



OCTOBER 2021

# INCIDENT RESPONSE RETAINER SERVICES

RESPONDING TO THE SCENE OF  
THE CRIME

Excerpt of full report featuring PwC capabilities



TARI SCHREIDER

IMPACT REPORT

# TABLE OF CONTENTS

INTRODUCTION..... 2

    METHODOLOGY ..... 3

THE MARKET..... 4

    IRR PROVIDER CATEGORIES..... 5

    IR FRAMEWORKS..... 8

    IR ORGANIZATIONS..... 8

    EXTENDING IR RETAINERS TO THE SUPPLY CHAIN..... 10

PRICEWATERHOUSECOOPERS..... 11

CONCLUSION..... 14

ABOUT AITE-NOVARICA GROUP ..... 15

    CONTACT..... 15

    AUTHOR INFORMATION ..... 15

## LIST OF FIGURES

FIGURE 1: IR RETAINER SERVICES BY CATEGORY ..... 7

FIGURE 2: SANS PICERL FRAMEWORK ..... 8

## LIST OF TABLES

TABLE A: IRR MARKET TRENDS..... 4

TABLE B: CERT ORGANIZATIONS..... 9

IMPACT REPORT

OCTOBER 2021

## INCIDENT RESPONSE RETAINER SERVICES

Responding to the Scene of  
the Crime

TARI SCHREIDER

*PwC may not be the first company that comes to mind when asked to name IRR firms, as this vendor is a best-kept secret. It is a proverbial elephant hiding in plain sight. With over 500 incident responders, seven years providing IRR services, and the sheer number of incidents to which it responded, PwC can be considered an outlier in the IR service business.*

## INTRODUCTION

The “assumption of breach” world we live in compels organizations to invest more in IR services to address the invariable security breach. Whether a breach originates from malicious insiders or nation-state attackers, organizations are compromised at an alarming rate, and attackers use increasingly creative attack vectors. The commonplace nature of data breaches has made customers numb to the news; it has almost become an expectation and even a forgivable event. What is generally not forgivable is poor execution of an organization’s IR processes, wherein customers are affected and subsequently harmed longer and greater than need be. The damage caused by data breaches has wide-ranging effects on financial services firms, including reputational damage, financial loss, customer attrition, and regulatory fines.

The need for financial services firms to have a well-rehearsed IR program is so essential that the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Treasury’s Office of the Comptroller of the Currency proposed a new rule on December 18, 2020. This proposed rule, the Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers,<sup>1</sup> reduces breach notification time to bank examiners to 36 hours. This proposed rule and other IR-related regulations make an IR program not only standard practice but also a regulatory requirement for institutions and their third-party service providers.

This Impact Report focuses on the IRR services market segment in which financial services firms may acquire external help with cybersecurity incidents through prenegotiated terms and conditions. This report looks at market representative IRR service providers ranging from managed security service providers (MSSP) to consulting-based solutions. This Impact Report will appeal to domain managers aligned to specific areas, including IR leads, CISOs, and disaster recovery managers. Buyers benefit from this report by knowing IR retainer programs’ intricacies, and vendors benefit from knowing how their services compare.

---

<sup>1</sup> “Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers,” The Office of the Comptroller of the Currency, Treasury, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation, January 12, 2021.

## METHODOLOGY

Aite-Novarica Group conducted desk research on industry publications and white papers, and reviewed nearly 200 vendors offering some form of IR service. Nearly 90 IRR vendors were identified by reviewing their respective service descriptions. Aite-Novarica Group selected 24 IRR vendors thought to provide comprehensive IRR services to complete a 65-question survey. Vendors reselling or repackaging other providers' IRR solutions were eliminated from consideration. The 24 vendors invited to participate in this Impact Report had what Aite-Novarica Group considered a demonstrated market presence. Aite-Novarica Group defines market presence as service recognition exemplified through customer use cases, size of an organization, number of employees, external investment or revenue, years of operational experience, and alignment with computer emergency response team (CERT) associations.

