IDC

The Critical Nature of Incident Readiness and Response in a Digitally Transformed World

RESEARCH BY:

Christina Richmond
Program Vice President,
Security Servicess, IDC

January 2022 | IDC Doc. #US48462621

Navigating this White Paper

Click on titles or page numbers to navigate to each section.

Situation Overview

Organizations are pursuing their "next normal" or "future enterprise vision" after making substantial operational changes required by the pandemic. Chief information security officers (CISOs) and other C-suite executives are focused on priorities including digital transformation, cloud migration, zero trust, risk, and incident readiness and response.

Evolving IT infrastructures, cloud-based applications, and cloud-based workloads elevate the importance of incident readiness and response. Organizations need to leverage expertise that helps them recover quickly, minimize downtime, and protect market share. A strong, mature cybersecurity posture, which includes fast, efficient response, helps organizations contain costs and reduce risk.

Incident readiness and response service providers and capabilities continue to evolve to meet organizational preferences and expectations. IDC research and insights into the trends, challenges, and benefits associated with incident readiness and incident response services offer organizations an independent opinion, perspective, and best practices that are helpful in evaluating and achieving goals. IDC also studied the maturity level of organizations and its influence on the purchase and use of incident readiness and incident response services. Interviews with security leaders contributed additional insights.

The research data enables organizations to see how they compare by industry and company size and to formulate action plans to improve their incident readiness and incident response.

Research Insights

Certain survey questions were designed to determine the cybersecurity maturity level of the participating organizations. The four levels of maturity are shown in **Table 1** (next page).

From lowest to highest, the levels are:

- **Vulnerable (least mature).** These organizations are poorly prepared for a cloud incident and have less confidence in their ability to find and manage threats and respond to them in a hybrid environment. Organizations in this category do not currently use incident readiness or response services and most will engage these services only for severe events. This stance is juxtaposed with lower confidence in the ability to discover and manage threats in a hybrid environment. In addition, most vulnerable organizations believe that responding to an incident within a hybrid environment is difficult to very difficult.
- **Aware.** These organizations are better prepared for a cloud incident than the vulnerable organizations, and most are currently using incident readiness or response services. Still, nearly one-fifth of these organizations are inclined to engage proactive or reactive services only in the event of a severe incident. Most aware companies believe that they have good threat visibility and can manage threats in a hybrid architecture. Contrarily, nearly half of them also believe that responding to an incident within a hybrid environment is difficult to very difficult.
- **Alert.** Organizations at this maturity level are much better prepared than the vulnerable and aware organizations. All alert organizations are currently using incident readiness or response services and have very high confidence in their ability to see threats and manage them in a hybrid environment. The concern of these organizations about responding to incidents in a hybrid environment is slightly higher than that of the resilient organizations.

→ **Resilient (most mature).** Resilient organizations are the best prepared for a cloud incident among all maturity categories. All resilient organizations engage in incident readiness or response services currently. Only a quarter of these organizations admit difficulty in attaining threat visibility in their hybrid environment. And only a quarter of these organizations admit that responding to an incident within a hybrid environment is difficult to very difficult.

TABLE 1

Range of Maturity in Incident Readiness and Response Services (%)

	Least Mature: Vulnerable	Aware	Alert	Most Mature: Resilient
Currently use incident readiness/response services	0	64	100	100
Engage incident readiness/ response services only in the event of a severe incident	59	17	0	0
Believe threat visibility and management of cloud architecture is effective/very effective	67	87	96	94
Responding to an incident in a hybrid environment is difficult to very difficult	54	50	40	24

Source: IDC, 2021

Findings validate that maturity level influences many aspects of service provider engagement, including the decision to invest in incident readiness and/or incident response services, the purchasing process, and cloud incident response confidence.

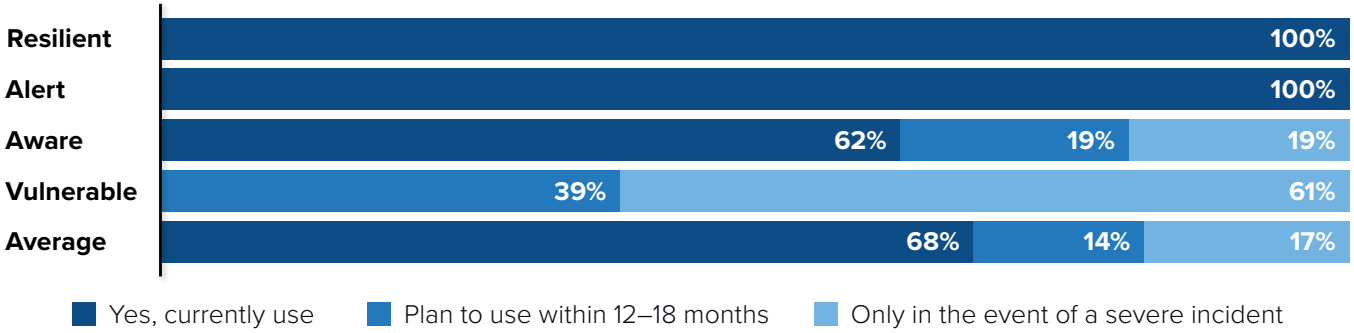
Who Uses Incident Readiness and Incident Response Services and Why?

