Moving Left and Right

Cybersecurity Processes and Outcomes in M&A Due Diligence

Center for Long-Term Cybersecurity, UC Berkeley

A CEO under pressure to consolidate her firm's position in the market hears from her business development team that a smaller competitor is keen to merge. How does she weigh the business case for the merger against the risk that the smaller firm may have hidden cybersecurity liabilities? Under what conditions might her own firm's cybersecurity audit function (along with colleagues across other functions) be able to identify, address, and remedy these concerns before and after a potential merger?

Traditionally, data security, privacy, and governance concerns would rarely cross her mind as she determines whether to explore a potential deal. But in a world in which the prevalence and severity of cyberattacks are increasing, ransomware groups are targeting midsize acquisition targets, and states are working to regulate data security, privacy, and governance — even in "non-tech" — sectors, business as usual no longer represents a viable option, for executives or at the board level. In response to this reality, much has been made of building "risk-based" assessment tools, which attempt to characterize cyber threats and provide process-oriented indicators as to whether a firm is well-placed to address them. Yet these tools remain nascent and unevenly distributed, and they overwhelmingly focus on the due diligence phase. So, how might firms broadly think about addressing cybersecurity concerns during mergers and acquisitions (M&A) processes?

In this study, researchers from the Center for Long-Term Cybersecurity at the University of California, Berkeley engaged with academics and practitioners who are experts in M&A to develop a cybersecurity model framework that can serve as guide during an M&A process. The purpose is to systematically improve on current due diligence for security risk and build a system that evolves along with the risk environment. Unlike most existing models, this framework relies upon an end-to-end approach; improving cybersecurity risk management and oversight in M&A requires that firms integrate cybersecurity considerations through the entire M&A process.

Challenges of Current Approaches

Current approaches to addressing cybersecurity concerns during the M&A process underrepresent cyber risk, with the consequence of eroding deal value. A number of factors lie behind this phenomenon.

First, measuring the capacity of a firm to address cybersecurity mirrors many of the accounting challenges associated with M&A, which result from lack of visibility into the "state zero" of the acquired party or merger partner — and the risk that sellers may have incentives to misrepresent the true state of affairs. Known vulnerabilities, as well as past and ongoing breaches, represent a risk to the purchaser — most obviously following the completion of the deal, but also during the due diligence process. Efforts to create assessment tools for use by would-be purchasers have been complicated by the contention that no two deals are the same. This may help explain firms' reliance on assessment tools that focus on process — e.g., "does the seller have an executive responsible for information security?" — rather than outcomes, e.g., "can the seller point to past examples of breaches, characterize their threats and vulnerabilities, and demonstrate where interventions have

improved their cybersecurity?" To some extent, addressing cybersecurity risk requires addressing the broader "culture of secrecy" that often surrounds mergers and acquisitions.

Second, on the purchaser's side of the equation, behavior and considerations during due diligence are focused primarily on the management of financial risk, rather than security risk. Moreover, externalities associated with cybersecurity risks — from the risk of the deal being made public prematurely, to the downstream consequences of a seller's vulnerabilities — remain poorly understood. Any effort to build a model framework for addressing cybersecurity risk during M&A needs to consider the variety of actors engaged on both the purchaser and seller side of any transaction. Beyond these players, other actors, from bankers to specialist lawyers, also have an interest in the deal — and these may or may not have an appreciation as to how cybersecurity threats and vulnerabilities represent risks to the firms that they advise.

Third, security risks represent a moving target at various stages of the deal cycle, from the sourcing of targets to integration. For example, attackers preying on a seller's vulnerable systems may tip off the market that firms are exploring potential deals early in the process, or vulnerabilities might be introduced into the purchaser's digital network as the purchasing firm integrates the target firm's legacy programs.

Finally, while the timelines associated with the M&A deal cycle vary based on deal size and complexity, there is often significant time pressure to close deals (and integrate the two merging organizations), which prevents the conducting of in-depth cybersecurity assessments over time. When cybersecurity is only considered during due diligence, this problem is particularly pronounced.

"As a result of these obstacles, acquiring companies often do not have a full understanding of the cybersecurity risk associated with an acquired company or merger partner."

