INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

APRIL 2023

Managing Insider Risk During Mergers and Acquisitions

Presented by

INSA'S INSIDER THREAT SUBCOMMITTEE

Building a Stronger Intelligence Community

EXECUTIVE SUMMARY

Corporate mergers and acquisitions (M&A) create significant security risks and vulnerabilities for both the buyer and seller. Large amounts of sensitive information are exchanged outside each company's normal security construct; changes in corporate culture and a climate of uncertainty could exacerbate employee anxieties; and the integration of new technologies may undermine a company's network defenses. In such an environment, the risks of insider threats increase, with potentially catastrophic consequences.

Globally, 62,000 M&A occurred worldwide in 2021 alone, amounting to more than $5.1 trillion in deals.[1] The defense industrial base (DIB), which collectively supports the Defense Department and the Intelligence Community with advanced technology and services, has seen many M&A in recent years. According to a Defense Department report on competition in the DIB, the defense sector has consolidated from 51 to 5 prime contractors since the 1990s, with defense industry M&A volumes ranging from $4.5 billion to $11 billion annually since 2001.[2]

Until a proposed merger is publicly announced, few people are likely to be aware that a merger is being considered. Typically, only C-Suite executives and board members are involved in such discussions, with financial analysis and legal assistance generally outsourced to investment banks, outside counsel, and other external advisors. Once an M&A is announced, the potential for data loss, data theft, or other personnel risks driven by insider threats increases significantly, as organizations attempt to balance the transparency necessary to assure their investors and employees with the need to keep some plans (e.g., for restructuring, layoffs, etc.) under wraps.[3] At this point, threats from insiders typically appear in three common forms:

First, M&A deals risk data loss by direct employee action. The potential disruption from a merger increases the likelihood of malicious theft, destruction, or release of sensitive data. For example, individuals from either side of the transaction who feel threatened, overlooked, or cheated by the pending action are more likely to steal data or compromise systems–either to punish their organization or to set themselves up for success in a new role elsewhere.[4]

Second, negligent insiders may compromise data throughout the M&A process. Due to the need for confidentiality, even after the merger or acquisition itself is announced, M&A activity can generate stress and anxiety among a company's workforce. According to a 2022 *Harvard Business Review* article, employees are much more likely to fail to follow cybersecurity protocols when experiencing stress.[5] Employees experiencing uncertainty, anxiety, fatigue, or time pressure because of the M&A deal may unwittingly or inadvertently introduce vulnerabilities (e.g., malware, etc.) into the technical environment.

Third, personnel at either the acquiring or target organization can sabotage the deal through reputational risk or brand damage resulting from adverse activities such as fraud, sexual harassment, substance abuse, or other unethical behavior.

Despite the potentially significant effect of these insider risks, many organizations fail to include or prioritize personnel risk indicators or insider risk practices throughout the M&A process. If insider risk is considered at all, it frequently occurs as an afterthought to satisfy compliance checklists. Organizations must move away from this ineffective and reactive paradigm and instead prioritize bringing insider risk stakeholders into the three significant stages of the M&A process: pre-deal, the diligence process, and post deal conclusion.

INTRODUCTION

The range of companies whose intellectual property (IP), operations, and personnel are placed at risk by mergers and acquisitions (M&A) is enormous. Globally, 62,000 M&A occurred worldwide in 2021 alone, amounting to more than $5.1 trillion in deals.[6] While loss of IP or sensitive data by individual companies can jeopardize shareholder assets, insider threats in some sectors–particularly the defense industrial base (DIB)–also imperil technologies and information that are critical to U.S. national security.

The DIB has seen a large number of M&A in recent years. According to a 2022 Defense Department report on competition in the DIB, the number of prime contractors consolidated from 51 to 5 since the 1990s.[7] Across the sector, defense industry M&A volumes have ranged from $4.5 billion to $11 billion annually since 2001.[8] The DIB shrank by 20 percent, from 85,000 companies to 68,000, in a five-year period following defense spending reductions mandated by the 2011 Budget Control Act.[9]

During an M&A, the potential for data loss, data theft, or other personnel risks driven by insider threats increases significantly, as organizations attempt to strike a balance between the transparency their investors and employees expect with the discretion required to prevent opposition from derailing the business deal.[10]

WHY ARE M&As HIGH-RISK ENVIRONMENTS FOR INSIDER THREAT?

