate malicious activity
  - **Backup as a service (BaaS).** A cloud-based service that provides offsite data storage and regular backup to help protect against data loss (The provider assumes responsibility for maintenance and management because backups are no longer performed on premises.)
  - **Disaster recovery as a service (DRaaS).** A cloud-based service that backs up an organization's data and IT infrastructure and enables restoration after a disaster or outage
  - **Threat hunting (by monitoring structured and unstructured data, email, and chats on the dark web versus compromise assessments).** Threat hunting performed by cybersecurity experts who search networks, endpoints, and files looking for malicious, suspicious, or risky attackers or activities that aren't discovered by cybersecurity tools or controls (Reactive threat hunters seek to eradicate the identified malware, and then search for other possible incursions by the attacker and the associated malware. Targeted threat hunts occur around the high-value assets of an organization. Proactive threat hunting is the hypothetical analysis of the tactics, techniques, and procedures of a likely adversary and hunting around a likely area of compromise.)
  - **IT asset discovery.** An inventory of IT assets used in an organization (Typically, discovery includes hardware devices, device configuration, and software.)
  - **Internet of Things (IoT) asset discovery.** The detection of Internet of Things devices in networks, including a determination of their connection status, for purposes of building an asset database (Details about device attributes and entitlements contribute to identity and access management decisions.)
  - **Operational technology (OT) asset discovery.** An inventory of operational technology industrial assets, physical or virtual, including location, make and model, hardware/software configuration, and any known vulnerabilities

Strategies and Capabilities Criteria

This section includes an overview of the characteristics that IDC believes buyers of incident readiness services should take into consideration. IDC weighs some sections higher than others. Tables 1 and 2 provide key strategy and capability measures for success related to incident readiness services, respectively.

TABLE 1

Key Strategy Measures for Success: Worldwide Incident Readiness Services

Criteria	Definition	Weight (%)
Cost management strategy	Providers plan to manage costs with attention to delivery, profitability, and customer value.	2.5
Customer service strategy	Providers plan to use numerous methods to measure customer satisfaction.	5.0
	Providers can describe in detail their future process for tracking planned customer service improvements and validating them with customers.	
Delivery strategy	Providers plan to have a defined, repeatable methodology for delivering incident response services.	10.0
	Providers plan to utilize an array of compliance standards.	
	Providers plan to offer an array of business personas.	
	Providers plan to offer a variety of criteria to use in formulating containment plans.	
Employee strategy	Providers have plans to describe criteria to evaluate employee performance after incident readiness engagements.	7.5
	Providers articulate their future tactics for attracting and hiring talent.	
	Providers describe the standards and/or best practices they expect to use in the future to evaluate the breadth and depth of their incident readiness professionals.	
Functionality or offering strategy	Providers plan to offer an array of consulting services.	35.0
	Providers plan to offer an array of incident readiness services.	
	Providers plan to offer an array of exercise or testing services.	
	Providers plan to offer an array of training services.	
Growth strategy	Providers have well-defined plans for growth in specific areas.	5.0

TABLE 1

Key Strategy Measures for Success: Worldwide Incident Readiness Services

Criteria	Definition	Weight (%)
	Providers plan to have well-defined strategies to overcome growth inhibitors.	
Innovation advanced technology strategy	Providers plan to pursue various innovation and R&D activities.	12.5
	Providers can describe planned, future incident readiness services innovations.	
	Providers have plans to incorporate AI/ML into incident readiness capabilities.	
	Providers have plans to incorporate automation into incident readiness capabilities.	
	Providers plan to have OT/IoT readiness capabilities.	
Marketing strategy	Providers plan to use numerous marketing tactics to promote their businesses.	10.0
	Providers plan to have programs that involve outreach to educational institutions.	
	Excellence is marked by planned, defined industry-focused marketing strategies.	
	Excellence is marked by well-defined geographic-focused marketing strategies.	
Portfolio strategy	Providers plan to make internal investments in their portfolio.	5.0
	Providers plan to have a process to apply lessons learned from incident readiness engagements.	
Pricing – retainer strategy	Providers plan to allow customers to apply unused retainer dollars toward other services.	2.5
Sales and distribution strategy	Providers plan to improve incident readiness service delivery through a well-reasoned sales/distribution strategy.	2.5
	Providers have a defined strategy for utilizing partners to deliver services.	2.5
Total		100.0