Vendor IRR services were normalized from marketing speak and classified into three categories: MSSP-based, consulting-based, and pure-play IR providers. MXDR and MDR are both categorized as MSSPs for this report. Ten of the 24 invited vendors agreed to participate; two vendors were subsequently eliminated for incomplete responses. Four IRR service providers are MSSP-based, three IRR service providers are consulting-based, and one is a pure-play IR provider. Aite-Novarica Group interviewed vendors, analyzed completed surveys, and reviewed relevant white papers and service descriptions during August and September 2021. Each participating vendor was provided an opportunity to verify its respective profile and service information for accuracy before report publication.

## THE MARKET

The general IR market comprises products, consulting services, certification courses, and education extending to segments as diverse as crisis response, product tampering, industrial accidents, and specialized environments such as supervisory and data acquisition systems. Aite-Novarica Group has laser-focused on the cybersecurity IRR market for this report. Digital forensics is not covered in detail within this report, although many IRR vendors provide this service and package it as digital forensics and incident response (DFIR) service. DFIR is a specialized subdomain of IR directly associated with cybercrimes. The legal aspects, specialized tools, and forensics certifications required of DFIR will be covered in a separate report. However, with that said, DFIR and other ancillary areas of IR are briefly discussed as points of comparison. Table A presents Aite-Novarica Group’s identified market trends for IRR services.

TABLE A: IRR MARKET TRENDS

MARKET TRENDS	MARKET IMPLICATIONS
<p>MSSPs continue to roll out accelerated IRR services to reduce customer churn and attract new customers.</p>	<p>MSSPs will offer IRR with managed versions of endpoint detection and response (EDR) and extended detection and response (XDR) service customers a broader portfolio of IRR services as a business model imperative.</p>
<p>MSSP vendors expand their business model to partner with IR channel partners.</p>	<p>MSSP providers rapidly extend their service portfolio to include IRR services to gain a competitive advantage. The expansion will likely lead MSSPs to acquire IR and IRR vendors. Large consulting companies will also make acquisitions in the IR space.</p>
<p>The COVID-19 pandemic has expanded IR scope requiring specialized tools and processes to address working from home without violating employee privacy.</p>	<p>IR programs will extend to the homemaker base making MSSPs offering managed EDR, MDR, and XDR services supporting bring your own device (BYOD) more attractive than in-house solutions.</p>

MARKET TRENDS	MARKET IMPLICATIONS
<p>IR becomes increasingly automated to overcome the dearth of trained and certified incident responders.</p>	<p>IRR service providers will look toward partnering or acquiring automation provided by SOAR and IR product solutions to serve as a force multiplier for incident responders, making responders more effective. Automation is the key to reducing IR's manual, repetitive nature to address the systemic burnout factor for incident responders. Areas of automation focus on responder chats, playbook automation, and wide-area communications and reporting.</p>
<p>Organizations without an IR program or poorly performing IR programs will more readily gravitate toward a third-party solution.</p>	<p>Organizations will find it overwhelming to create an IR program this late in the game and seek the least-resistant path by securing an IRR service agreement.</p>
<p>Legal and regulatory requirements for IR programs covering third-party service providers will drive increased adoption of IRR services.</p>	<p>Organizations already find it difficult to keep pace with third-party risk oversight, let alone engage when a security breach occurs within the supply chain. Organizations will acquire or expand IRR services to cover third-party breach scenarios.</p>
<p>IR resources are in high demand. On any given day, job recruiting sites have over 5,000 open positions listing IR analyst roles.</p>	<p>The lack of available and suitable candidates and competition to hire incident responders to fill open positions may lead organizations toward an IRR service agreement.</p>
<p>MSSP-based IRR service pricing will remain relatively stable as managed services contracts underwrite IRR services.</p>	<p>MSSP vendors providing IRR services will be hesitant to raise pricing in light of increased competition. Vendors will look toward automation to stave off the increased cost of incident responder salaries.</p>

