IDC MarketScape

IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment

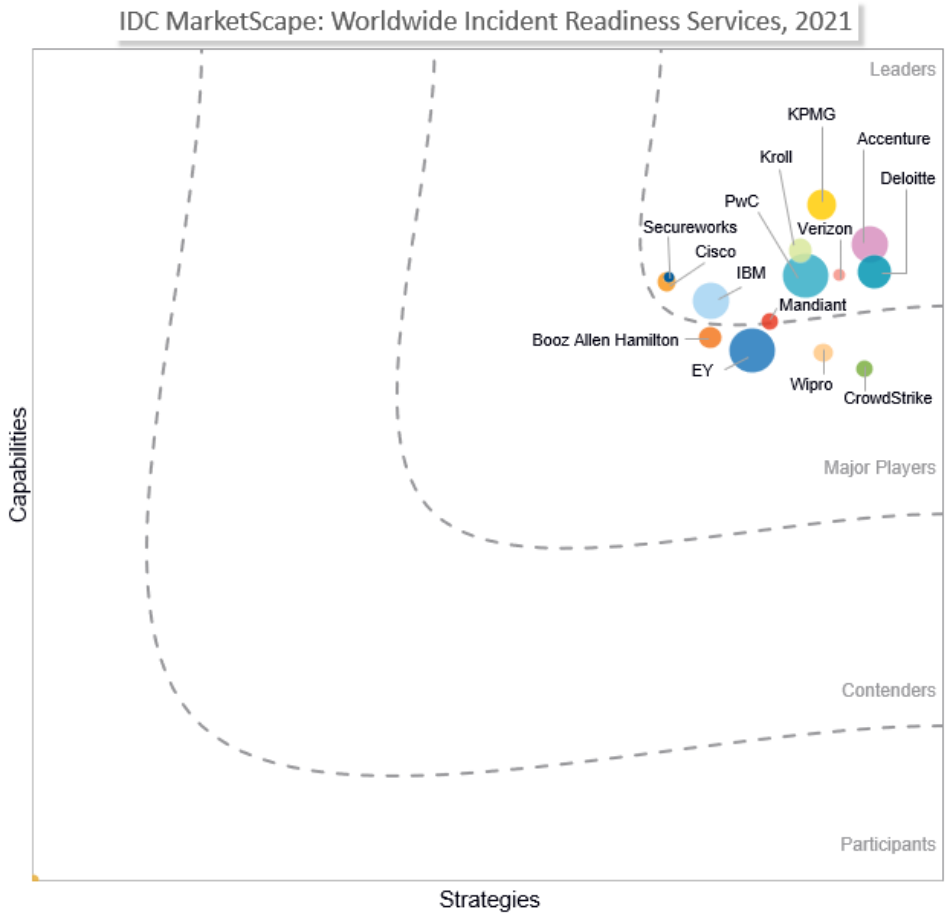
Craig Robinson Christina Richmond

THIS IDC MARKETSCAPE EXCERPT FEATURES IBM

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Incident Readiness Services Vendor Assessment



Source: IDC, 2021

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

November 2021, IDC #US46741420e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment (Doc # US46741420). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1, 2 and 3.

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.

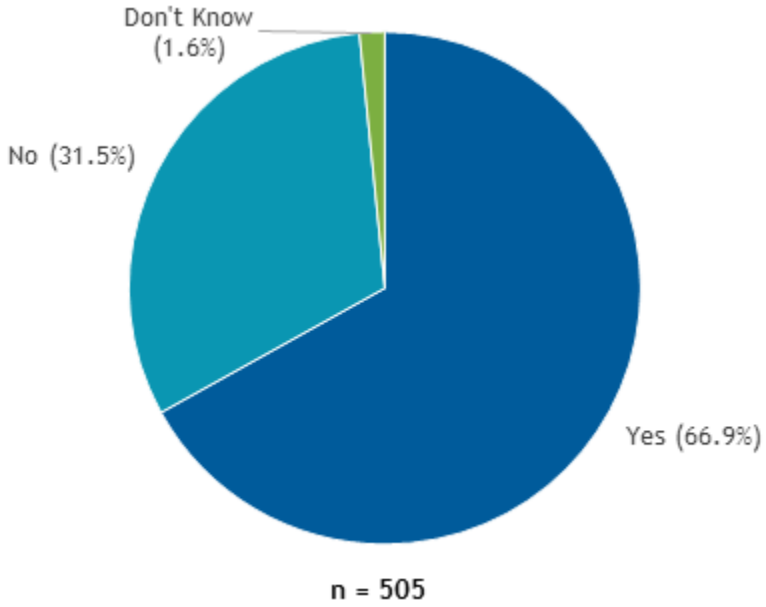
IDC has noted that incident response providers are formalizing the use of these funds to serve dual purposes. One is providing access to the exact types of services that can help minimize the need for or duration of future incident response engagements. The second is funding anticipated incident response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

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.

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.

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

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