Corporate Cybersecurity in the Context of M&A Transactions

Cameron Beck, Junior, William & Mary

Research Mentor:

Dr. Iria Giuffrida, Professor of the Practice of Law, William & Mary Law School, and Visiting Faculty for Business Law, Raymond A. Mason School of Business

Contents

I. Introduction

The rapid rise of digital devices has unlocked a new dimension of innovation and prosperity in the 21st century. Computers are now an integrated and ubiquitous part of our global culture. You would be hard-pressed to walk into any given room without several computer chips humming inaudibly inside the machines that facilitate our modern world. Even lightbulbs and doorbells are connected to the Internet, capturing information from the world around them and sending that information to the Cloud. The Internet expands access to communication, international marketplaces, entertainment, professional resources, and nearly every book in the world.

The sheer amount of information passing through servers is staggering. Every 60 minutes, 30,000 hours of video is uploaded to YouTube, a popular video and social media platform.[1] That equates to roughly 3.5 years of new footage every hour. Users upload more than 300 million photos to Facebook every day.[2] These incomprehensibly large chunks of information contain valuable pieces of data that can be used by companies to build models, analyze patterns, and visualize relationships. Simultaneously, this commoditization of data creates online opportunities and lucrative heists for skilled criminals.

In May 2021, the U.S.A.'s largest gasoline pipeline shut down after the operator suffered a cyberattack.[3] Hackers hacked into Colonial Pipeline's computer system and released ransomware, a type of code that seizes the system and is generally accompanied by demands for payment from the victim to have it unlocked. The Houston company carried nearly half of all gasoline and diesel fuel consumed on the East Coast. The attacker was not a terror group or state-sponsored collective, but an

[1] L Published by L. Ceci, "Youtube: Hours of Video Uploaded Every Minute 2020," Statista, April 4, 2022, https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/.
[2] Cooper Smith, "Facebook Users Are Uploading 350 Million New Photos Each Day," Business Insider (Business Insider, September 18, 2013), https://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9.
[3] Collin Eaton, "Cyberattack Forces Closure of Largest U.S. Refined-Fuel Pipeline," Ideal Cryptos | Cryptocurrency News and tips, May 8, 2021, https://www.idealcryptos.com/cyberattack-forces-closure-of-largest-u-s-refined-fuel-pipeline/.

organized criminal extortion ring. The attack caused panic buying at gas stations which induced shortages across the East Coast and Southeast.[4] Cybercrime is the fastest growing crime, expected to reach $10.5 trillion in costs by 2025.[5]

Corporations hold vast troves of aggregate data, and often are behind the curve on cybersecurity measures and threat detection. This is because shoring up defenses doesn't appeal to investors or offer avenues for future growth – in other words, it is seen as a sunk cost. Furthermore, society bears much of the cost resulting from corporate data breaches.[6] Insurance policies and tax reductions for corporations subject to cyberattacks let victims recover a significant portion of their losses in tax-write-offs.[7] However, the recent proliferation in state-sponsored cyberattacks has led cyber insurance companies to raise premiums and tighten contractual language in an effort to mitigate underwriting losses.[8] The reluctance to invest in cybersecurity is compounded by the fact that compensation due to management and corporate boards is frequently linked to stock performance. This incentivizes the C-Suite to aggressively pursue growth and chase earnings expectations instead of sustainably outperforming competitors on a risk-adjusted basis. Allocating precious capital towards security vulnerabilities directs the firm away from other projects and is unattractive in the eyes of shareholders. Companies neglect to invest in virtual protection because the paltry financial incentives do not outweigh the sunk cost.

[4] Vanessa Romo, "Panic Drives Gas Shortages after Colonial Pipeline Ransomware Attack," NPR (NPR, May 12, 2021), https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack.
[5] Steve Morgan, "Cybercrime to Cost the World $10.5 Trillion Annually by 2025," Cybercrime Magazine, April 27, 2021, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
[6] J.D. King, "Why Some Companies Don't Invest in Cybersecurity," Columbia Magazine, 2015, https://magazine.columbia.edu/article/why-some-companies-dont-invest-cybersecurity#:~:text=%E2%80%9CBuilding%20barriers%20and%20encrypting%20data,t%20seem%20like%20necessary%20investments.%E2%80%9D
[7] Ibid.
[8] Unknown, "Russian Cyberattacks May Test Insurer War Exclusion Policy Language," Fitch Ratings: Credit Ratings & Analysis for Financial Markets, accessed April 15, 2022, https://www.fitchratings.com/research/insurance/russian-cyberattacks-may-test-insurer-war-exclusion-policy-language-01-03-2022.