Source: Aite-Novarica Group

## IRR PROVIDER CATEGORIES

IRR services conform to three basic delivery categories: consulting services, MSSP-based, and pure-play IR providers. The largest segment is MSSP-based, followed by consulting services and then pure-play IR providers:

- **Consulting services:** IRR vendors in this category specialize in full life cycle incident response, with many extending their IR to digital forensics using essentially the same resources. Providers in this category often offer penetration testing, threat hunting, red-teaming, etc. This category can be confusing, as several large consulting organizations also provide MSSP-based IRR services. Providers can use single resources to deliver multiple related services; however, not all resources can be experts at penetration testing, threat hunting, IR, and digital forensics. Consulting-based IRR services have been typically delivered on-site; however, due to the COVID-19 pandemic, vendors in this segment have had to develop robust remote capabilities. Large multinational organizations have an advantage in delivering local on-site IR services.

- **MSSP-based services:** This category is experiencing the greatest growth, building on the base of 83% of the top 250 MSSPs offering IR services.<sup>2</sup> IRR vendors within this category typically offer an included and premium level of IRR. MSSP-based IRR services are mostly provided to their respective customers; however, MSSP vendors are beginning to offer IRR to non-MSSP customers hoping they become customers. MSSP-based IRR service providers typically included 90-days of their MDR or MXDR service following incident eradication and system restoration.

Vendors in this category are increasingly looking for services to differentiate themselves from the competition. MSSP vendors with an existing relationship and knowledge of an organization are uniquely positioned to offer the IR service along with threat hunting and digital forensic services. Vendors in this category tend to provide their IRR services remotely; however, exceptions exist wherein accommodations are made to premium-tiered customers.

- **Pure-play IRR services:** IRR service providers within this category provide IR services to a retainer and nonretainer customers. The cost to nonretainer customers can be extremely expensive and is provided on a best-effort basis. Their response is typically limited geographically and by the number of available incident responders. However, providers in this category do provide on-demand IR; they provide preferential access to retainer customers.