As a result of these obstacles, acquiring companies often do not have a full understanding of the cybersecurity risk associated with an acquired company or merger partner. This can lead to inaccurate valuation, as well as potential legal, financial, and reputational risk for the acquiring company, and can ultimately lead to underperformance of the merged entity.

Too often, decisions come down to a "gut check" by security executives, and there is no quantifiable framework for making security and C-suite executives' assessments observable, transparent, and subject to interrogation by the board. There may not even be a clear threshold for when to escalate security risk to the board. Of course, cybersecurity risk is not the only challenge facing M&A valuations and decision-making, but it is a significant one that is likely to become more important over time.

In our discussions, it became clear that the type of industry, maturity of the board, quality of CEO, quality of CIO/CISO, and size of the company drive the sophistication of cybersecurity risk considerations in M&A. On a scale of 1-10 (with 1 representing the least sophisticated and 10 representing the most sophisticated approach to cybersecurity risk management in M&A), participants suggested that larger companies on average scored a 5 while smaller companies score

a 2. This may not be surprising given the resources at the disposal of large versus small firms, but the distance from "10" in both cases is notable. Participants also noted that while cases such as Verizon-Yahoo and Marriott-Starwood – where cybersecurity liabilities have negatively affected the deal – have attracted a lot of notoriety, over time the market is getting a sense of examples where best practices have been observed (e.g., Safeway's merger with Albertson's, Blue Shield-Care1st, and multiple deals at Juniper Networks and HP — the latter after several bad experiences).

This project attempts to integrate insights and best practices into a broadly applicable model framework. Below, we outline the heterogeneity of M&A processes that need to be addressed by the model framework. Then, we examine the actors involved in M&A and their roles in managing cybersecurity risk. Finally, we outline the parameters of the model framework, organized by stages in the deal cycle and the business considerations, cyber risk questions, and desired outcomes across each stage.

The Heterogeneity of Mergers and Acquisitions

There are several motivations that lead firms to pursue an M&A strategy, including the potential to drive costs down through consolidation and achieving economies of scale; gain access to new channels of distribution; acquire new products, services, or new capabilities; gain new customers; access new countries or markets; and increase production capacity. Because of the variety of these goals, each M&A project tends to have its own unique set of questions and considerations.

During our study, we identified several variables that drive the heterogeneity of mergers and acquisitions. Those most relevant and with the most impact to questions surrounding cybersecurity risk include the plans of the purchaser concerning the level of integration, and the industry within which the purchaser and target firm operate. Below, we examine each in turn.

Types of Integration

The proposed level of integration between the firms represents an important variable that might condition due diligence requirements.

Empirically, the level of integration between the firms in a merger or acquisition falls along a continuum. We can point to examples of acquired firms being fully integrated into existing business units of the purchaser and, at the opposite end of the spectrum, acquired firms operating entirely independently. In a full integration, the acquired company loses its identity over time as the buyer combines the entities through a shared culture, operating infrastructure, distribution channels, and other policies and processes. In a partial integration, the day-to-day operations remain with the target company, while strategic planning and staff functions are merged into the parent company. However, the target company is kept as an independent and separate entity. A select number of staff functions might be consolidated for cost synergies, but the day-to-day operations and decision-making remain with the target company. Juniper Networks' 2019 acquisition of MIST and Cisco's 2012 acquisition of Meraki fit this category.

At the other end of the spectrum, firms may also engage in an M&A for the purpose of leveraging the human capital within the target firm – an "acqui-hire". Google's acquisitions of HTC's smartphone team and Deepmind or Facebook's acquisition of Drop.io in 2010 serve as prototypical examples of this type of M&A project.

Between these extremes lies a middle space, with acquired firms in various stages of integration. Interestingly, participants in the study noted that, even in cases where full integration is desirable, the process of integration takes time, and during that interstitial period, the acquiring firm can take on liability – legal, financial, and reputational – associated with the acquired firm. This in-between period marks an occasion where the cybersecurity audit carried out during due diligence – as well as a broader appreciation of data security, privacy, and governance concerns – are particularly important.

Sector-Specific Considerations

The NIST Cybersecurity Framework, a set of guidelines developed by the U.S. National Institute of Standards and Technology, provides a starting point for thinking about cybersecurity risk. Across interviews, participants noted that the externalities associated with cyber risks, such as theft of intellectual property or loss of personally identifiable information (PII), might vary across industries, and that standards already created for a given sector might provide a useful starting point for thinking about potential consequences of cyber risk.