Source: IDC, 2021

TABLE 2

Key Capability Measures for Success: Worldwide Incident Readiness Services

Criteria	Definition	Weight (%)
Cost competitiveness	Providers manage costs with attention to delivery, profitability, and customer value.	5.0
	Providers have multiple strategies to competitively price their services.	
Customer service offering	Providers have a variety of methods to measure customer satisfaction.	10.0
	Providers can describe in detail their process for tracking planned customer service improvements and validating them with customers.	
	Providers rated on their current clients' willingness to recommend them.	
Delivery	Providers have a defined, repeatable methodology for delivering incident readiness services.	12.0
	Providers offer an array of delivery frameworks.	
	Providers utilize an array of compliance standards.	
	Providers have a consistent defined process for measuring success.	
	Providers utilize an array of business personas.	
	Providers offer a variety of criteria to use in formulating containment plans.	
Employee management	Providers describe criteria to evaluate employee performance after incident readiness engagements.	4.0
	Providers articulate their tactics for attracting and hiring talent.	
	Providers describe the standards and/or best practices they use to evaluate the breadth and depth of their incident readiness professionals.	
Functionality or offering	Providers offer an array of incident readiness services.	40.0
	Providers offer an array of exercise or testing services.	
	Providers viewed as capable in incident readiness exercises or testing.	
	Providers offer an array of training services.	
	Providers are viewed as offering a full spectrum of incident readiness capabilities.	
	Providers are rated on security, strategy and risk mitigation consulting, creation of IR playbooks, and so forth.	
	Providers are rated on risk, network architecture, vulnerability assessments, and so forth.	

TABLE 2

Key Capability Measures for Success: Worldwide Incident Readiness Services

Criteria	Definition	Weight (%)
	Providers are rated on training capabilities.	
	Providers are rated on incident readiness/response policy creation.	
	Providers are rated on incident scenarios covered by the IR plan.	
Innovation advanced technology	Providers pursue various innovation and R&D activities.	8.0
	Providers have incorporated AI/ML into incident readiness capabilities.	
	Providers incorporate automation into incident readiness capabilities.	
	Providers have OT/IoT readiness capabilities.	
Marketing execution	Providers utilize a variety of techniques for new customer acquisition.	6.0
	Excellence is marked by well-defined industry-focused marketing strategies.	
	Excellence is marked by well-defined geographic-focused marketing strategies.	
	Providers distinguish their marketing and value propositions based on the persona targeted.	
Portfolio	Providers have a process to identify and improve gaps in their standard operating procedures.	2.0
Pricing	Providers have introduced new, innovative pricing options.	12.0
	Providers benchmark their pricing against other providers.	
	Providers are rated on the ability to use unused retainer dollars on consulting and assessments.	
Sales and partner distribution	Providers have a defined strategy for utilizing partners to deliver services.	1.0
Total		100.0

Source: IDC, 2021

LEARN MORE

Related Research

- *Market Analysis Perspective: Worldwide Security Services, 2021* (IDC #US48246421, September 2021)
- *IDC MarketScape: U.S. Managed Detection and Response Services 2021 Vendor Assessment* (IDC #US48129921, August 2021)
- *Accelerate Threat Detection and Response with Advanced Tools, Technologies, and Expertise* (IDC #US47724721, June 2021)
- *IDC PlanScape: Breach Attack Simulation Services* (IDC #US47649921, May 2021)

Synopsis

This IDC study presents a vendor assessment of vendors offering incident readiness services through the IDC MarketScape model. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for incident readiness services. The evaluation is based on a comprehensive and rigorous framework that assesses how each vendor stacks up to one another, and the framework highlights the key factors that are expected to be the most significant for achieving success in the incident readiness services market over the short term and the long term.

"Cybersecurity budgets are largely continuing to grow year over year, but the areas that they are growing in is changing. Security leaders are wisely recognizing that they need to diversify their investments to account for the very real possibility that they will face an attack that requires the special skill set that incident response providers bring to the table. Working with a provider that can provide the types of incident readiness services that can help the organizations respond and recover from a major cyberattack is a proactive measure. Incident readiness providers are equipped to create the plans, conduct the proper range of assessments, and test the capabilities of their clients' cyberdefenders to detect, contain, and respond to cyberthreats that make their way into their expanded network topology. IDC believes that the capabilities that incident readiness service providers bring to the market is going to be a key method for raising the overall cybersecurity maturity and cyber-resilience of the organizations that consume these valuable services." — Craig Robinson, program director, Worldwide Security Services at IDC

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com