Benchmark Insights

–

Assessing cyber risk in M&A

Unearth hidden costs before you pay them

IBM **Institute for Business Value**

About the authors

Julian Meyrick

Managing Partner and Vice President
Security Strategy Risk and Compliance
Security Transformation Services
IBM Cloud and Cognitive Software
linkedin.com/in/julianmeyrick/
julian_meyrick@uk.ibm.com

Julian helps clients develop their security strategies in the context of the cyber business risks they face. He has a particular focus on advising boards on the potential business impact of cybersecurity.

Julio Gomes

Vice President and Senior Partner,
Digital Strategy
Global Enterprise Agility Leader
IBM Services
linkedin.com/in/julio-gomes-a72223/
Julio.Gomes@ibm.com

Julio has 30 years of consulting and executive experience across several industries, functions, and geographies. Before joining IBM, he was a banking CIO and COO. He also worked for McKinsey and Boston Consulting Group, where he participated in and led several M&A transactions. Since joining IBM, he has focused on supporting clients in digital and IT transformations, including M&A.

Nick Coleman

Global Leader, Cyber Security
Intelligence and Risk
IBM Cloud and Cognitive Software
linkedin.com/in/colemannick/
n_coleman@uk.ibm.com

Nick has deep expertise in designing and leading cybersecurity programs across global organizations and jurisdictions. He has led teams through new and emerging risk scenarios from digital transformation through to mergers and acquisitions and developed thought leadership on the impact of new technologies on cyber threats.

Stephen Getty

Partner, Cloud Advisory CoC Leader
Global IT M&A Leader
IBM Services
linkedin.com/in/sgetty/
spgetty@us.ibm.com

Stephen focuses on helping clients achieve strategic business objectives through innovative and proven technology modernization strategies, operations, and large transformative programs driven by Cloud enablement, M&A driven IT transformation, and new technology adoption.

> Half of 350 surveyed risk managers identified industry consolidation as a major risk for business as a result of the COVID-19 pandemic. But risk can also present opportunity.

Key takeaways

Security should be part of the M&A team
Security experts should be embedded in the corporate M&A process and play a key role in all its phases. Failure to understand how a merger or divestiture impacts operational risk exposure detracts from future value realization.

Execute security assessments early.
More than half of companies don’t perform cybersecurity assessments until after due diligence is completed, according to 2019 IBM Benchmarking data.

Quantify the cybersecurity exposure.
Risk factors and security vulnerabilities must be analyzed and quantified. This should include currency-adjusted cyber risk models for pre-merger and post-merger operations, including potential financial and reputational risks.

Risky business

In mergers and acquisitions (M&A), value realization is typically top of mind. But cyber-risk is real. Considering data privacy regulations and mandatory breach disclosure laws, cyber risk exposure has the potential to significantly impact post-merger valuations. When assessing the value of a potential acquisition, acquiring organizations must factor in the cost of cyber risk as part of their deal strategy.

In 2016, a telecom provider based in the UK was heavily fined when a customer database it acquired earlier was hacked. In 2017, the price of Verizon’s acquisition of Yahoo’s internet business plunged USD 350 million after Yahoo disclosed three massive data breaches compromising more than 1 billion customer accounts.[1] (See Insight: The impact of data breaches on value.)

Companies exploring M&A would be wise to consider a recent example from April 2020: a pending merger had 5 percent of its total purchase price set aside to cover the potential fallout from a ransomware attack.[2] In addition to known operational liabilities, unknown costs such as lawsuits and noncompliance sanctions can detract from the acquired company’s value.

A different normal for M&A

Since the pandemic started, nearly every industry has been affected by lockdowns, fractured supply chains, and changing customer demand. In a May 2020 survey by the World Economic Forum, half of 350 surveyed risk managers identified industry consolidation as a major risk for business as a result of the COVID-19 pandemic.[3] But risk can also present opportunity. While some organizations have faltered, others are growing again.