For example, the financial services industry, which may face threats from organized crime, hacktivists, nation-state actors, and insider threats, will be most concerned with financial theft, theft of intellectual property, business disruption, destruction of critical infrastructure, reputational risk damage, and meeting regulatory requirements. Relevant standards associated with this particular industry include the Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), FFIEC (Federal Financial Institutions Examination Council) Cybersecurity Assessment, Basel III IT Operational Controls, and PaymentCard Industry Data Security Standard (PCI DSS).

Other highly regulated industries include healthcare, where health information technology related to patient information and access controls for medical devices are central concerns. Relevant standards associated with this sector include the Healthcare Insurance Portability and Accountability Act (HIPAA), and the Healthcare Information Trust Alliance (HITRUST), which was developed alongside the Common Security Framework (CSF) based on a variety of federal and state regulations, frameworks, and standards. Other standards that shape the current cybersecurity risk discussions related to engaging in government contracting include the Defense Federal Acquisition Regulation Supplement (DFARS), Cybersecurity Maturity Model Certification (CMMC), and Federal Information Security Management Act (FISMA).

Many view these requirements as idiosyncratic rather than systematized, however. At the very least, a target firm should make clear how they are meeting the requirements associated with the relevant sector-specific standards and, where only voluntary standards exist, explain the conditions under

which they are meeting these obligations (e.g., at Tier 2 of the NIST Cybersecurity Framework[1]). Respondents also noted existing standards and requirements from a variety of industries that might drive an appreciation of cyber risk in deal-making. Indeed, some participants noted that, in highly regulated industries, these standards and requirements may serve as a trusted baseline, potentially making cybersecurity concerns less germane to consider during the early stages of the deal cycle. Of course, this depends on the degree to which players in that industry adhere to those standards.

> ". . . it's also worth noting that a number of sectors (e.g., manufacturing, wholesale) have no industry-specific cybersecurity standards at all"

Of course, it's also worth noting that a number of sectors (e.g., manufacturing, wholesale) have no industry-specific cybersecurity standards at all.

M&A Actors

In addition to mapping the M&A space by outlining the ways in which M&A processes vary, we also consider the various actors involved in M&A. As outlined above, these actors may have diverging interests concerning the completion of a deal and how cybersecurity risk is described, measured, and ultimately impacts the likelihood of a deal and its price.

The beginning of the M&A process is typically kept among a few executives, primarily the chief executive officer, chief financial officer, and corporate business development team. As the details of the potential deal become public, other stakeholders (for example, bankers, lawyers, consultants, and third-party audit companies) are looped in on the agreement's details.

For the purposes of simplicity, our model framework assumes a set of key primary actors, given their importance to existing M&A practices related to cybersecurity. These include:

- Executives on the purchaser and target side of the deal responsible for establishing the deal price and embarking upon the M&A process.
- Business development professionals, who are primarily responsible for sourcing M&A deals to the benefit of the purchaser's business.
- Boards on both sides of the deal with a fiduciary responsibility to the shareholders or stakeholders on each side of the deal.

[1] The challenge with voluntary and non-binding standards like the NIST Cybersecurity Framework is that there are few costs associated with non-compliance, making it possible for a firm to conclude that it meets the "risk-informed" Tier 2 of the Framework even as it carries on with nominal cybersecurity practices.

- Cybersecurity professionals in an audit function who are traditionally tasked with carrying out a brief due diligence process, and who increasingly are tasked with strategic planning surrounding IT/cybersecurity integration post-merger. Related, IT and cybersecurity professionals within the target firm may be responsible for providing information during the due diligence phase of the deal.

A series of secondary actors, including lawyers advising on the deal and investment bankers financing the deal, also have interests that need to be taken into account when considering the treatment of risk in any particular transaction.

The degree to which these actors play a role during the M&A process varies across the deal cycle. In the section below, we outline the six stages of the deal cycle and use it as the basis for creating the model framework.

M&A Deal Cycle

In simplest terms, any M&A involves two phases: the "close the deal" phase and the "operationalizing the deal" phase. Within the close the deal phase, we identify four subprocesses: source target, target identification, due diligence, and deal close. Under operationalizing, there are two subprocesses: integration and learning.