Until a proposed merger is publicly announced, few people–typically, only C-Suite executives and board members–are likely to be aware that a merger is being considered. Financial analysis and legal assistance are generally outsourced to investment banks, outside counsel, and other external advisors who have little motivation to leak information; for them, a deal is just a deal, as they stand to gain or lose little (except for billable hours) from its success or failure. Sometimes, however, corporate executives make it well known that a company is seeking to be acquired or is entertaining offers from suitors; in such cases, reporters, investors, and competitors swarm in search of information, which a self-interested and well-placed insider could readily provide to the detriment of the company.

Regardless of acquisition type, the introduction of a new company and its integration brings an element of risk to the acquiring company. It is a vulnerable business situation for both the buyer and seller because sensitive information is being exchanged between multiple individuals outside the company's normal security construct. It also creates instability within each company's corporate culture and a climate of uncertainty that could lead to employee disgruntlement or job security anxiety. How a company defines and addresses insider risk, beyond compliance with minimum regulatory requirements, is often underexamined or incomplete.[11] Moreover, the misalignment, or lack of insider risk programs, often decreases the insider risk mitigation posture, which can produce disastrous consequences.

Additionally, the integration of new technology into existing products and capabilities may affect a company's ability to both detect malicious actors and protect against them. Kurt John, Chief Cybersecurity Officer at Siemens USA, noted M&As are a "variant of the supply chain attack…larger companies are snapping up smaller companies."[12] He hints these smaller companies may be compromised in the near term, and "hedging their bets for when an acquisition happens so that they get a foothold into a larger organization."[13]

The chaotic transition from two organizations to one can create process and technology challenges that delay the establishment of a mature insider risk program at the new merged organization. This can prevent vetting of new employees and risk

monitoring of the existing employee population. If not properly vetted during pre-hire and onboarding, and then enrolled in a robust continuous insider threat program, insider threats from personnel may have cascading effects. Both new and current employees may introduce risk into the new company. Individual employees may already have crossed the line and be an insider threat.

> During an M&A, the potential for data loss, data theft, or other personnel risks driven by insider threats increases significantly, as organizations attempt to strike a balance between the transparency their investors and employees expect with the discretion required to prevent opposition from derailing the business deal.

CURRENT ISSUES

In general, current M&A risk diligence practices fail to adequately account for insider risk concerns throughout the three main stages of a deal. A survey of recently published material from consulting firms and other subject matter experts indicates that most M&A-related personnel risk assessment are primarily focused on employee retention and successfully merging corporate cultures than on managing insider risks.[14, 15, 16] Reputational and business risks stemming from past events–such as cyber breaches, workplace violence, toxic leadership, sexual harassment, and drug and alcohol abuse–could jeopardize the deal from closing or impact the overall valuation of the company being acquired. Additionally, business risks stemming from future insider threat vulnerabilities–such as the theft of intellectual property by an employee whom the merger disadvantaged–are rarely assessed before the deal is concluded. To best prevent these consequences, acquiring organizations should consider insider risk at three stages of the process:

PRE-ACQUISITION: MATURITY, CONTINUITY, FRAMEWORK

The pre-acquisition stage is a valuable opportunity for both the target and acquiring organizations to set the conditions to prioritize inclusion of insider risk indicators as part of the pre-M&A diligence and vetting process, and to involve as many stakeholders as possible as early as possible. Particularly in the case of companies known to be acquisition targets, it is critical to involve insider threat professionals at this early stage to prevent espionage or leaks that could jeopardize a deal.

Companies' chief information security officers (CISOs) and chief human capital officers (CHCOs) must be brought into M&A discussions on day one. Both executives are positioned to assess risks and vulnerabilities among their organization's workforce and networks. They can task their teams and/or insider threat program teams to evaluate potential risks without revealing that a merger or acquisition is being considered. Such assessments can enable a company to mitigate risks–by limiting access to sensitive data, enhancing user activity monitoring on networks, identifying categories of employees who may be disadvantaged by the merger, and increasing the amount of insider threat awareness training for employees–before the business deal becomes widely known.