Insight: The impact of data breaches on value

In 2017, during negotiations to sell a stake to Softbank, Uber reported that a data breach had exposed the private information of 57 million customers. Uber's lead security executive had sought to contain the damage by negotiating a USD 100,000 ransom payment to the hackers.[6] The breach was not publicly disclosed for more than a year, a decision Uber's new CEO acknowledged as problematic.[7] While the effect of the hack on deal terms was not disclosed, it is believed to have exacted a cost on Uber both reputationally and financially. The deal was ultimately closed at USD 48 billion, a 30 percent discount to Uber's initial valuation of USD 68 billion.[8]

Economic uncertainty has contributed to a decline in M&A activity in the first half of 2020. However, some analysts expect a resurgence of deals later in 2020 based on a convergence of conditions:

1. Some sectors have been hammered and need injections of capital and assurances of operational stability.
2. Companies with stronger positions will be opportunistic and looking to accelerate their transformations with new capabilities and intellectual property.
3. Acquisition efforts may be aided by marketplace liquidity. The US private equity industry alone holds USD 1.5 trillion in cash.[4] Non-financial corporations in the US have more than USD 4 trillion.[5] Moreover, interest rates in many areas are at or near historic lows.

Even in ordinary times, M&A deals are complex, time-consuming, and inherently risky. In assuming the assets and liabilities of the target, the acquirer absorbs its digital platforms, intellectual property, and customer databases. In other words, they absorb virtually any exposure to cybersecurity threats and all compliance risks within the target's information systems, as well as all risks that arise as a result of the target's administrative and operational practices.

Highly sophisticated threat actors target M&A activities because they offer the potential for short-term and long-term reward. With operations in transition, high-value data is often vulnerable. When publicly held companies are involved, the resulting media coverage can exacerbate the risk that threat actors will seize the opportunity to attack.

Furthermore, the data of the company being acquired/divested may not be the ultimate target. Instead, it may serve as an expedient way to break into the acquiring company. This is an entirely different category of advanced persistent threat (APT): one that is carried over into the newly merged company by mistake. This tactic underscores the importance of cybersecurity oversight during M&A activities.

More than one in three executives surveyed said they have experienced data breaches that can be attributed to M&A activity during integration.

Engaging CISOs in the M&A lifecycle

Chief Information Security Officers (CISOs) and their teams are key to protecting the assets and brand reputation of acquirers. They should play a significant advisory role in all activities of the M&A lifecycle (see Figure 1).

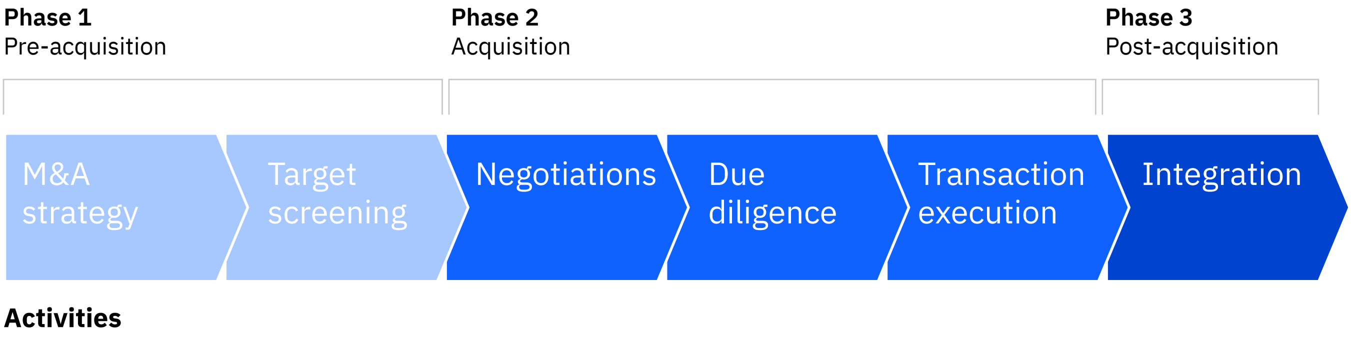
All too often, CISOs learn about, or are asked to engage in, acquisitions late in the deal lifecycle. This exposes organizations to significant risk, for example, when a breach occurs immediately post-acquisition.

In Q4 2019, the IBM Institute for Business Value (IBV) surveyed 720 executives responsible for the M&A functions at acquirer organizations. More than one in three said they have experienced data breaches that can be attributed to M&A activity during integration. Almost one in five experienced such breaches post-integration.[9]

There are several reasons why companies delay or disregard engaging security experts during M&A. In some cases, it's attributable to inexperience with the complex M&A lifecycle. In others, there may be a desire to limit the number of people with knowledge of an impending merger. Restricting "line of sight" to a potential merger is understandable during the pre-acquisition phase; however, excluding risk and security domain experts is problematic as security and compliance issues represent potential liabilities.

