Aite Novarica

MAY 2022

INCIDENT RESPONSE RETAINER SERVICES

RESPONDING TO THE SCENE OF THE CRIME

TARI SCHREIDER

This excerpt provided compliments of:

GROUP-IB

IMPACT REPORT

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

IMPACT REPORT

MAY 2022

INCIDENT RESPONSE RETAINER SERVICES

Responding to the Scene of the Crime

TARI SCHREIDER

This report is an excerpt from an October 2021 report produced by Aite-Novarica Group.

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,[1] 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.

[1] "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
MSSPs continue to roll out accelerated IRR services to reduce customer churn and attract new customers.	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.
MSSP vendors expand their business model to partner with IR channel partners.	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.
The COVID-19 pandemic has expanded IR scope requiring specialized tools and processes to address working from home without violating employee privacy.	IR programs will extend to the homeworker base making MSSPs offering managed EDR, MDR, and XDR services supporting bring your own device (BYOD) more attractive than in-house solutions.

MARKET TRENDS	MARKET IMPLICATIONS
IR becomes increasingly automated to overcome the dearth of trained and certified incident responders.	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.
Organizations without an IR program or poorly performing IR programs will more readily gravitate toward a third-party solution.	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.
Legal and regulatory requirements for IR programs covering third-party service providers will drive increased adoption of IRR services.	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.
IR resources are in high demand. On any given day, job recruiting sites have over 5,000 open positions listing IR analyst roles.	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.
MSSP-based IRR service pricing will remain relatively stable as managed services contracts underwrite IRR services.	MSSP vendors providing IRR services will be hesitant to raise pricing considering increased competition. Vendors will look toward automation to stave off the increased cost of incident responder salaries.

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.[2] 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.

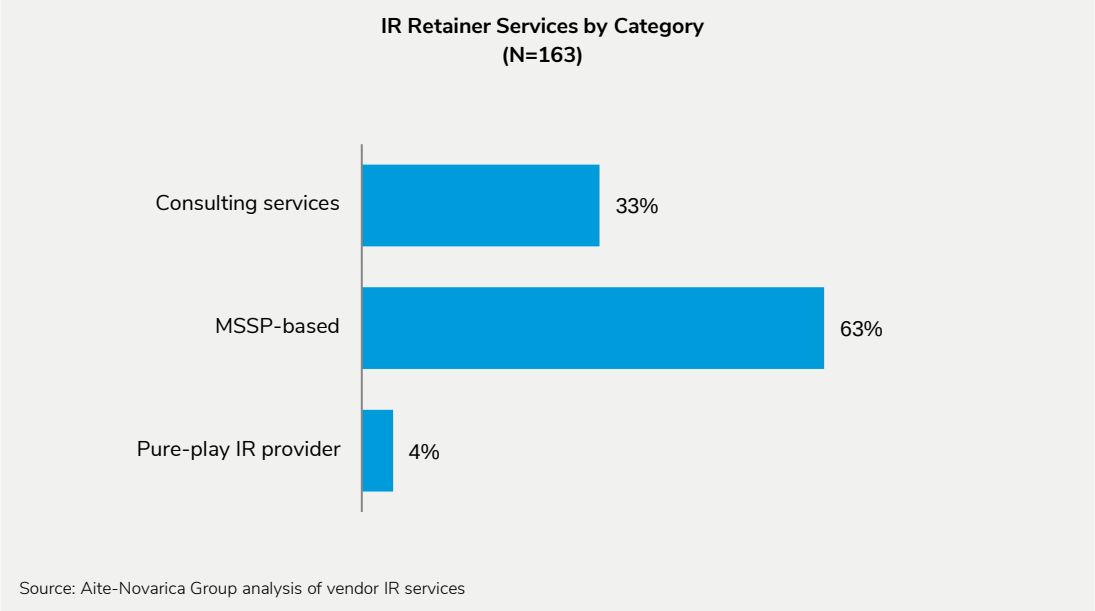
- **Pure-play IRR services:** IRR service providers within this category provide IR services to a retainer and nonretainer customers. The cost to nonretainer customers can be extremely expensive and is provided on a best-effort basis. Their response is typically limited geographically and by the number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

[2] 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.[3]