1. Sourcing and Targeting

Sourcing and targeting primarily involve the corporate business development team (professionals who often have management consulting backgrounds), who translate a business's needs and examine the marketplace for potential acquisitions, in some cases with the aid of bespoke firms that specialize in this phase of the deal cycle. Those surveyed in this project noted that cybersecurity risk ought to be considered in this phase based on industrial sector and the disposition of the acquiring and target firm. During this phase, executives might also consider the relevance of cyber risk to the deal type, enterprise value, or otherwise the "secret sauce" that is being acquired. Indeed, if a firm is being acquired for human capital and will be shut down immediately following the transaction, cybersecurity concerns are less significant than when a firm is sought whose trade secrets are vulnerable to theft. Developing an initial high-level cyber risk assessment at this stage, based on exogenous data sources, represents a best practice.

2. Preliminary Negotiations

Upon the identification of a target acquisition, the two sides will begin negotiating on price and sign a letter of intent (LOI) and confidentiality agreements. Conversations between executives of the two firms are explicit at this stage.[2] Some participants in the study noted that this phase is where a deeper appreciation of cybersecurity risk might add considerable value as executives consider strategic, operational, leadership, and cultural fit. If nothing else, the conversations at this stage will start to shed light on management and governance and establish whether the

[2] In some cases, they are implicit during the preceding stage.

target firm has a C-level executive responsible for cyber risk and, if so, who this individual is. Participants also noted that there is considerable variation in how cybersecurity responsibilities are distributed across an org chart, with some firms organizing around a chief information officer (CIO) or chief information security officer (CISO), while others roll up responsibility for cybersecurity into the office of the chief operating officer (COO) or chief financial officer (CFO). While these choices are often interrogated by process-oriented evaluative frameworks that tend to reward having a CIO/CISO, this report does not make a normative statement as to which method for organizing the C-suite to address cyber risk is more appropriate, as these choices are largely dictated by sector and firm characteristics. More important than process are the outcomes of a particular organizational design. The goal of the acquiring company's M&A team can be to construct a preliminary cyber-risk assessment of the target company (aka "smoke signals") that can provide a guide for deeper investigation and validation during the due diligence stage of the deal.

3. Due Diligence

The due diligence phase is where existing cybersecurity audit functions are empowered to interrogate the cybersecurity standards and practices of the target firm. Currently, there are several checklists that firms use to quickly get a best sense of whether there are red flags that might lead executives to revisit deal terms or, in unusual circumstances, terminate the deal. The cyber audit function, like other audit functions during M&A, is primarily concerned with where target firm policies, procedures, and practices might lead to either liability or vulnerability for the purchaser.

Practices that might be examined during due diligence include reporting standards for cybersecurity incidents in line with appropriate regulatory standards; competence related to handling data (e.g., customer data, PII, and financial data); past audit paperwork; evidence of red teaming, pen-testing, and tabletop exercises (TTX) activities focused on cybersecurity concerns; and an evaluation of employees who are directly involved with cybersecurity-relevant functions (e.g., turnover statistics within IT and cybersecurity roles, if the latter exists). Also valuable are data and material related to past breaches, as well as steps the firm took to address them. Cyber audit functions might also interrogate training materials and HR-related data concerning insider-threat training and compliance with policies and procedures. Interviews and focus groups with rank-and-file employees also can provide useful data related to the practices of a firm.

This process must be both rigorous and fast, and so the cyber audit function should be engaged as early as possible in the deal cycle. A thorough, data-driven cyber-risk assessment produced at the conclusion of the due diligence phase can provide material information that is relevant to the deal terms, including deal valuation.

4. Deal Close

At deal close, executives internalize due diligence and come to a valuation to complete the transaction based on previously established ranges. Participants in this project noted that cybersecurity risk is likely to play an increasing role in driving the final price of a deal, particularly where IP represents the "secret sauce" associated with the deal.