This makes them a favorite target of criminals and nefarious state-sponsored actors who wield cutting-edge software against their targets.[9] These issues affect the value of firms and introduce a relatively new aspect of Mergers & Acquisition due diligence. In this paper, I will examine cybersecurity and its role in corporate transactions, as well as governance and best practices for firms involved in the Merger & Acquisition deal cycle.

II. Cybersecurity is an Issue for the IT Team … or Is It?

As business leaders seek growth in a post-pandemic world, many look towards acquisitions to reduce costs and leverage economies of scale. Global Mergers and Acquisition (M&A) volume hit an all-time high in 2021, up 64% year-over-year.[10] Corporate finance departments and other buy-side entities are on a spending spree, eager to put excess cash to work in an acquisition. When a firm signals interest in acquiring a target, the target's management team paints their company in the best light possible, which can create dangerous situations as business executives attempt to conceal weaknesses within the firm. Acquisitions of targets with poor cybersecurity infrastructure or a history of data breaches opens the door to potential cyberattacks in the future and inspires mistrust among the customer base.[11] Integrating two companies is not like flicking on a light switch. The necessary decoupling and integration of databases, software, and personnel offers new opportunities to hackers who will capitalize on weakened cybersecurity hygiene.

[9] Taylre Janak, "Ransomware: The Cutting-Edge Cybercrime Taking over the Country and What You Can Do to Stop It," National Association of Attorneys General, November 9, 2020, https://www.naag.org/attorney-general-journal/ransomware-the-cutting-edge-cybercrime-taking-over-the-country-and-what-you-can-do-to-stop-it/.

[10] Niket Nishant, "Global M&A Volumes Hit Record High in 2021, Breach $5 Trillion for First Time," Reuters (Thomson Reuters, December 31, 2021), https://www.reuters.com/markets/us/global-ma-volumes-hit-record-high-2021-breach-5-trillion-first-time-2021-12-31/.

[11] Kazi Kabir, "Council Post: Cybersecurity Is the Future of Customer Acquisition," Forbes (Forbes Magazine, August 26, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/08/27/cybersecurity-is-the-future-of-customer-acquisition/?sh=6fabfea12a89%3B+https%3A%2F%2Fwww.forescout.com%2Fresources%2Fcybersecurity-in-merger-and-acquisition-report%2F.

Just like crime in the physical world, clever threat actors continue to innovate in the relatively new cyber-realm. Cybercrime takes countless forms but can be organized into a few broad categories that encompass most malicious activity. Malware is an umbrella term for programs that are designed to damage, disrupt, or hack a device.[12] These malicious programs come in several types including ransomware, spyware, and viruses. This type of cyberattack has become one of the most significant external threats. Once implemented, the malicious program follows instructions according to its code. It may reveal itself by crippling the operating system or choose to remain concealed, unbeknownst to the owners and users of the infected computer network.

These latent breaches are of particular concern for companies because undetected "bugs" that have already bypassed the defense mechanisms and infiltrated the network are notoriously difficult to unearth.[13] Spyware attempts to hide on a device and violate the privacy of the user, sometimes by illicitly recording video through accessing the webcam. This type of software can even steal sensitive personal data like bank login credentials and various passwords by tracking your keystrokes.[14] Ransomware locks users out of their files until a ransom payment is made, usually through an encrypted payment method such as cryptocurrency. It has been suggested that ransomware is the most common form of cybercrime worldwide.

[12] "What Is Malware? - Definition and Examples," Cisco (Cisco, April 1, 2022), https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html.
[13] "What Is Fileless Malware? - Crowdstrike," crowdstrike.com, March 29, 2022, https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/.
[14] "Spyware - What Is It & How to Remove It?," Malwarebytes, 2021, https://www.malwarebytes.com/spyware.