Purchasers should also account for insider risk in their pre-acquisition diligence process to ensure they do not acquire a company with deep internal security risks. Similarly, the acquisition target has a responsibility to ensure that poor insider risk practices neither create risks that undermine its value nor jeopardize the deal. While it is impossible to foresee all issues that could arise from an acquisition, the pre-acquisition stage is the time for industry to ensure that all risk-focused stakeholders, including insider threat teams, are involved in the due diligence process.

Although the secrecy inherent to corporate M&As limits public disclosure of insider threat failures, the following examples have made their way into the public realm.

– Within the past three years, a *Fortune 500* company ("Parent") engaged in selling a smaller subsidiary company. The insider risk team at the Parent was "engaged in M&A activity only after the transaction was publicly announced to all three companies, at which point any number of actors who felt aggrieved by the announcement could have begun to engage in harmful activities. The insider risk team's high-level assessment, which was only completed

mid-way through the acquisition, unearthed gaps in the due diligence process."[17] Specifically, the assessment uncovered significant personnel risk behavior on the part of the company's key personnel. Through legal action, the selling company was awarded "roughly $1 million to recoup costs related to the M&A activity."[18] This significant finding would have been avoided if insider risk program personnel were able to evaluate the impact of inheriting workforce risk earlier in the process.

- In 2001, when both Proctor and Gamble (P&G) and Unilever were competing to acquire Clairol, P&G was found culpable of illegal intelligence gathering when the company "confessed to rifling through the trash to gain information on rival Unilever's hair-care business."[19] Though P&G ultimately succeeded in acquiring the company, it was forced to pay $10 million in compensation to Unilever.[20] P&G's dumpster diving highlights that insiders don't have to be malicious to disclose information about a pending merger; carelessness by Clairol employees exposed information that a suitor could have used to its advantage in negotiating the purchase.
- In 2019, a malicious employee conducting corporate espionage pre-deal put a significant acquisition in jeopardy. The London Ritz Hotel had received several acquisition bids of almost $1.3B but was forced to sell for less than half its market value after one of the owner's nephews was caught bugging the hotel conservatory to uncover private conversations.[21, 22]

MID-ACQUISITION ASSESSMENTS: PREVENTING LOSS THROUGH NEGLIGENCE OR IGNORANCE

The Mid-Acquisition stage represents the highest risk and deal vulnerability because the acquiring company is assessing enterprise risk, remediations are in process or have not yet taken place, and public communication about the M&A activity could allow for external bad actors to exploit gaps and target negligent employees through phishing, ransomware attacks, or other tactics.

There are three primary risk factors affecting this phase of an M&A deal.

1. The first is heightened stress to the workforce from the uncertainty surrounding the impact of the M&A to their careers. This stress could result in more cybersecurity breaches because of human error due to stress, fatigue, distraction, or anxiety, according to a recent report from a cyber threat monitoring organization.[23]
2. The second factor is the increased rate of targeting by external attackers attempting to take advantage of the uncertainty, increased volume of email communications, and weak security that characterize the M&A process.[24]
3. The third risk factor is the potential for one company's network security to be undermined by vulnerabilities in the other's. As both organization's networks are combined, malicious software present in one network could infect the other's, putting its data and computer security at risk. The network that is being incorporated into the larger whole must be quarantined until information security officers can ensure they are not importing new risks into the combined system. This network security diligence is especially critical when the company being acquired is substantially smaller than the purchaser, which makes it likely that its information security practices are less rigorous.

As the M&A process advances and becomes public, more attackers will appear seeking to target distracted employees through phishing and business email compromise attacks.[25] Exploiting companies during these time-sensitive transactions has even become a trend among criminal and nation state attackers.[26]

- Marriott's acquisition of Starwood hotels was affected by a high-profile hack of Starwood data during the acquisition process, which was enabled by a negligent insider falling prey to a phishing email. Although the hack was state-sponsored and led by an external party, it was executed through email spoofing. As a result of the breach, Marriott shares dropped almost 7%, and remedying the issues cost Marriott significant revenue and reputational damage. Hasty decisions made during pre-acquisition had downstream negative effects to the acquisition process and incorporated more risk to an already high-risk situation. This example highlights several missed opportunities to close risk gaps such as targeted comms to all employees with security awareness reminders, increased technical controls regarding email domains, and advanced threat assessments since this was one of the largest M&A activities in recent years.