5. Integration

In our study, it became clear that cyber audit teams that play a significant role in due diligence also have an important role to play during integration of the firms, at least where the deal type does not involve ceasing the operations of the target firm. Even in circumstances of a partial merger, where the acquired firm remains separate from the purchaser, there are cyber risks associated with shared supply chains, as well as any shared systems used for redundant applications (e.g., human resources, payroll, etc.). In the case of full integration, the cybersecurity audit develops a clear picture as to where immediate concerns are that need to be prioritized for remediation. This is often the period during which firms are most vulnerable, and where cybersecurity concerns often fail to come to the surface amid the drive to extract business value from the transaction. Proper assessment of cyber-risks during phases 1-4 can serve as an effective starting point toward developing a roadmap for the integration phase. Participants in the study highlighted that, in the absence of a sufficient understanding of cyber-risks, companies often engage in endless discussions and negotiations, leading to delays in the integration.

6. Lessons Learned

Every merger or acquisition offers an opportunity for functions across an organization to perform a post-mortem and get a sense of those aspects of the transactions that worked well and those that did not. Given the abbreviated nature of the due diligence process in many transactions, those firms that frequently engage in M&A activity are at an advantage in terms of finding the "smoke signals" associated with cyber risk, should they leverage opportunities to learn from past deals. Of course, current and future deals do not necessarily mirror those of the past, but recognizing cyber risk is an imperfect science, and firms should not waste the opportunity to learn from their experiences. It is also worth noting that insights derived from often-ignored constituencies might be worthy of consideration, including those from the target firm and the investing teams. We recommend a "whole-of-business" learning process with a core cybersecurity component, rather than a cybersecurity-focused post-mortem.

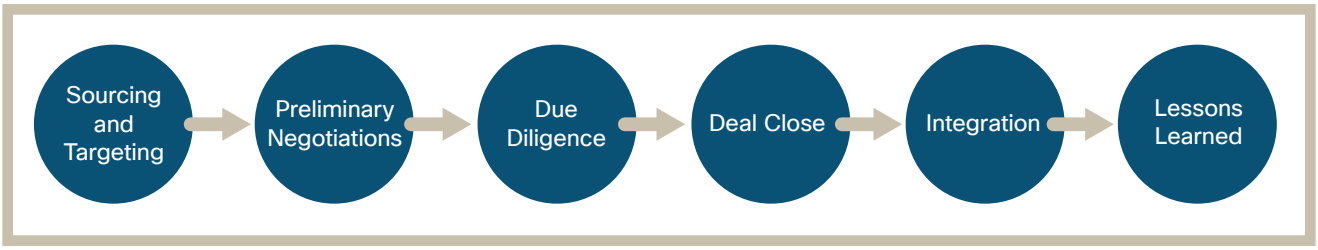

Figure 1: M&A Deal Cycle

As a growing number of academics and practitioners have noted, cybersecurity concerns are present across all six of the M&A stages outlined above. In practice, and to the extent that they exist on a continuum, cybersecurity audit functions already "move right" into the integration process based on the type of deal in question, as they have a head start in understanding the target firm and have an insider's perspective as to the capabilities of their own firm. Their "move left" is perhaps more controversial, as cybersecurity concerns impact the equities of business

development or other parts of the business that are proponents of a potential deal. Ancillary to these particular issues are concerns that executives are not cybersecurity-literate, as they in many cases come from other parts of the business, and that cybersecurity staff are ill-equipped to appropriately communicate with these constituents. These communication challenges are one motivation for creating a model framework that can support internal discussions as to how firms in varying sectors and of various sizes might start to think about moving both left and right.

Cybersecurity M&A Model Framework

The Cybersecurity M&A Model Framework addresses three primary factors: key business considerations, cyber risk questions, and desired outcome.

Key Business Considerations: First, we outline the key business considerations germane to each phase in the deal cycle. It is against these considerations that cyber risk questions are asked and answered.

Cyber Risk Questions: This phase requires asking, what are the questions that ought to be the focus of investing teams, executives, and cyber auditors at each stage of the deal cycle?

Desired Outcome: While process-oriented assessments offer a useful and necessary first step, purchasers in a merger or acquisition require assurances that data security, privacy, and governance concerns are taken seriously by virtue of resource allocation, and that these processes yield appropriate outcomes, understanding that the perennial problem for cybersecurity staff to "prove a negative" is present here. This final row outlines the conclusion that investing teams, executives, and cyber auditors ought to be able to draw at the end of each phase of the deal cycle.

This model framework avoids a checklist-based approach, but rather represents a starting point for firms to tailor their approach to the cybersecurity audit process during a merger or acquisition. While checklists are often deemed desirable as they can form the basis of a "systematic" process, they are also vulnerable to gaming by firms engaged in the M&A process and may not, in fact, reflect the sophistication of a firm's responses to specific threats and vulnerabilities that impact their business.