Figure 1

Throughout the M&A process, security teams need to stay engaged



Source: IBM Institute for Business Value benchmark study, 2019; n =720.

More than half of companies wait until due diligence is completed to perform cybersecurity assessments.

Why timing of discovery is so pivotal

It's critically important that potential liabilities are identified and accounted for in M&A deal valuation, and reflected in purchase, sale, and transition service agreements. Yet, more than 50 percent of companies wait until due diligence is completed to perform cybersecurity assessments to investigate and identify the cybersecurity and data privacy risks and liabilities posed by M&A transactions (see Figure 2).[10]

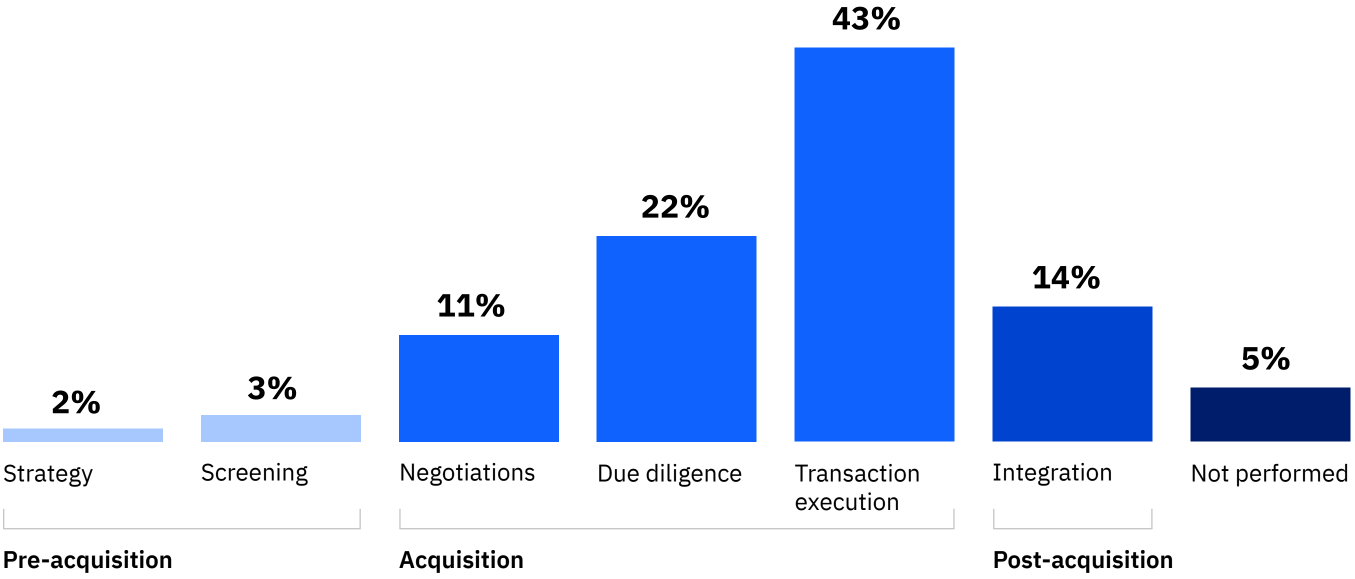
Respondents were also asked about their M&A governance and execution models; M&A organization and process maturity; and M&A tools, such as automation of workflow/process, and the application of analytics and AI throughout the M&A lifecycle.

Thirty-two percent have sophisticated M&A capabilities and achieve better outcomes from their M&A activity. Almost 60 percent of these organizations have CISOs and information security teams start assessing the cybersecurity posture of potential targets earlier in the M&A lifecycle.[11]

With some businesses more exposed financially and operationally than before the pandemic started, and others looking to add capability and reach, it makes sense to look at how cybersecurity fits in each of the three M&A lifecycle phases.

Figure 2

When organizations perform a comprehensive cybersecurity assessment



Source: IBM Institute for Business Value benchmark study, 2019; n =720.

Phase 1: Pre-acquisition

A security team can take a variety of actions to review the security posture of potential targets as early as target identification and screening.