Alert and resilient organizations all currently use or plan to use incident readiness and/or incident response services, and nearly two-thirds of aware organizations currently use the services (see **Figure 1**, next page).

FIGURE 1

Use of Incident Readiness and Incident Response Services

Q. Does your organization currently use or plan to use incident readiness and/or response services? (% of respondents)



n = 501; Base = all respondents; Notes: Data is managed by IDC's Quantitative Research Group. Data is not weighted. Multiple responses were allowed. Use caution when interpreting small sample sizes. Source: IDC's *U.S. Incident Response Survey*, June 2021

Approximately two-thirds of CISOs in larger organizations have used incident readiness or response services, and resilient organizations are four to seven times more likely to use an incident readiness or response provider.

When asked about the main reasons an organization decided to or is planning to engage with an incident readiness or response provider, more than half (54%) of the respondents cite a decision from senior management and just over half (52%) say business transformation. Midmarket and retail companies are most influenced by a management decision. Business transformation resonates most highly with manufacturing, transportation, and organizations with 2,000 or more employees. IDC has found that the combined effects of the pandemic and digital transformation, along with ongoing worry about imminent attacks, cause more organizations to review their readiness.

Organizations that understand the value of their data also understand the importance of incident response services:

- 80% of alert organizations and 95% of resilient organizations have evaluated the full cost of a data exposure, and 100% of them have invested in incident response.
- Only 16% of vulnerable organizations have evaluated the full cost of a data exposure, and 0% have incident response.

Security leaders that evaluate the cost of data exposure review determinants such as data availability, data integrity, insurance industry reports on cost to remediate breaches, value of intellectual property, loss of production outputs, and financial statements of public companies.

100% of alert and resilient organizations invest in incident response after evaluating the full cost of a data exposure.

Drivers of Incident Readiness Engagements

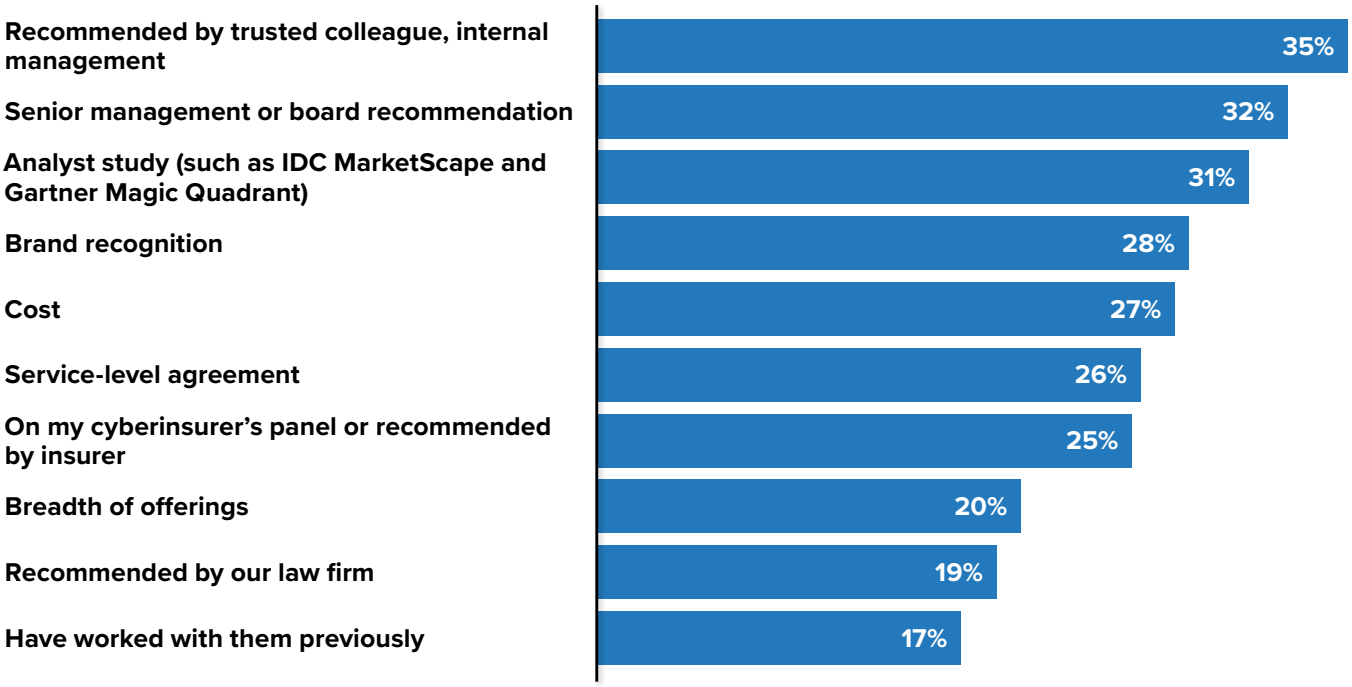
The drivers of engagement are shown in **Figure 2**. Recommendations are gold. The top two recommendations come from trusted colleagues and senior management. Finance depends most heavily on recommendations from trusted colleagues or internal managers. Companies with fewer than 1,000 employees and manufacturing organizations are most influenced by senior managers or board members. Brand recognition and cost are important to more than one-quarter of the respondents.