The model framework aims to serve as a tailored process that meets the needs of firms across deal types, industries, and firm size that meet their respective needs.

Cybersecurity M&A Model Framework

	Key Business Considerations
STAGE 1: Sourcing and Targeting (Evaluate M&A options)	Define acquisition type based on: · Business objectives · Company growth strategy · Acquisition type Acquisition criteria: · Cost structure · Operating model, such as absorb or stand-alone · Access to new customers, geos, markets, technology, and people skills Regulatory requirements by sector: · For example, financial services, healthcare, banking, and critical infrastructure
STAGE 2: Identify Target (Letter of intent and confidentiality agreement)	Identify target company: · Range of dollar spend for acquisition · ROI and deal valuation · Fit: strategic, leadership, culture, or operational
STAGE 3: Due Diligence (Terminate deal, resolve concerns, or ignore)	Due diligence areas: · Financial risks and liabilities · Legal structure and exposures · Operational synergies (leverage and optimization) · Integration roadmap (people, process, systems) · Environmental · Human capital retention · IP · Cyber risk validation and quantification
STAGE 4: Deal Close	Agglomeration of due diligence information will inform: · Deal terms, including valuation · Legal structure · Operating model · Governance and leadership structure
STAGE 5: Integration (People, process, systems, policies)	Deal type matters: · Integration roadmap (stand-alone versus partial versus full integration) · Scope includes people, process, systems, and policies · Costs for integration and revenue impact · Associated legal, governance, and leadership structure
STAGE 6: Post-Mortem (Learning)	Key learnings: · Board involvement · Executive involvement · Target firm feedback · Investing team feedback · Cybersecurity assessment and integration · Simplify and streamline key cyber risk questions

	Key Cyber Risk Questions
STAGE 1: Sourcing and Targeting (Evaluate M&A options)	Cybersecurity risk by sector: · Characterizing threat, vulnerability, and consequences for a modal cyberattack in the sector · Distribution of cyberattacks across sector · Matching cybersecurity considerations to business case (e.g., deal type) · Empirical record of attacks by sector
STAGE 2: Identify Target (Letter of intent and confidentiality agreement)	Cyber breach information for target from exogenous data sources: · News · SEC or other searchable filings Preliminary assessment from target leadership: · Governance (board oversight, expertise, level of rigor) · Management practices (ownership, oversight, CIO/CISO, reporting structure) · Cyber risk management strategy (design and program definition)
STAGE 3: Due Diligence (Terminate deal, resolve concerns, or ignore)	Cyber program management due diligence: Board governance: · Committee structure, reporting requirements, expertise and board seat for cybersecurity concerns, cybersecurity program oversight, and periodic assessment Executive functions: · CIO/CISO role; reporting structure; program, policies, and procedures; and training · QA/QC audit functions cybersecurity, including employee training, compliance, and third-party audits IT Layer: · Program ownership and management, reporting structure, program updates, third-party data, incident response plan, stress test program, inventory of digital assets, and risk assessment Ombudsman: · Training and education
STAGE 4: Deal Close	Cybersecurity integration planning: · Cyber audit conclusion as to urgent requests for remediation
STAGE 5: Integration (People, process, systems, policies)	Detailed cybersecurity integration roadmap: · Program management and resourcing · Governance and oversight of new company for cybersecurity program implementation and compliance · New company training
STAGE 6: Post-Mortem (Learning)	Integrating cybersecurity risk in future M&A processes: · Assessment of the role of cybersecurity audit across the deal cycle. · Was the cyber audit function moved “left”? · Moved “right”? · What are the sources of institutional friction when integrating cybersecurity risk considerations?