– In 2022, Tassel Parent, a subsidiary of private equity firm KKR, completed their mid-acquisition assessments to acquire their target company, Graduation Alliance, Inc., for $130M. External bad actors exploited the communication challenges, complexity, and tight deadlines of the M&A process to conduct a business email compromise where a false email was sent to Tassel's paying agent, instructing them to "change banking details from Zions Bank in Utah to […] a Hong Kong bank with the payment made in the name of *HongKong Wemakos Furniture Trading Co."*[27] This request should have been an immediate red flag for any employee who had been trained to watch out for phishing and email scams, or any organization with a threat-based process in place to prevent individuals falling victim to these scams. However, the paying agent office made the change without confirming with anyone at the organization, and the $130M was lost.[28] This example highlights how people involved with an M&A may overlook small inconsistencies in emails since things across the company are changing and new people are getting involved. "By exploiting those changes and the pressure—real or perceived—to make the transition go as smoothly as possible, scammers tricked employees into making payments and sharing sensitive information."[29]

POST-ACQUISITION: PREVENTING THEFT FROM FEARFUL, MALICIOUS OR DISGRUNTLED INSIDERS

In the Post-Acquisition stage, the M&A has been completed and employees are discovering what this means for their new roles and career paths. This stage is high-risk for employee data theft. Preventative measures to monitor employee network behavior could prevent the theft of valuable company information, like intellectual property or financial records. Industry data shows that around 60 percent of employees leaving an organization by choice or through termination attempt to exfiltrate IP and other data as they leave.[30,31] Fear of layoffs can also contribute to hostile or malicious behavior and can drive an employee to purposefully take sensitive data "to either cause harm to the organization they're leaving or give themselves an advantage in their next venture."[32]

The examples below demonstrate failures to catch malicious theft of data that directly affected companies after a merger or acquisition.

– Anthony Levandowski, a founding member of Google's self-driving vehicle project, left the company to start Otto Trucking. Within eight months, Otto Trucking was acquired by Uber. Google claimed Levandowski stole autonomy technology trade secrets. It has been disclosed in court documents that Levandowski downloaded and copied proprietary files from Google onto his laptop before he resigned. While not directly stated, a lack of detective controls around data loss prevention and weak corporate policies regarding employee monitoring, especially around those leaving the company, made Google vulnerable to IP theft.[33] Because of an existing indemnification agreement stemming from the Otto acquisition, Uber was compelled to represent Levandowski's interests against Google. Under settlement, Uber agreed not to use any hardware and software from the acquisition and pay out a percentage of equity to Google. At the time, the equity payout was approximately $245M. Levandowski also faces 27 months in prison in addition to judgment against him of $179M for the data theft.[34] The insider threat posed by Levandowski impacted both the company from which he left and the acquiring company.

– In 2021, a system administrator feared layoffs after a merger. He "embedded malicious code within scripts on his organization's servers, which were responsible for managing prescription benefit plans."[35] The individual had set the logic bomb to go off in 6 months, but even after he survived the layoff and transition period, he did not disable the malicious code, and its execution would have caused "widespread financial damage," impact to 70 of the company's servers, and potentially serious health consequences for the company's customers. The event was discovered prior to the date of execution and the individual was sentenced to a fine and jail time, but it took several months for the company to discover the incident.[36]

SOLUTIONS AND RECOMMENDATIONS

When merging with a new company, the acquisition target's security ultimately affects the acquiring company's own security. The earlier examples highlighted insider risk themes regularly seen in the M&A process:

- Negligent insiders enabling data theft.
- Hostile or malicious insiders conducting data theft.
- Business risk introduced through employee actions.