FIGURE 2

Drivers for Engaging an Incident Readiness Provider

Q. What are/would be the main drivers of your organization's decision to engage with a specific incident readiness or response provider?

(% of respondents)



n = 501; Base = all respondents; Notes: Data is managed by IDC's Quantitative Research Group. Data is not weighted. Multiple responses were allowed. Use caution when interpreting small sample sizes. Source: IDC's *U.S. Incident Response Survey*, June 2021

While recommendations may open the door for service providers, organizations report difficulties associated with changing providers. Obstacles include timing, onboarding, retainers, and negotiation.

More than half of the survey participants state that contract negotiation is a leading obstacle. Large companies and finance are notably concerned about procurement hurdles, and the largest companies identify both contract negotiation and vendor lock-in as concerns. These findings make sense. Procurement is likely to be more involved in the purchase decision in larger organizations, as well as regulated industries such as finance, with a goal of standardizing contracts and terms through a negotiating process.

Vendor lock-in, however, is the other side of the coin because contracts and service-level agreements (SLAs) can be lengthy. Some providers want organizations to use their gear, which can be expensive if the engagement requires lift and shift. If the negotiating process becomes too lengthy, complicated, or expensive, service providers may be viewed as difficult to work with.

Purchase Methods, Retainers, and SLAs

Organizations purchase incident response services in a variety of ways. The most common way to consume incident response is through a managed detection and response (MDR) subscription.

Retainers, which average two-and-a-half years in duration, are purchased by 14% of organizations. Other methods of acquiring incident response services are through cyber insurance claims as an emergency service when needed or as part of a managed security services subscription.

When asked about what influences retainer length, buyers commented on the following:

- The ability to purchase cybersecurity consulting and/or incident readiness services with unused retainer dollars.
- A shorter term that makes it easier to use retainer dollars for other services (a multiyear retainer ties up the money for a longer period).
- The expertise of the provider (a one-year retainer offers more assurance compared with a longer term, with fewer provider staffing changes, acquisitions, or strategic redirections that could affect quality).
- Cost and potential discounts based on length.

SLAs for emergency response vary from under an hour to multiple days. The actual response time of an incident response provider in an emergency and the preferred timing for an SLA are nearly identical across survey participants. Resilient organizations prefer response in under one hour, yet only about half actually receive emergency response in less than one hour. Less mature organizations may not be able to afford the fastest response times, negotiate as effectively, or direct procurement appropriately on desired SLAs.

In addition to response time, security leaders cite other SLA priorities, including the ability to put boots on the ground, expertise on industrial control systems (the operational technology side of the business), active investigatory skills, remote analysis capabilities, recovery points, data that's synchronized and available to clients for recovery and system restoration purposes, and the provider's reputation.

Investing in Incident Readiness Services

Readiness services include an array of offerings: risk assessments, network/cloud/edge architecture assessments, cybersecurity maturity, security and strategy, incident response planning, penetration testing, tabletop exercises, red/blue team exercises, and media and communications training. **Figure 3** (next page) shows that all readiness services are delivered in both remote and onsite scenarios — 50–84% of resilient organizations have invested in both options, and they invest more in all readiness services compared with alert and aware organizations. Tabletop exercises lead the list of services for onsite delivery only.

Resilient organizations want both remote and onsite options. They want the assurance that a provider can come onsite if remote services don't clean up an incident and they want the flexibility to use one or the other depending on circumstances.