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



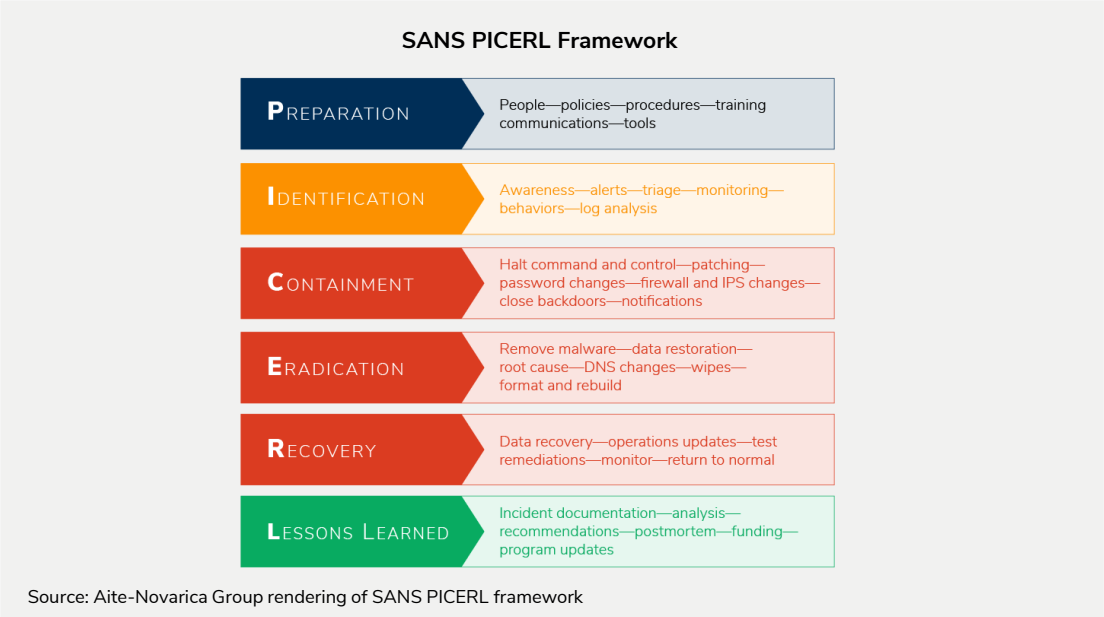
Source: Aite-Novarica Group analysis of vendor IR services

[3] "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.[4] 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



Source: Aite-Novarica Group rendering of 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,[5] ensuring an applicable CERT organization to any industry or technology.

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

[5] "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. Table B presents several of the largest CERT organizations.

TABLE B: CERT ORGANIZATIONS

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

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 inquires.[6] These statistics alone provide a substantial impetus for an organization to expand IR programs to include the supply chain.

Prework 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.

[6] 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.

GROUP-IB LTD.

Group-IB Ltd. (Group-IB), founded in 2003, is a private 600-employee cybersecurity service and software company based in Central Region Singapore. Group-IB is one of the world's largest and most experienced IR companies, with over 80 incident responders. It has extensive global coverage provided through Amsterdam, Dubai, Malaysia, Russia, Singapore, and Vietnam offices. Group-IB IR services are available to any organization with no prerequisites. Group-IB has an eye toward expanding throughout the North American market.

Ilya Sachkov (former CEO) and Dmitry Volkov, (current CEO) co-founded Group-IB. Ilya is listed as one of the 26 prominent independent commissioners for the Global Commission on the Stability of Cyberspace, a member of cybercrime expert committees in the Council of Europe and the Organization for Security and Co-operation in Europe. He takes part in the work of the World Economic Forum's Centre for Cybersecurity. In 2010, Ilya became the first Russian national to win the Digital Crimes Consortium award to contribute to the international exchange of experience in computer forensics. In 2016, he became a member of the Europol EC3 Advisory Group on Internet Security.

Dmitry is the mastermind behind most of Group-IB's products. He is a graduate of Russia's leading engineering university—Moscow State Technical University of N.E. Bauman. From day one, he has been a prominent voice leading Group-IB toward becoming the go-to expert in threat hunting and cyber intelligence. Since co-founding Group-IB in 2003, Dmitry Volkov plays a key role in the company's technological development.

Group-IB has a specialty practice around financial fraud and has returned hundreds of millions of U.S. dollars to customers in the past 18 years. It provides independent investigations to identify fraud, misappropriation, theft, abuse of power, losses and their causes, and persons responsible. In support of e-discovery, it collects, identifies, and prepares digital evidence so that it can be presented in court—the company is commonly contracted to perform a systematic analysis of finances to detect suspicious transactions and promptly identify threats and violations.