Ideally, security representatives should work with the corporate development team to define a clear process for the commitment of security expert resources. This can help strengthen protection, assessment, and regulatory compliance in each activity in the M&A lifecycle, starting with strategic planning.

As simple as it seems, the most straightforward step is a review of publicly available materials. A comprehensive review of news articles and public filings can uncover any security breaches that have been disclosed. A similar review of social media may reveal items that may not have garnered public attention.

The search for the undisclosed or unknown

At a deeper level, a review of the "dark web," which is the part of the internet that is not accessible by typical search engines, is important. Estimates suggests that 60 percent of the dark web has materials that may be harmful to businesses.[12] Enterprises lacking the skills to undertake such research can find third-party consulting firms with deep experience in handling these types of reviews.

Prior to and during due diligence are the best times for acquirers to assess a target's security operating model. Application of additional security oversight should be responsive to, but also accommodated by, proposed deal timelines. An important, often overlooked consideration is that M&A presents an opportunity to simplify and streamline cybersecurity operations. Modernizing operations as part of post-merger integration requires even more careful analysis and planning.

Insight: Security implications of divestures

While mergers typically garner more attention, divestitures are also a component of M&As with important security requirements. Global or geographically-distributed digital operations share many back office systems and data stores. However, a divesting company is often selling only a part of its overall business. That makes access and control of data vitally important.

Consider the case of one company selling a piece of a business to a competitor. Managing access to applications that may hold much more data than is being sold can be a significant issue.

For example, a digital media company is selling one of two engagement platforms to a competitor. However, it operates a single core application that captures customer data from both platforms. The divesting company needs to establish control measures to separate and cleanse data to keep it out of reach of prospective competitors. Furthermore, this deal requires assessing data lifecycle and data retention considerations, privacy concerns, and customer-notification requirements.

Maintaining a strong security posture through the entire process is important for the divesting company because it promotes trust and transparency among participants and instills confidence with current and future customers.

Risk and security concerns, as well as opportunities generated by enhanced cyber resilience, are some of the most important financial considerations in any deal.

Pre-acquisition security assessments should help the acquiring company properly evaluate the merits of an offer, the size of the offer, and any potential discounts or clawback mechanisms. Undisclosed data breaches are deal-breakers for most companies (see "Insight: The impact of data breaches on value" on page 2).[13] As a premium is often paid to acquire a business, it's critically important that potential liabilities are identified to keep the premium in line with overall value.

More than 20 percent of companies say insufficient focus on cybersecurity during due diligence and integration is one of their top three M&A-related challenges.[14] This represents a clear opportunity for improvement.

Phase 2: Acquisition

During due diligence, organizations will want to identify potential security issues that create financial exposure, compliance issues, and other risks. Assessing the target's security posture, specifically current security practices and operational vulnerabilities, is crucial to understanding the level of potential risk.

In addition, suppliers and partners should be assessed. A company's entire supply chain is a potential source of risk. This is especially true for acquiring companies that may not be familiar with the target's value chain or ecosystem.

Risk and security assessments with carve-outs and clawback mechanisms are vital to deal valuation terms because issues that surface during due diligence can negate the value of a deal. Sixty-one percent of respondents in the 2019 IBV Benchmarking survey cite compliance issues as the number one reason for their decisions not to proceed with M&A deals. Thirty-five percent said they found cybersecurity risks to be too great for a deal to proceed.[15]

Phase 3: Post-acquisition integration

Though it may be difficult to quantify risks in dollar terms, finding data or compliance issues is generally least costly when found prior to deal close.

Consider the following: on average, companies devote up to 7 percent of their total annual revenue toward executing M&A activities, more than 80 percent of which is spent on the acquisition and post-close integration phases (see Figure 3). If a cybersecurity issue or potential liability found during screening (pre-acquisition) is significant enough to disqualify a target, this could translate to a substantial operational cost avoidance.

Yet for many organizations, cyber risk and cybersecurity operations planning takes place late in the M&A lifecycle—after deal valuations are established. Risk and security concerns, as well as potential cost savings, are easily overlooked (or undervalued) unless they are translated into financial terms and intentionally factored into deal valuation models.