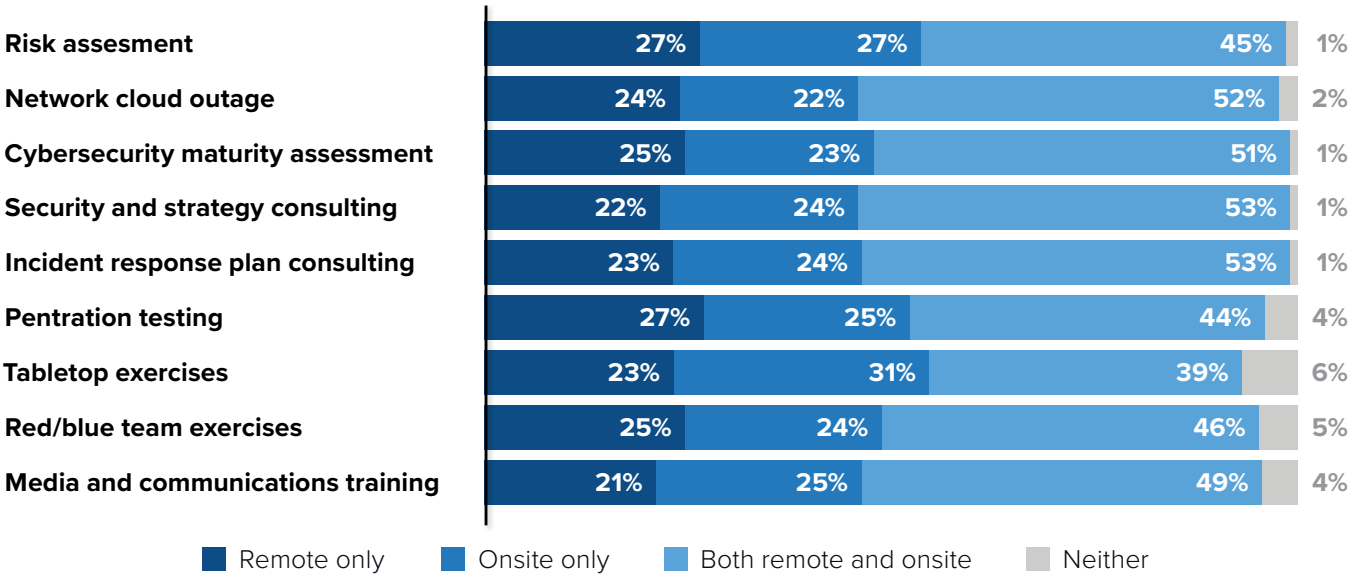
Overall, 48% of organizations have invested in both remote and onsite delivery of incident readiness services. The other 52% are split equally between the two.

FIGURE 3

Services Paid for Remote or Onsite Delivery of Incident Readiness and Response Services

Q. Which of the following incident readiness services has your organization paid for remote or onsite delivery in the past 12–18 months?

(% of respondents)



n = 342; Notes: Data is managed by IDC's Quantitative Research Group. Data is not weighted. Multiple responses were allowed. Use caution when interpreting small sample sizes. Source: IDC's *U.S. Incident Response Survey,* June 2021

One Is Not Enough

The largest companies, with 10,000 or more employees, are more likely to engage multiple providers (62%), and slightly more than half of the buyers in finance, manufacturing, and transportation prefer multiple providers. These industries are known for their diverse environments, and they need service providers that understand their business, industry, and applicable regulatory compliance requirements. Service providers may desire to be a one-and-done supplier, but even if they can tick all the requirement boxes, they have a roughly 50% chance of success.

Security decision makers explained some of the thinking that led to the engagement of multiple providers:

- The risk of receiving the same viewpoints over time versus gathering the viewpoints of different firms and their experts.
- Consideration of the depth of industry knowledge and familiarity with industry-specific threat actors.

- The investigation methodology (for example, a self-installing, self-running set of tools that can be centrally deployed and that report back to a centralized repository is preferable to a provider supplying scripts for in-house staff to run at different plants or offices).
- Specialization is important (providers generally have specific areas of expertise. A single provider might not meet all of an organization's needs).
- Not all providers are knowledgeable about OT and IT.
- The extent of familiarity with providers and/or prior relationships with providers.

Top Service Provider Capabilities

The top capabilities a provider can deliver are shown in **Figure 4** (next page). In aggregate, expertise and best practices that are tested and aligned with industry standards lead the list. Following closely is the full spectrum of MDR or extended detection and response (XDR) capabilities. Interestingly, looking at just resilient organizations, the priority of top capabilities flips to full spectrum of MDR or XDR capabilities as the most important. These two capabilities are the most important to small and large organizations, finance, manufacturing, small companies, and midmarket firms. This may be due in part to the perception that these services are a magic bullet because of a platform automated response. An understanding of the customer's business and industry ranked highly, and this is particularly important to healthcare organizations.