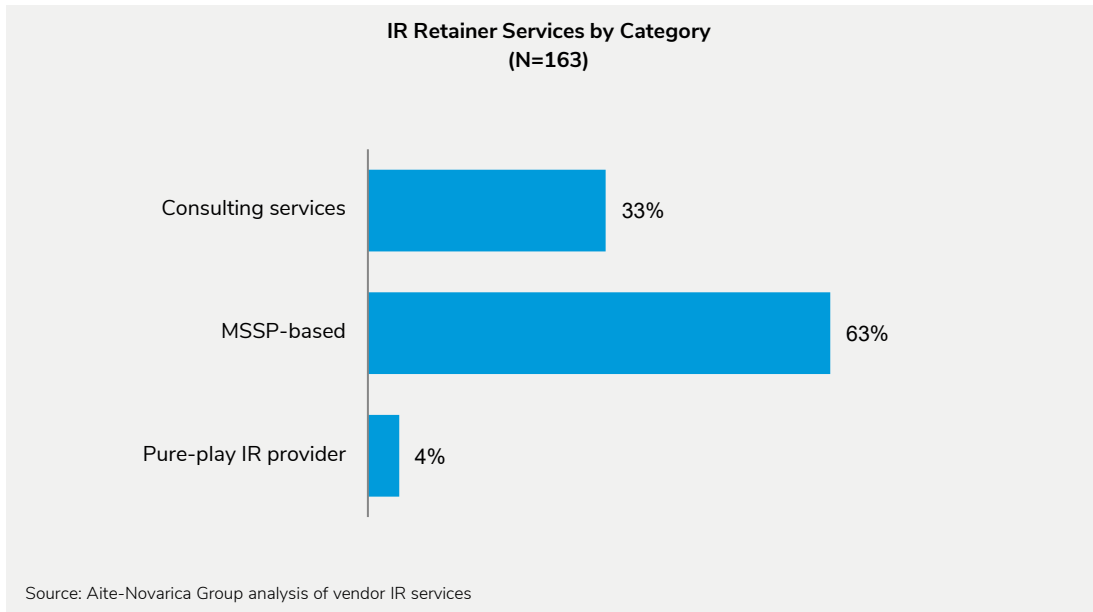
---

<sup>2</sup> Amy Katz and Joe Panettieri, "Top 250 MSSPs 2020 Edition: Company List and Research for 2020," MSSP Alert and After Nines Inc., accessed September 15, 2021, <https://www.msspalert.com/top250/list-2020/>.

Pure-play IR providers can also offer penetration testing and threat hunting; they focus almost exclusively on incident response and forensics. These providers have built a reputation for providing expert witness testimony and can handle virtually any type of cyber incident. Vendors in this category have been known to be acquired by larger consulting or insurance companies. For example, Aon acquired Cytelligence, an international DFIR provider, in June of 2020.<sup>3</sup>

Figure 1 shows the classification distribution for the IRR services of the providers researched for this Impact Report.

FIGURE 1: IR RETAINER SERVICES BY CATEGORY



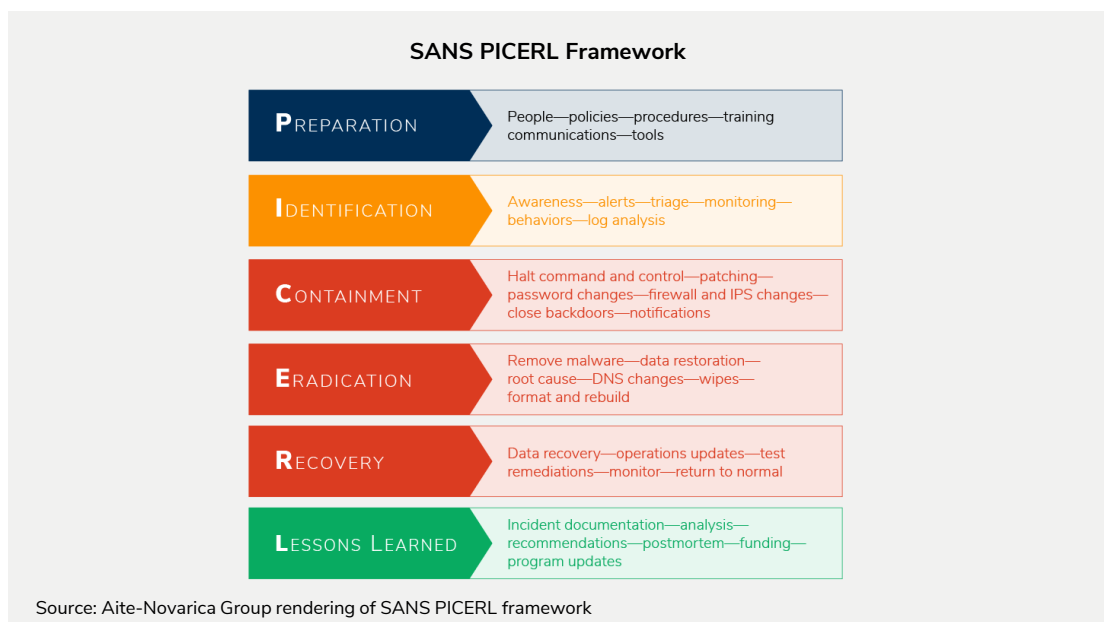
<sup>3</sup> "Aon Acquires Cytelligence, a Leading International Cyber Security Firm With Deep Expertise in Cyber Incident Response and Digital Forensic Investigations," Aon, February 4, 2020, accessed September 22, 2021, <https://www.aon.com/cyber-solutions/thinking/aon-acquires-cytelligence-a-leading-international-cyber-security-firm-with-deep-expertise-in-cyber-incident-response-and-digital-forensic-investigations/>.