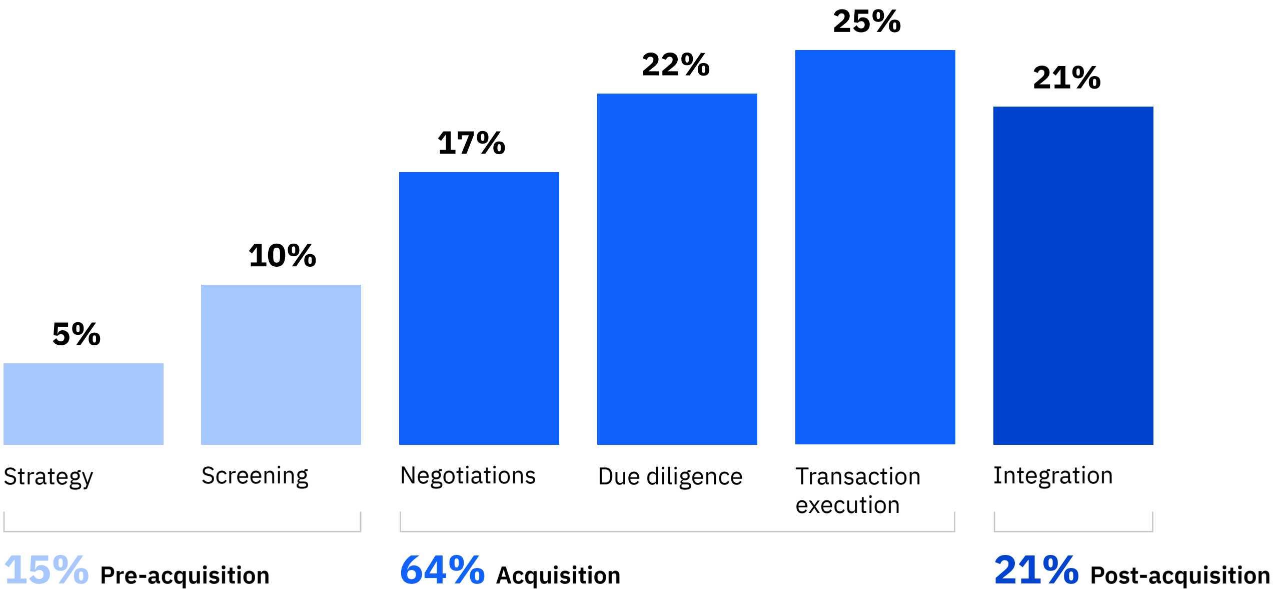
Determining the optimal degree of integration

Once the organization has made the decision to acquire or divest, it needs a plan to remediate compliance concerns, address risk exposure, and integrate security operations—where appropriate. This starts with a consolidated technology, security, and operations roadmap.

Finally, acquirers should consider the merits of maintaining discrete operations with separate business and operating models. If the assets of the target will merge with core business operations, then integration is called for.

Figure 3

Distribution of M&A cost by phase



Source: IBM Institute for Business Value benchmark study, 2019; n =720.

There are a host of considerations that determine the desired level of integration. Post-merger organizations may choose to define a new cyber risk profile based on a small set of common security controls, then maintain separate operations and security controls with limited data exposure across functional or geographic boundaries.

Alternatively, post-merger organizations may choose to fully integrate back office operations and consolidate data stores in order to drive value. This requires a more comprehensive assessment of cyber security strategy, including a new cyber risk profile and security controls consistent with new operational demands.

With the increase in cyber risk arising from COVID-19 disruption, organizations need to re-assess their current risk profile and cybersecurity posture. This is especially true for organizations considering acquisitions or divestitures. Engaging in-house and third-party experts at each phase of the mergers and acquisitions lifecycle can make a substantial impact on future value realization. Given the importance of digital engagement platforms, proprietary data, and customer privacy and compliance concerns, cyber risk and cybersecurity considerations can mean the difference between M&A success or failure.

Action guide

Cybersecurity risk in mergers and acquisitions

There are a number of proactive measures organizations can take to reduce cybersecurity risk throughout the M&A lifecycle.

Pre-acquisition actions:

- Make sure cyber risk and cybersecurity experts are included as key members of the M&A team, preferably as part of an ongoing operational practice and not on a case-by-case basis.
- Understand the acquisition in terms of business goals and brand objectives and articulate how they are enabled by security.
- Assess the cybersecurity resilience of a target. Identify relevant information on prior attacks, incidents, and public filings to determine potential business risks and liabilities.
- Begin to assess the regulatory and compliance requirements of the target being acquired based on impacts to the acquiring organization's technology and security operating models.