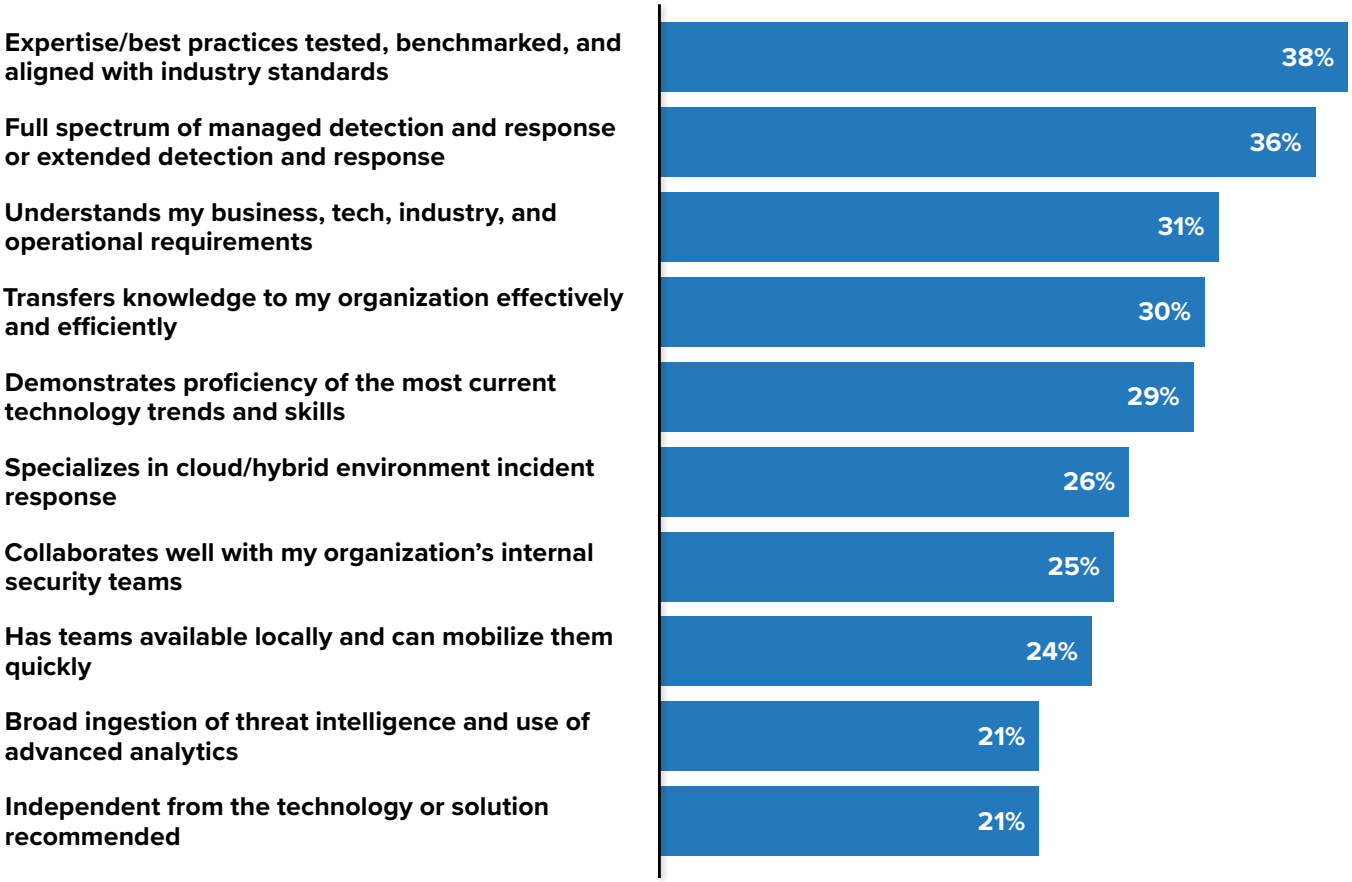
MDR in its purest form is an elevated managed service that utilizes the same features and functionality that an XDR platform offers. XDR in its purest form is an integrated platform that offers detection and response capabilities, utilizing e(X)tended telemetry sources that are managed by the purchasing entity. MDR providers either natively have the IP to look at various telemetry or utilize an XDR platform. The market is fluid, and XDR is more nascent. MDR and XDR providers often layer on additional services that can blur offering lines.

FIGURE 4

Top Capabilities for an Incident Response Provider

Q. Please select the top three capabilities your organization would look for in an incident readiness/response provider

(% of respondents)



n = 501; Notes: Data is managed by IDC's Quantitative Research Group. Data is not weighted. Multiple responses were allowed. Use caution when interpreting small sample sizes. Source: IDC's *U.S. Incident Response Survey*, June 2021

The largest companies, which already have in-house analysts for triage and response, typically view service providers as partners. They expect knowledge transfer as a way to understand what partners do and how they do it so they can replicate the activities in-house and function in lockstep with providers.

The largest organizations expect knowledge transfer to improve their internal incident response effectiveness and efficiency.

What Services Are Missing? None, But...

Nearly two-thirds of the organizations report there is nothing missing from their provider today. Those that report missing elements mention service/support (could be better or, for a small percentage of respondents, could be onsite), response time (could be faster), and security protocols/ransomware prevention (could be better). During the early pandemic months, response became entirely remote. Now a differentiator for service providers is to have boots onsite. IDC believes it is important for service providers to offer both remote and onsite services for both readiness and response.