	Desired Cyber Risk Assessment Outcome
STAGE 1: Sourcing and Targeting (Evaluate M&A options)	Derive an initial high-level cyber risk assessment from exogenous data sources for sector/target companies: · Cyber risk quantification (high, medium, low) · Identify potential risk areas and exposure for consideration by executives
STAGE 2: Identify Target (Letter of intent and confidentiality agreement)	Derive a cyber risk assessment prior to due diligence (aka "smoke signals") of target company from: · Exogenous sources · Target leadership · Target firm filings · Target firm shared policies, procedures, data Risk assessment from this stage should provide guidance for validation during due diligence stage 3, primarily handled by cyber audit
STAGE 3: Due Diligence (Terminate deal, resolve concerns, or ignore)	Prepare a detailed cyber risk assessment for each of the five areas (board governance, executive functions, QA/QC, IT layer, and ombudsman): · Risk scoring on a scale of 1–5 · Heatmap with red, yellow, and green, with comments for further investigation and actions Executive cyber risk summary to inform the deal team
STAGE 4: Deal Close	Forecasting of integration challenges Preparation for proximate cyber threats and vulnerabilities unique to the acquisition
STAGE 5: Integration (People, process, systems, policies)	Alignment to the acquiring company program, policies, and governance Leverage best practices from target firm for NewCo (to include stock-taking for purchaser)
STAGE 6: Post-Mortem (Learning)	Simplify and streamline key cyber risk questions for future M&As Consideration of the place and role of cybersecurity audit across the organization

Process and Outcomes

The model framework outlined above is designed to support executives, cyber auditors, investing teams, and boards as they consider cybersecurity risk during the M&A process.

It provides a framework to consider the context and comparison in performance of a target firm against the broader industry. It also establishes where existing policies and procedures, along with historical patterns of attack, suggest that a target company's assets and vulnerabilities need to be protected. And it provides information that allows cyber audit functions to evaluate whether the target firm is following industry standards, whether voluntary or otherwise.

Across the various institutions and job functions that we engaged with, respondents noted the importance of engaging cybersecurity professionals early in the acquisition process – potentially alongside investing teams – while also engaging senior management and the company boards to consider information security liabilities as an aspect of deal-making. We look forward to hearing responses from the community as to the advantages of outcome-oriented due diligence and the spread of cybersecurity considerations both to the left and to the right across the deal cycle.

Future Work

As cybersecurity concerns are internalized as a unique risk within mergers and acquisitions, we expect that firms will learn valuable lessons related to threats, vulnerabilities, and mitigations. Future research ought to focus on collecting data related to cybersecurity outcomes associated with M&A. From this study, it became clear the degree to which insights were idiosyncratic and tied to years of experience in the space, with many of the cases that underpinned proposed solutions necessarily anecdotal. Indeed, a large-scale, systematic treatment of cyber risk and outcomes in the context of M&As is sorely needed.

Firms might also consider creating venues for sharing their own processes to internalize a model framework to address cyber risk, with academic participation to outline the variation between industries, firm type, and leadership culture.

About the Authors

Dr. Andrew Reddie is an Assistant Professor of Practice at the University of California, Berkeley's School of Information where he works on projects related to cybersecurity, nuclear weapons policy, wargaming, and emerging military technologies. He is also currently serving as Co-Faculty Director of the Center for Long-Term Cybersecurity. Andrew is currently a Bridging the Gap New Era fellow, Hans J. Morgenthau fellow at Notre Dame University, a non-resident fellow at the Brute Krulak Center at Marine Corps University, and deputy director at the Berkeley APEC Study Center. Previously, Andrew served as deputy director of the Nuclear Policy Working Group, predoctoral researcher at Lawrence Livermore National Laboratory's Center for Global Security Research, and as an associate at the Council on Foreign Relations in Washington, DC.

Prakash Krishnan is currently a full-time graduate student in the Master of Information and Data Science (MIDS) Program at the University of California, Berkeley's School of Information. Prakash holds an MBA in Marketing and a Master of Science in Industrial Engineering from the Ohio State University, Columbus, Ohio. Prakash brings rich business experience in M&As, corporate strategy, sales operations, and product marketing, having worked in leadership positions at Honeywell, Hewlett Packard, Cisco, and Juniper Networks.

Acknowledgments

The authors would like to thank the Center for Long-Term Cybersecurity at the University of California, Berkeley for providing guidance and help on this project, as well as everyone who engaged with our interviews and workshops. We would particularly like to thank Jacob Bolotin and Jason Button at Cisco for their insights and support, as well as Rudy Bakalov for his counsel and expertise. We also want to recognize Omar Garcia for his contributions to this project as a graduate student researcher. This project was made possible by a gift from Cisco in support of independent academic research.

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Center for Long-Term Cybersecurity

@CLTCBerkeley