Acquisition actions:

- During due diligence, conduct detailed cybersecurity examinations of the target's information systems, tools, policies, and regulatory positions to identify security gaps, risks, and potential liabilities.
- Translate your findings into specific monetary values for pricing and negotiation considerations. Consider establishing a contingency fund to be held in escrow for potential exposures that may occur after closing.
- Monitor media coverage to gauge public interest and potential threats.
- Conduct a detailed cost of acquisition evaluation, including aligning security for base services, such as email and file sharing; more complex services, such as development tools and methods; and administrative concerns such as managing software licenses and network access. Risk management and cybersecurity costs associated with the acquisition should be factored into deal valuation terms and subject to negotiation.
- Consider engaging third parties that offer "brand protection tools," "penetration testing," or "risk quantification tools." Supplement internal teams with partners offering specialized M&A skills, such as technology infrastructure, operations, risk and cyber, and security domain expertise.

Post-acquisition and post-merger integration actions:

- Refresh the target and security operating models established during due diligence with new topics from assessment activities. Build a detailed integration roadmap.
- Maintain high security vigilance and monitoring at both companies for increased threats due to media exposure. Develop a playbook for isolating emergent risks.
- Keep tight controls in place. During integration there may be some sense of relaxation of security protocols that could be exploited as networks are combined.
- Anticipate M&A-related impacts to the workforce and factor these into risk planning. This includes employees and partners who may be negatively impacted by the deal.
- Leverage the M&A process to enhance cyber resilience. Streamline risk and security operations and reinforce the role of trust as a common cause connecting suppliers, partners, and customers.

Notes and sources

[1] Kirk, Jeremy. "Yahoo Takes $350 Million Hit in Verizon Deal." Bank Info Security. February 22, 2017. https://www.bankinfosecurity.com/yahoo-takes-350-million-hit-in-verizon-deal-a-9736

[2] Cimpanu, Catalin. "Gambling company to set aside $30 million to deal with cyber-attack fallout." *ZDNet*. April 10, 2020. https://www.zdnet.com/article/gambling-company-to-set-aside-30-million-to-deal-with-cyber-attack-fallout/

[3] "COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications." World Economic Forum. May 2020. http://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf

[4] Perlberg, Heather. "Rescue Cash Too Hot for KKR Proves Irresistible to Many PE Peers." *Bloomberg Law*. July 2, 2020. https://news.bloomberglaw.com/banking-law/private-equity-on-edge-with-u-s-plan-to-name-relief-recipients

[5] Hankins, Kristine W. and Mitchell Petersen. "Why Are Companies Sitting on So Much Cash?" *Harvard Business Review*. January 17, 2020. https://hbr.org/2020/01/why-are-companies-sitting-on-so-much-cash

[6] Weise, Elizabeth. "Uber paid hackers $100,000 to hide year-old breach of 57 million users." *USA Today.* November 22, 2017. https://www.usatoday.com/story/tech/2017/11/21/uber-kept-mum-year-hack-info-57-million-riders-and-drivers/887002001/

[7] Khosrowshahi, Dara. "2016 Data Security Incident." Uber Newsroom. November 21, 2017. https://www.uber.com/newsroom/2016-data-incident

[8] Nolter, Chris. "Uber's Rough Year Ends With Big SoftBank Investment." *The Street*. December 19, 2017. https://www.thestreet.com/markets/mergers-and-acquisitions/uber-s-rough-road-leads-to-softbank-deal-14431727

[9] IBM Institute for Business Value M&A Benchmark Study, 2019, unpublished data.

[10] Ibid.

[11] Ibid.

[12] Guccione, Darren. "What is the dark web? How to access it and what you'll find." *CSO*. March 5, 2020. https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html

[13] "The Role of Cybersecurity in Mergers and Acquisitions Diligence." Forescout. 2019. https://www.forescout.com/company/resources/cybersecurity-in-merger-and-acquisition-report/

[14] IBM Institute for Business Value M&A Benchmark Study, 2019, unpublished data.

[15] Ibid.

About Benchmark Insights

Benchmark Insights feature insights for executives on important business and related technology topics. They are based on analysis of performance data and other benchmarking measures. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
September 2020

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an "as is" basis and IBM makes no representations or warranties, express or implied.