Other onsite services are important for several reasons. Some organizations value in-person workshops and assessments because they produce better, more complete answers. When stakeholders are together, they can read facial expressions and body language and build trust. Walk-throughs of plants and offices are helpful for risk assessment/breach readiness. For example, experts can confirm readiness associated with components such as network cabinets, server rooms, and flow regulator connections, or they can point out a device that doesn't appear on a network diagram.

The Importance of Telemetry

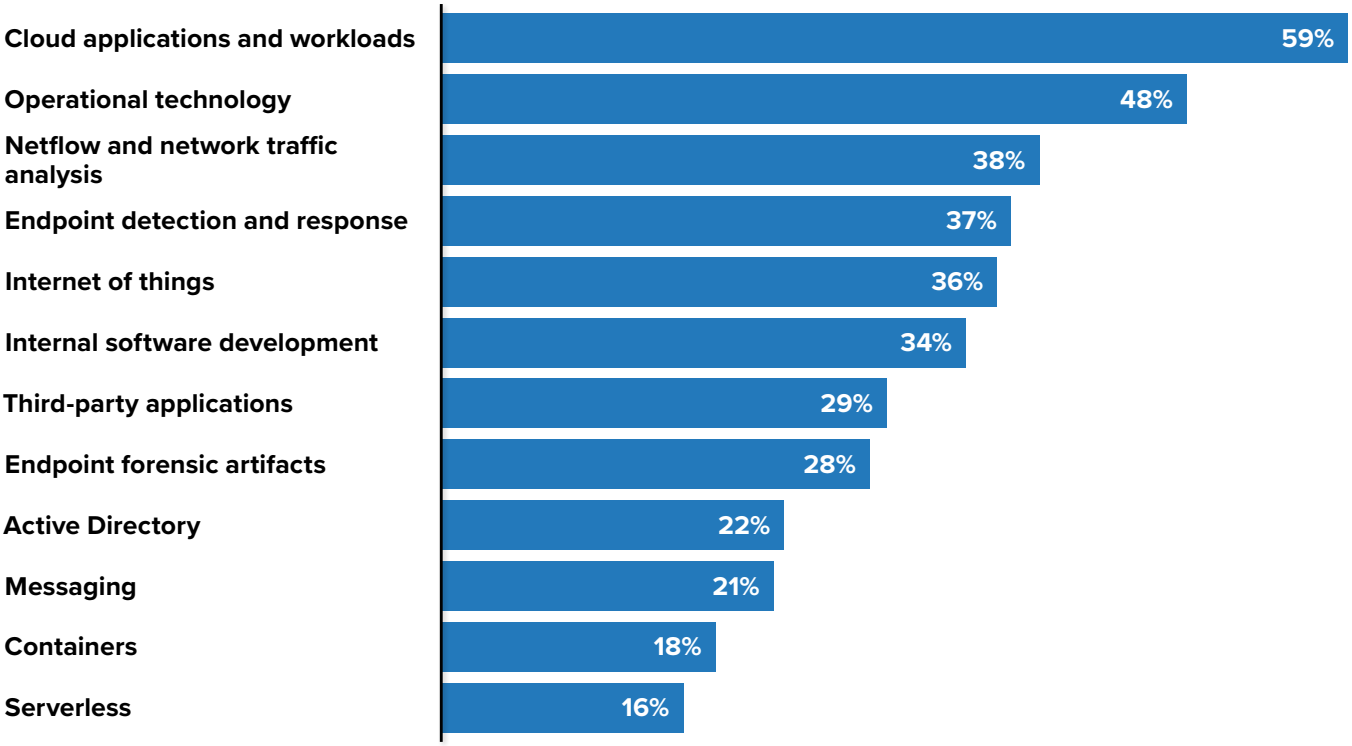
Telemetry is a differentiator among service providers. Greater visibility enables organizations to identify and respond to potential threats faster, thereby reducing risk. XDR expands collection to sources such as network, packet capture, cloud, email, messaging, internet of things, industrial internet of things, internet of medical things, operational technology devices, and edges.

Figure 5 (next page) shows how survey respondents rated the importance of telemetry to forensic analysis for incident response. 59% of the organizations surveyed believe that data from cloud applications and workloads is the most important telemetry. The most resilient organizations rate it even higher with 90% saying data from that telemetry cloud applications and workloads is the most important telemetry.