Basic Firm Information

- **Headquarters location:** Singapore Central Region
- **Founded:** 2003
- **Type:** Private
- **Stage:** Growth
- **Funding:** Self-funded
- **Employees:** 600
- **LinkedIn followers:** 21,528

IRR Service Information

- **Service name:** Group-IB Incident Response Retainer
- **Category:** Cybersecurity software and consulting
- **Service launched:** 2015
- **Total incidents handled since launch:** 3,000 (Group-IB has responded to incidents since its founding in 2003)
- **Service area:** The Asia-Pacific, the Commonwealth of Independent States, the Middle East, Europe, and Africa
- **Service environment:** Cloud computing, endpoints, IoT, mobile, and networks
- **Excluded IR responses:** Crisis management and risk management
- **Response service coverage:** APT, bank fraud, botnets, critical infrastructure attacks, DDoS, data breaches, data theft, insider fraud, money theft, ransomware, unauthorized access, and more
- **Approved insurance provider:** Yes, AIG
- **CERT memberships:** CERT-GIB, FIRST, OIC-CERT, IMPACT, Trusted Introducer
- **IRR page:** https://www.group-ib.com/incident-response/retainer.html

Service Overview

Group-IB is one of a handful of IR vendors with an authorized international CERT, CERT-GIB. At any one time, Group-IB has over 150 active retainer clients, including the top 30 largest banks and financial services firms globally. Its methodology is based on the SANS PICERL framework, with its incident responders referencing the NIST SP 800-61 Rev. 2 IR handbook. The Group-IB threat hunting framework is the central part of its IR toolset.

Group-IB employs various technical and strategic services to build a proactive approach to IR for customers. Signed SLAs to guarantee timely service and 24/7 emergency response are the cornerstone of its tier service levels. It offers flexible retainer terms, including a discounted rate for additional consulting services. Customers can repurpose prepaid hours toward selecting proactive, reactive, and educational services ranging from penetration-testing, red-teaming, and IR training.

Group-IB designed IRR agreements in different ways to fit various budget and business needs and to minimize downtime during a cyberattack. Three tiers are available, ranging from lite, standard, and premium. Each is offered in one-year durations, and all include prepaid hours. The lite tier provides an SLA of seven hours for an initial response, whereas the premium tier's SLA is three hours. An on-site response can range from best effort (generally three hours) up to 48 hours. Response time is longer for distant regions. Group-IB's approach includes the following:

- **Step 1—network traffic analysis:** Under the guidance of Group-IB experts, customers are directed to implement its threat hunting framework for network traffic monitoring and suspicious behavior detection often missed by signature-based cybersecurity systems.
- **Step 2—forensic analysis:** Group-IB specialists conduct express forensic analysis of workstations and servers used by cybercriminals to identify the initial attack vector, applied tools and techniques, and exploited vulnerabilities.
- **Step 3—malware analysis:** GIAC-certified malware analysts perform basic or advanced static and dynamic analysis of malicious code discovered during an investigation to determine other affected assets in the environment and prevent further intrusions.

Group-IB can check out incidents faster than other IRR service providers that operate without an EDR solution. Incident responders can detect previously unknown threats based on Group-IB's threat intelligence and attribution ability, and proactively search for anomalies, hidden tunnels, and signs of communications with command and control servers. Its approach exposes adversaries' infrastructure, tools, techniques, and procedures to highlight attack intent and approach. This approach significantly reduces the potential for reinfection, uncovering where adversaries deeply hide future compromise payloads.

Aite-Novarica Group's Take

Group-IB is the largest and most experienced IRR service provider profiled in this report and one of the top IRR service firms in the world. It has been responding to cyber incidents for 18 years, involving over 1,300 investigations across 60 countries, and racking up 70,000 hours of hands-on IR experience. This experience makes it an outlier seven times over. Group-IB is a partner and participant in joint investigations with Interpol and Europol. Its pedigree in IR within the financial services industry is virtually unmatched. Financial services firms throughout the world have Group-IB on speed dial. The lack of a North American presence may create headwinds in growing its IRR service, although it can remotely support customers in this region. Aite-Novarica Group believes Group-IB represents an outstanding option for international organizations requiring an IRR service with the scale and reach necessary to support complex incident responses. Despite the arrest of Ilya, Aite-Novarica Group believes Group-IB will continue to operate as usual and offers the most serious of IRR services profiled within this report.

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

Press and conference inquiries:
Aite-Novarica Group PR
+1.617.398.5048
pr@aite-novarica.com

For all other inquiries, contact:
info@aite-novarica.com

Global headquarters:
280 Summer Street, 6th Floor
Boston, MA 02210
www.aite-novarica.com

AUTHOR INFORMATION

Tari Schreider
+1.478.304.2115
tschreider@aite-novarica.com