## IR FRAMEWORKS

IRR service providers follow one or more IR frameworks, including ISO, NIST, and SANS. These frameworks are discussed in more detail in Aite-Novarica Group's recent Impact Brief.<sup>4</sup> It is important to understand to which IR framework a potential IRR service provider adheres. Having this understanding provides insight to align with an existing in-house IR program. Figure 2 presents the SANS PICERL framework as an example of what is typically contained within an IR framework.

FIGURE 2: SANS PICERL FRAMEWORK



## IR ORGANIZATIONS

Organizations are well served to belong to one or more CERT organizations. There are nearly 600 CERT organizations and teams worldwide,<sup>5</sup> ensuring an applicable CERT organization to any industry or technology.

<sup>4</sup> See Aite-Novarica Group's report [Incident Response Program Design: Living in an "Assumption of Breach" World](#), October 2021.

<sup>5</sup> "FIRST Teams," Forum of Incident Response and Security, accessed October 14, 2021, <https://www.first.org/members/teams/>.

A key indicator of an IRR vendor's commitment to IR is its membership and contributions to an accredited CERT. Some IRR service providers have established CERTs, such as Group-IB's CERT-GIB and Netitude's Netitude's experienced Computer Emergency Response Team (NCERT). Table B presents several of the largest CERT organizations.

TABLE B: CERT ORGANIZATIONS

NAME	ORGANIZATION	PURPOSE	WEBSITE
CREST	CREST International	Not-for-profit accreditation body cyber IR organization	<a href="http://www.crest-approved.org">www.crest-approved.org</a>
FIRST	Forum of Incident Response and Security Teams Inc.	A global forum for IR and security teams	<a href="http://www.first.org">www.first.org</a>
IRC	Incident Response Consortium	IR community laser-focused on remediation processes, best practices, playbooks, runbooks, and product connectors	<a href="http://www.incidentresponse.com">www.incidentresponse.com</a>
NCCIC	The National Cybersecurity and Communications Integration Center	Flagship cyber defense, IR, and operational integration center	<a href="http://www.cisa.gov/cyber-incident-reponse">www.cisa.gov/cyber-incident-reponse</a>
US-CERT	The United States Computer Emergency Readiness Team	Analyze and reduce cyber threats and vulnerabilities, disseminate cyberthreat warning information, and coordinate IR activities	<a href="http://www.cisa.gov/cyber-reosource-hub">www.cisa.gov/cyber-reosource-hub</a>

Source: IR organizations

## EXTENDING IR RETAINERS TO THE SUPPLY CHAIN

The 2021 BakerHostetler Data Security Incident Response Report analyzed over 1,250 cyberattacks, in which 24% of the total incidents resulted from third-party service providers. Eighty percent of these incidents triggered breach notifications, and 25% prompted regulatory inquiries.<sup>6</sup> These statistics alone provide a substantial impetus for an organization to expand IR programs to include the supply chain.

Pework is required before an IR retainer can or should be used to attend to an incident response occurring at an essential third-party vendor. This prework includes revising third-party vendor agreements, stating a requirement to cooperate with an organization's agent or IRR service provider. Not all third-party vendors will allow your organization to conduct an incident investigation. It is important to understand if the IRR service provider can support your IR program's requirement to investigate third parties. Organizations using a SOAR solution or IR product can create supply-chain-specific incident response playbooks.

---

<sup>6</sup> Ted Kobus, "2021 Data Security Incident Response Report," BakerHostetler, 2021, accessed September 7, 2021, [https://f.datasrvr.com/fr1/021/74237/2021\\_DSIR\\_Report.pdf](https://f.datasrvr.com/fr1/021/74237/2021_DSIR_Report.pdf).