FIGURE 5

Telemetry Important to Forensic Analysis for Incident Response

Q. Which of the following types of telemetry are very important in forensic analysis (top 5 shown below)? (% of respondents)



n = 501; Base = all respondents; Notes: Data is managed by IDC's Quantitative Research Group. Data is not weighted. Multiple responses were allowed. Use caution when interpreting small sample sizes. Source: IDC's *U.S. Incident Response Survey*, June 2021

Figure 5 shows how survey respondents rated the importance of telemetry to forensic analysis. OT telemetry follows cloud applications and workloads in importance and is the most important to manufacturing. While air gapping is a common practice to isolate and protect systems and IP, manufacturers and others with OT systems need to resolve a dilemma. Air gapping limits or prevents visibility when logging isn't turned on or isn't possible at the device level. Many organizations with OT systems are waking up to the need to bring OT and IT together due in large part to 5G and edge computing.

Other findings include:

- Resilient organizations report the highest number (six) of types of telemetry, which is considered very important in forensic analysis.
- The largest firms appear to have the least concern about cloud apps and cloud workloads, but large firms aren't always the most resilient and they're not the only firms that fall into the resilient maturity level.

90% of resilient organizations rate the telemetry from cloud applications and workloads as most important in forensic analysis for incident response.

- Cloud app telemetry is of top importance to midmarket, healthcare, and retail organizations.
- Cloud workloads are of top importance to manufacturers.

When asked about what telemetry is missing in the cloud, buyers pointed to the vendor space and the vendor portion of shared responsibilities. For example, cloud service providers may not share information related to insider activity, near misses, minor compromises of internal systems, and software testing life-cycle issues. Is it important for security leaders to know about vendor events? It depends. The knowledge may be useful in evaluating cloud service providers or tracking industry-related events but, ultimately, cloud infrastructure security is owned by the cloud service providers.

Cloud Incident Response and Remediation

Certain industries have a preference for a specific type of cloud incident response provider. Telcos, systems integrators, vendors, and consultancies are frequently engaged for incident response services. Manufacturers prefer telcos and consultancies.

Overall cloud incident response is not as difficult as hypothesized, but certain maturity segments find it easier or harder. Resilient organizations find it much easier to conduct incident response in the cloud, and they are two to seven times more confident than organizations of lower maturity that they have incident response, regardless of the environment. And resilient organizations are two to four times more confident than organizations of lower maturity that they can deal with these critical elements of cloud incident response: correlating logs across cloud providers, governance across multiple cloud providers, and threat visibility.

However, when asked to rate their cloud incident response experience as "not difficult at all," only 26% of resilient organizations apply this description to software as a service (SaaS) environments and 38% to infrastructure as a service (IaaS) environments. Approximately 15% of all respondents say it's very difficult (five out of five) to respond in mixed IaaS/SaaS and on-premises — or hybrid — environments. Conversely, a quarter of resilient organizations believe response in a hybrid environment is not difficult at all.

These findings place a majority of organizations in the "difficult zone." What contributes to difficulty? Organizations don't have to deal with infrastructure, but communications in third-party cloud environments and network connectivity may be factors. For example, instead of relying on in-house datacenter staff to do the legwork and take various actions, organizations must rely on vendors. And common servers could be part of an attack over which an organization has less control.

About Palo Alto Networks Unit 42

Palo Alto Networks helps organizations shape their cloud-centric future with technology designed to transform the way people and organizations operate. The company's mission is to be the cybersecurity partner of choice, protecting a digital way of life. The company's vision is a world in which each day is safer and more secure than the one before.

Security challenges are addressed with continuous innovation that builds on breakthroughs in artificial intelligence, analytics, automation, and orchestration. An integrated platform and partner ecosystem enable Palo Alto Networks to protect tens of thousands of organizations across clouds, networks, and mobile devices.

Unit 42 brings together threat researchers, incident responders, and security consultants in an organization steeped in intelligence and response readiness. Backed by a reputation for delivering industry-leading threat intelligence, Unit 42 has expanded its scope to provide incident response and cyber-risk management services. Consultants serve as trusted advisors to help organizations assess and validate security controls against relevant threats, evolve security strategies based on threat intelligence, and respond to incidents rapidly.

Unit 42 delivers both proactive and reactive incident response services organized as follows:

- **Respond** includes services such as data breach response, digital forensics and investigations, compromise assessments, and litigation support.
- **Prevent** includes strategic advisory services spanning security programs, C-suite and board reviews, and testing and assessment activities such as ransomware readiness assessment, business email compromise assessment, cloud security assessment, tabletop exercises, penetration testing, vulnerability assessments, red/purple teaming, and breach readiness reviews.

The Unit 42 retainer allows clients to use prepaid hours for incident response, threat intelligence, and cyber-risk management services on demand. The Unit 42 retainer budget can be used for Unit 42's full menu of incident response and cyber-risk management services scoped for use within the term of the retainer.

Retainers can help organizations

- **Mitigate cyber-risk** to lower the likelihood and impact of a breach by improving readiness and outcomes with proactive cyber-risk management services.
- **Recover faster** by using Unit 42 as an extension of incident response teams with an SLA-based response, prearranged communication channels, and playbooks.
- **Manage resources** to lower the cost of an incident with faster recovery and downstream impact on brand and reputation while adding predictability to budgets.