To detect, counter, mitigate, or manage these risks throughout all stages of the M&A process, organizations should consider implementing the following best practices with the necessary compartmentation to protect the confidentiality of the deal:

1. **Treat insider risk as a critical element of the M&A diligence process.**

   Corporate leaders must treat insider risk considerations as a principal concern, rather than as an afterthought in the M&A diligence process. Security executives and insider threat program managers must be informed about potential risks in all M&A tasks. Importantly, insider risk stakeholders must be engaged in the earliest stages of the M&A diligence process.

2. **At the highest level, manage insider risk throughout all stages of the M&A process.**

   Pre-deal: Ideally, both companies would have robust insider risk awareness training conducted, and independent insider risk maturity assessments executed by outside specialists before the due diligence process, with any/all vulnerabilities addressed and mitigated. An automated whole person/whole threat continuous evaluation mechanism should be in place that creates efficiency and effectiveness for their trained insider risk analysts. Without unduly spreading knowledge of a potential M&A, corporate executives should identify security vulnerabilities, such as inadequate information security practices. They should also identify teams or categories of employees who may lose responsibility and/or stature because of the merger, as these team members may have a higher likelihood of reacting maliciously.

   During M&A Diligence: Both organizations should focus on preventing loss through negligence or ignorance. The companies should ensure that continuity plans are in place to reduce redundancy and vulnerability as two disparate corporate cultures and computer networks are combined into one. Additionally, a mission owner should be identified for insider risk education and increasing employee awareness (particularly around phishing and business email compromise scams to ensure that employees maintain a threat-based mindset throughout the chaotic period of the M&A deal).

> The most impactful action for companies involved in an M&A deal to take is involving insider risk stakeholders early and consistently throughout the M&A process.

Then, the acquisition target company should make insider risk governance documentation and risk maturity assessments available so that the acquiring company can identify potential issues in the M&A process before they create vulnerabilities that put the deal in jeopardy.

To do so, it may address the following points:

- How does the target organization define insider risk?
- Do they seek to manage insider risk, or just cover compliance risk?
- Is there budget and support for an insider threat program?
- What are the elements of their insider risk program?

- Do they balance physical, cyber, and human risk?
- How do they address potential risks introduced via third party contractors?
- How do they conduct insider risk training?
- Do they have a risk board or formal insider threat program office?
- Is the insider risk program integrated with the cybersecurity program?
- Do they have a tool to track and support insider threat capability?
- Are there definitional insider risk differences between the companies?
- Could these differences result in employee disgruntlement or challenge?

Post-deal: The acquiring organization should have technical and non-technical processes in place that can identify patterns of concern in employee behavior. They should monitor employee behavior to ensure that stress or disgruntlement is not leading to malicious behavior, data theft, economic espionage, or other exfiltration of intellectual property. Following the M&A, companies should identify the alignment of insider risk with the new organization's enterprise risk strategy, reassess the new organization's insider risk, identify the most valuable assets meriting enhanced protections, and refine the overall insider risk mitigation strategy. This equates to merging the best practices of each company's insider threat program. Develop, or obtain a 3rd party red-team and execute a plan to integrate people, processes, and technology efficiently and effectively. Post-merger actions will need to include new consent banners, new employment agreements, NDAs, non-competes (if authorized by law), and new policies. Determine exactly who has access to sensitive materials. Continuous evaluation of employees for early warning of potential insider indicators. If warranted, conduct new background checks against newly established standards.

CONCLUSION

As the rate of M&A deals increases in the post-pandemic environment, it is critical for companies to consider the potential to onboard risk via this threat vector, which has already been exploited by malicious actors in numerous recent deals. Throughout the case studies across all stages of an M&A deal, a key commonality is the need for proactive risk flagging to identify and respond to indicators before a compromise or vulnerability occurs that could jeopardize the deal or result in catastrophic intellectual property loss. To protect the confidentiality of potential deals, effective compartmentation of insider risk activity must be maintained. Failure could not only derail a merger; it could reveal intellectual property or valuable data that cripples one or both companies or, in the case of DIB companies, expose sensitive national security information.

The most impactful action for companies involved in an M&A deal to take is involving insider risk stakeholders early and consistently throughout the M&A process. Key stakeholders should be assigned roles and accountable actions so that each partner's responsibilities during M&A due diligence can be defined along with risk impacts and potential mitigation strategies. Security best practices must be executed prior to public announcement and must continue during the acquisition assessment and after the deal has concluded.