## PRICEWATERHOUSECOOPERS

PricewaterhouseCoopers (PwC) is a private, US\$43 billion, over 250,000-employee self-funded full-service consulting and services company headquartered in London. Formed in 1998 from a merger between Price Waterhouse and Coopers & Lybrand, PwC has a rich history solving client needs that date back to the 19th century. Both accounting firms originated in London during the mid-1800s. PwC's cybersecurity, privacy, and forensics practice have grown to one of the largest information security consulting and services firms globally. Today, this practice serves 66 territories with over 4,850 practitioners, generating US\$975 million across 27 information security service offerings.

### Basic Firm Information

- **Headquarters location:** London
- **Founded:** 1998
- **Type:** Private
- **Stage:** Mature
- **Funding:** Self-funded
- **Employees:** 251,644
- **LinkedIn followers:** 3,595,921

### IRR Service Information

- **Service name:** IR services
- **Category:** Consulting-based
- **Service launched:** 2014
- **Total incidents handled since launch:** Thousands
- **Service area:** The Americas, the Asia-Pacific, Europe, the Middle East, and Africa
- **Service environment:** Cloud infrastructure, endpoint devices, IoT, network, mobile devices, networks, and servers

- **Excluded IR responses:** None
- **Response service coverage:** APT, business email compromise, data breaches, espionage, infrastructure disruptions, insider threats, ransomware, DFIR, and any technology and infrastructure disruption
- **CERT membership:** CERT Coordination Center, CSD-CSIRT, CSIRT, US-CERT, etc.
- **Approved insurance provider:** Yes
- **IRR page:** <https://www.pwccn.com/en/issues/cybersecurity-and-data-privacy/cyber-security-incident-response-retainer-services-mar2021.pdf>

### Service Overview

PwC's IRR services are a threat intelligence-led consulting service, part of its cybersecurity privacy and forensics practice—Incident and Threat Management Solution offering. PwC's core incident readiness and response teams are supported by a wide breadth of specialist teams available to support pre-breach, breach response, and strategic remediation stages. Specialists cover threat intelligence, vulnerability management, malware reverse engineering, cybersecurity infrastructure, applications, data consulting, and enterprise risk and regulatory support.

PwC has one of the largest numbers (500) of any IR or IRR service provider incident responders. It invests in incident responder growth, with many responders holding IR and forensic certifications consisting of CSIH, CIHE, EC-CIH, GCIH, etc. PwC's IR team handles up to 400 incidents annually; the number of incidents it has handled since the launch of its practice is estimated at over 2,500. Its IRR service is available to any organization with no required prerequisites. Eighty percent of responses are handled remotely.

PwC's Incident Response Readiness and Resilience (IR3) service is based on its IR methodology, delivery experience, and intellectual property in combination with several industry standards, including CREST Cyber Security Incident Response Guide, NIST 800-61, and the SANS 6-Step Incident Response Cycle. PwC can engage a customer with its IR3 assessment methodology to assess 20 core IR competencies. IR3 is derived from leading practices and global cyber guidance and frameworks, and is sold as a fixed-fee engagement. For midsize and large organizations, this is a valued service. PwC

can be contracted to develop IR plans and playbooks, perform threat modeling, deliver first responder training, assess and enhance the availability of forensic artifacts, and run red team assessments.

It has also developed a four-phase exercise methodology based on simulated attack scenarios escalating to live executive exercises.

PwC is an acknowledged leader in digital forensics through its Forensic Technology Solutions (FTS) team. The FTS team provides an extensive range of digital forensics, information governance, e-discovery, data analytics, and cyber security services. PwC's FTS team assists clients through the dispute resolution process and provides independent expert testimony. It handles a wide range of disputes, including litigation, arbitration, mediation, expert determination, and regulatory matters.