Because cloud environments are inherently designed to be dynamic and scalable, even simple mistakes can lead to expensive, complicated incidents with outsized impact. Many incident response teams delay response by using traditional digital forensics and incident response (DFIR) methods for cloud environments.

This approach can create challenges:

- Simple mistakes can lead to complicated incidents with outsized impact.
- Primary causes include misconfigurations, insecure remote access, exposed account credentials, and unpatched vulnerabilities.
- Traditional DFIR is not designed for dynamic cloud-based incidents.

Unit 42 offers an approach for each stage of the cloud incident life cycle to accelerate recovery. The Unit 42 cloud incident response team consists of experienced cloud experts who understand the special nature of cloud security investigations. They use leading cloud tools to identify, respond to, and contain cloud-specific threats.

Unit 42 further assists organizations with the identification and mitigation of cloud-based cyber-risk, including homing in on the key indicators of compromise in cloud environments. This capability can relieve in-house teams of the need to learn tools, concepts, and other capabilities during an incident. Unit 42's cloud technology includes Cortex XDR, Cortex Xpanse, and Prisma Cloud. These tools are designed to discover the attack vector, identify the extent of access and the data at risk, and take the appropriate remediation actions.

Challenges and Opportunities

As organizations pursue digital transformation, cloud migration, zero trust, and other initiatives, their operating environments evolve rapidly. Organizations of all sizes need a unified, proactive cybersecurity program aligned to their new normal or future enterprise vision. Alignment may require a third-party perspective, updated policies and standards, assessments, an information security program, a library of standards and guidelines, recommendations, staff augmentation, and/or third-party incident response.

Hybrid IT and cloud applications and workloads increase cybersecurity complexity across expanding attack surfaces. Incident readiness/incident response providers offer an array of remote and onsite services designed to help organizations recover quickly, manage cost, and lower risk.

During provider evaluation, organizations may want to consider:

- Industry-specific and compliance expertise
- SLA and retainer flexibility to match requirements
- The working relationship with cloud service providers
- Telemetry and visibility, especially in OT and cloud environments
- Onsite and remote services
- Threat intelligence expertise
- Knowledge transfer
- Maturity models or assessments

Conclusion

In a digitally transformed world, incident readiness and incident response services are increasingly important elements of cybersecurity programs. Organizational size, maturity, and industry factor into decisions to engage or not to engage a service provider and into decision criteria.

Service providers can help organizations to be as ready as possible for inevitable adversaries with:

- Incident readiness services such as security and strategy consulting, incident response plan review, cybersecurity maturity assessment, network/cloud/edge architecture assessments, and tabletop exercises.
- Comprehensive, automated remote and onsite incident response services (MDR, XDR, and security orchestration, automation and response).
- Tailored SLAs and response times to meet organizational requirements.
- Expertise and best practices that are tested and aligned with industry standards.
- An understanding of business, technology, industry, operational, and regulatory requirements.
- Expertise in cloud threat detection, response, remediation, and communications, which will become increasingly important as hybrid cloud access expands and organizations use multiple cloud infrastructures.
- Ability to demonstrate ways of reducing cybersecurity risk and cost.

Methodology

The survey conducted by IDC to support this white paper was conducted in the second quarter of 2021. Participating organizations have 100% of their headquarter offices in the United States. A majority of the organizations (85%) also have most of their infrastructure and security within the United States. The 500 respondents are either the primary decision maker or part of a team that makes decisions regarding the use of various cybersecurity services. Two-thirds of the organizations in the survey currently use incident readiness and/or response services.

The top five industries represented in the survey are manufacturing, retail/wholesale, finance, transportation/communications/utilities, and healthcare.

The company size breakout is evenly distributed across organizations with 500–999 employees to those with over 20,000 employees.

Certain questions in the survey were used to develop a four-level maturity model and to determine the influence of maturity on the use of incident readiness and incident response services.

About the Analyst

Christina Richmond
Program Vice President, Security Services, IDC

Christina Richmond is the Program Vice President for IDC's Security Services research practice. She is responsible for the day-to-day management of the program. Core research coverage for the team includes, but is not limited to, security consulting, integration, and managed services. In addition, the team looks at services that help organizations adopt emerging technologies like cloud, edge, and IoT as well as key focus areas such as risk, data privacy, and compliance. Christina brings a wealth of security services expertise and knowledge to the position and is frequently sought after by IT security executives to share her research and insights on dynamics and trends in the security industry.

Christina also focuses on the global IDC Technology for Social Good program, which examines technology innovation and best practices, trends, portfolio offers, and initiatives developed by technology vendors and social entrepreneurs. The practice seeks to highlight technology that works to solve society's largest challenges with climate impact, environmental sustainability, diversity and inclusion, and communities at risk.

More about Christina Richmond

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC @idc @idc idc.com