In the end, each partner, stakeholder, and investor seek a successful merger or acquisition. Effective insider risk mitigation helps ensure this outcome by protecting sensitive information and technologies that underpin the value proposition.

REFERENCES

[1]"Global M&A Industry Trends: 2022 Mid-Year Update," PricewaterhouseCoopers, June 28, 2022. At https://pwc.to/3mWE2xL.

[2]Office of the Under Secretary of Defense for Acquisition and Sustainment, State of Competition within the Defense Industrial Base, February 2022, pp. 1, 4. At https://media.defense.gov/2022/Feb/15/2002939087/-1/-1/1/STATE-OF-COMPETITION-WITHIN-THE-DEFENSE-INDUSTRIAL-BASE.PDF.

[3]"Three M&A Security Threats to Keep on Your Radar," DTEX Systems, August 20, 2015. At https://www.dtexsystems.com/blog/three-ma-security-threats-to-keep-on-your-radar/.

[4]Jony Fischbein, "Insider Threats: How the 'Great Resignation' is Impacting Data Security," World Economic Forum, May 10, 2022. At https://www.weforum.org/agenda/2022/05/insider-threats-how-the-great-resignation-is-impacting-data-security/.

[5]Clay Posey and Mindy Shoss, "Research: Why Employees Violate Cybersecurity Policies," Harvard Business Review, January 20, 2022. At https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies.

[6]"Global M&A Industry Trends: 2022 Mid-Year Update."

[7]Office of the Under Secretary of Defense for Acquisition and Sustainment, p. 1.

[8]Office of the Under Secretary of Defense for Acquisition and Sustainment, p. 4.

[9]Andrew P. Hunter, Gregory Sanders, and Zach Huitink, Evaluating Consolidation and the Threat of Monopolies within Industrial Sectors (Washington, DC: Center for Strategic and International Studies, February 2019), p. 5. At https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190208_Sanders_Monopolies_WEB_v2.pdf. See also Rhys McCormack, Andrew P. Hunter, and Greg Sanders, Measuring the Impact of Sequestration and the Defense Drawdown on the Defense Industrial Base (Washington, DC: Center for Strategic and International Studies, December 2017), p. xiv. At https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180111_McCormick_ImpactOfSequestration_Web.pdf.

[10]"Three M&A Security Threats to Keep on Your Radar".

[11]Joe Payne, "Insider Threats: An M&A Dealmaker's Nightmare," Dark Reading, July 9, 2019. At https://www.darkreading.com/perimeter/insider-threats-an-m-a-dealmaker-s-nightmare.

[12]"Ask the Experts," Technology Reseller, March 26, 2022. At https://www.technologyreseller.uk/news/ask-the-experts/.

[13]"Ask the Experts," March 26, 2022.

[14]Robert W. Heller, "Managing Merger Risk during the Post-Selection Phase," dissertation, Georgia State University, 2013. https://doi.org/10.57709/4335144.

[15]Jeff Weirens, Olivier May, et al, "M&A Making the Deal Work: Perspectives on Driving Merger and Acquisition Value," Deloitte M&A Institute, 2017. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/mergers-acqisitions/us-ma-making-the-deal-work-compendium.pdf

[16]Colin G. Chesley, "Merging Cultures: Organizational Behavior, Leadership, and Differentiation in a Health System Merger," Electronic Theses and Dissertations, paper 3271 (2017). https://dc.etsu.edu/etd/3.

[17]Interview by INSA member W. Woolsey, May 27, 2022.

[18]Interview by INSA member W. Woolsey, May 27, 2022.

[19]"Building a Business Case for a Proactive TSCM Strategy," Esoteric, December 18, 2017. At https://www.esotericltd.com/2017/12/18/news-story-2/.

[20]"Building a Business Case for a Proactive TSCM Strategy," December 18, 2017.