### Aite-Novarica Group's Take

PwC may not be the first company that comes to mind when asked to name IRR firms, as this vendor is a best-kept secret. It is a proverbial elephant hiding in plain sight. With over 500 incident responders, seven years providing IRR services, and the sheer number of incidents to which it responded, PwC can be considered an outlier in the IR service business. It is one of the few firms that can put boots on the ground globally and handle the world's largest and most complex cyberattacks. Aite-Novarica Group found its breach readiness assessment (IR3) tool and crisis simulation solutions perfect for ensuring the level of IRR services would be commensurate with an organization's needs.

Aite-Novarica Group recommends taking a serious look at PwC's IRR tiers and IR readiness services. A key evaluation consideration is its portfolio of incident readiness services, consisting of framework and policies assessment; development of playbooks, forensics, and incident response readiness assessments; first responder training; threat profiling and modeling; and IR engineering. Avoid the temptation to dismiss this large consulting firm as too expensive; its price structure is quite similar to any other high-end IRR service provider.

## CONCLUSION

- Organizations should perform a cyber insurance readiness assessment, including verifying the estimated cost and coverage for hours consumed by the IRR provider during a cyberattack. Organizations should set the minimum baseline hours between 30 and 40 hours.
- Organizations need a robust set of IR metrics to track and report on the effectiveness of IRR service providers. Metrics should be understandable, transparent, and easily reported. Metrics should be used to define IRR service providers' SLAs.
- There are many aspects to integrating an external IRR service provider with an organization's internal IR program. Organizations are strongly encouraged to simulate a cyberattack with their IRR service provider. Failure to practice response scenarios with the IRR service provider leads to inevitable delays, wrong decisions, and potentially failed response attempts.
- It is imperative that IRR services extend to third-party service providers as the number of third parties makes it more likely, and a cyberattack will often affect an organization.
- IRR service providers offer a wide array of digital forensics services. It is important to understand what level of digital forensics is included with a retainer and whether contractual terms change when switching from IR to forensics.
- Organizations need to understand how an IRR service provider handles a mass cyber-event. Depending on their answer, you may need a Plan B if an organization is deprioritized or lost out on a first-come, first-served basis.
- Organizations without an effective IR plan could find cyber breach insurance policy premiums more expensive. The cost of borrowing money may also increase as lending institutions evaluate operational risks, including cyber breaches. Credit rating companies already consider cyber risk as an indicator of creditworthiness.
- The legal landscape for lawsuit disclosure is changing; recent precedents can make IR post-mortem reporting discoverable. Define legal protocols for report preparation and disclosure with inside counsel to afford the maximum attorney-client privilege.

## ABOUT AITE-NOVARICA GROUP

Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base. The quality of our research, insights, and advice is driven by our core values: independence, objectivity, curiosity, and integrity.

### CONTACT

**Research and consulting services:**

Aite-Novarica Group Sales  
+1.617.338.6050  
[sales@aite-novarica.com](mailto:sales@aite-novarica.com)

**Press and conference inquiries:**

Aite-Novarica Group PR  
+1.617.398.5048  
[pr@aite-novarica.com](mailto:pr@aite-novarica.com)

**For all other inquiries, contact:**

[info@aite-novarica.com](mailto:info@aite-novarica.com)

**Global headquarters:**

280 Summer Street, 6th Floor  
Boston, MA 02210  
[www.aite-novarica.com](http://www.aite-novarica.com)

### AUTHOR INFORMATION

Tari Schreider  
+1.478.304.2115  
[tschreider@aite-novarica.com](mailto:tschreider@aite-novarica.com)

© 2021 Aite-Novarica Group. All rights reserved. Reproduction of this report by any means is strictly prohibited. Photocopying or electronic distribution of this document or any of its contents without prior written consent of the publisher violates US copyright law, and is punishable by statutory damages of up to US \$150,000 per infringement, plus attorneys' fees (17 USC 504 et seq.). Without advance permission, illegal copying includes regular photocopying, faxing, excerpting, forwarding electronically, and sharing of online access.