[21]*Agence France Presse, "Ritz London Co-Owner Reveals 1 Billion Pound+ Offers for Hotel," Yahoo Finance, March 4, 2020. At https://finance.yahoo.com/news/ritz-london-co-owner-reveals-1bn-offers-hotel-133658955.html.*

[22]*Clive Coleman, "Sir Frederick Barclay's Nephew 'Caught with Bugging Device' at Ritz Hotel," BBC News, May 18, 2020. At https://www.bbc.com/news/uk-52699018.*

[23]*"Spear Phishing Threat Landscape 2021," Tessian Research, 2021. At https://www.tessian.com/research/spear-phishing-threat-landscape/.*

[24]*"FireEye M-Trends 2019: Hidden Phishing Risks During Mergers and Acquisitions," SecureSense, March 8, 2020. At https://securesense.ca/fireeye-m-trends-2019-hidden-phishing-risks-during-mergers-and-acquisitions/.*

[25]*Maria Korolov, "Merging Firms Appealing Targets for Attackers," CSO, March 30, 2016. At https://www.csoonline.com/article/3049402/merging-firms-appealing-targets-for-attackers.html.*

[26]*"Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims," private industry notification, Federal Bureau of Investigation Cyber Division, November 1, 2021. At https://www.ic3.gov/Media/News/2021/211101.pdf.*

[27]*Stu Sjouwerman, "Think BEC Won't Cost You Much? How Does $130 Million Sound?" KnowBe4, May 13, 2022. At https://blog.knowbe4.com/think-bec-wont-cost-you-much-how-does-130-million-sound.*

[28]*"When Legal Counsel's Emails Are Hacked and a Stockholder's Merger Consideration is Paid to the Hackers, Who is Liable?" Fried Frank M&A/PE Quarterly (Spring 2022). At https://www.friedfrank.com/siteFiles/Publications/FriedFrankM%26AQuarterlyApril2022.pdf.*

[29]*Raymond Lim, "M&As Put Your company at Risk for BEC Losses and Data Breach Liability," Agari Email Security Blog, January 17, 2019. At https://www.agari.com/email-security-blog/mergers-acquisitions-losses-liability/.*

[30]*Code42, "Code42 Incydr Series: Why Most Companies Can't Stop Departing Employee Data Theft," ThreatPost, November 4, 2020. At https://threatpost.com/code42-incydr-series-why-most-companies-cant-stop-departing-employee-data-theft/160879/.*

[31]*Fischbein, "Insider Threats."*

[32]*Fischbein, "Insider Threats."*

[33]*Nick Statt, "Former Google Exec Anthony Levandowski Sentenced to 18 Months for Stealing Self-Driving Car Secrets," The Verge, August 4, 2020. At https://www.theverge.com/2020/8/4/21354906/anthony-levandowski-waymo-uber-lawsuit-sentence-18-months-prison-lawsuit.*

[34]*Nick Statt, "Former Google Exec Anthony Levandowski Sentenced to 18 Months for Stealing Self-Driving Car Secrets."*

[35]*Dawn Cappelli, Andrew Moore, and Randall Trzeciak, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (New York: Addison-Wesley, 2012), p. 252.*

[36]*Cappelli, et. al., p. 252.*

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this paper.

INSA MEMBERS

Sue Steinke, *Peraton; Insider Threat Subcommittee Chair*

Julie Coonce, *Premise; Insider Threat Subcommittee Vice Chair*

Cathy Albright, *Thomson Reuters Special Services*

Jen Boone, *Booz Allen Hamilton*

Theresa Campobasso, *Exiger*

Michael Hudson, *ClearForce*

Val LeTellier

John Mendoza, *CGI Federal*

Matthew Novak, *JP Morgan Chase*

Wailohia Woolsey, *Palo Alto Networks*

Shawnee Delaney

Michael Gips

Frank Greitzer, *PsyberAnalytix*

Jeff Sauntry

Shawn Thompson

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Director of Communications and Policy*

Cassie Crotty, *Intern*

Emma McCaleb, *Intern*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and its 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S INSIDER THREAT SUBCOMMITTEE

INSA's Insider Threat Subcommittee researches, discusses, analyzes, and assesses counterintelligence and insider threat issues that affect government agencies, cleared contractors, and other public and private sector organizations. The Subcommittee works to enhance the effectiveness, efficiency, and security of government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private and academic sectors.

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

Building a Stronger Intelligence Community