Figure 1: Spin Technology[15]

Ransomware made headlines in 2021 when blue-chip companies like the National Basketball Association (NBA) and JBS Foods were attacked.[16] This type of software has become so popular that some authors sell their packaged ransomware to cybercriminals as a weapon, which is known as Ransomware-as-a-service.[17] Since 2018, the majority of businesses worldwide are subject to ransomware attacks and the attack frequency rises with each passing year.

[15] Anastasia Unknown, "24 Recent Ransomware Attacks," SpinOne, December 15, 2020, https://spinbackup.com/blog/24-biggest-ransomware-attacks-in-2019/.
[16] Touro College, "The 10 Biggest Ransomware Attacks of 2021," Touro College Illinois (Touro College, November 12, 2021), https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php.
[17] "What Is Ransomware?: How to Protect against Ransomware," What is Ransomware? | How to Protect Against, 2021, https://www.malwarebytes.com/ransomware.

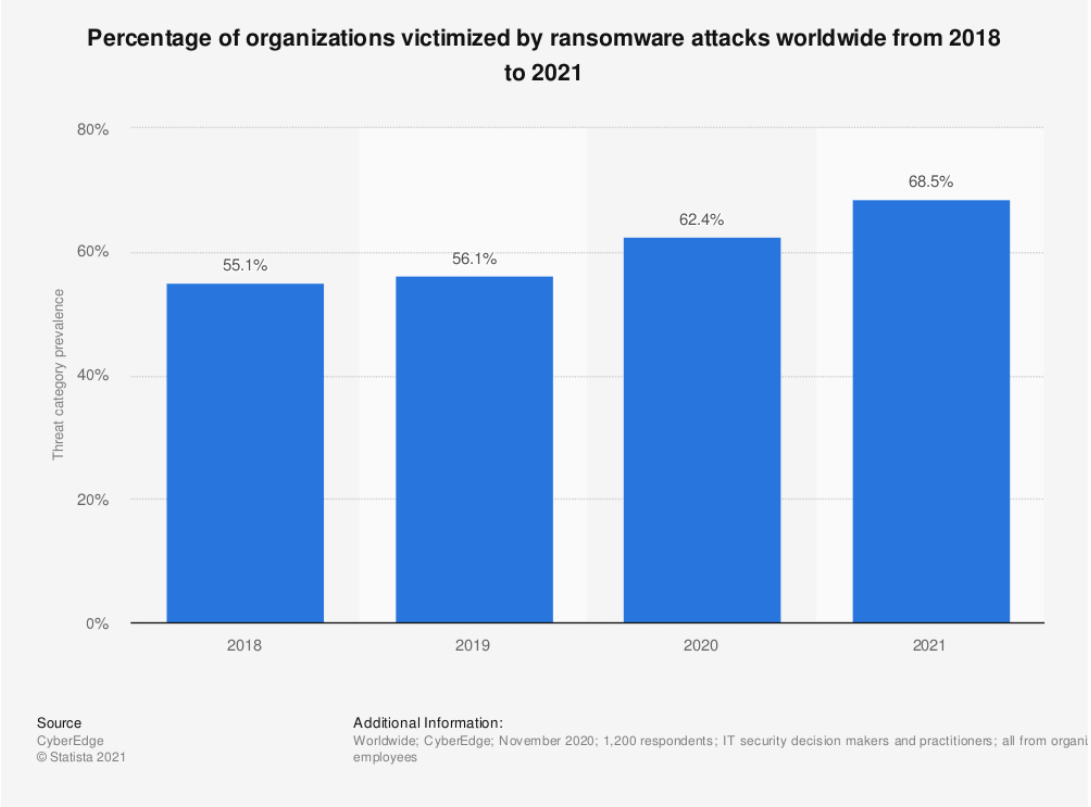

Figure 2: Statista, 2021[18]

Non-malware attacks (confusingly called "fileless malware") are different in that the virus does not need to install software to infect the machine. Fileless malware takes advantage of existing vulnerabilities, living in the computer's RAM or memory. Traditional antivirus tools cannot detect the threat due to the absence of identifiable code. The Ponemon Institute, a research organization focused on privacy and data, estimates that fileless attacks are about 10 times more likely to succeed than file-based attacks.[19] Fortunately, a system reboot will usually remove fileless malware because the computer's memory is wiped. Clearing cached browser information can also eliminate threats.

[18] Joseph Johnson, "Global Ransomware Victimization Rate 2021," Statista, May 10, 2021, https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/.
[19] "Fileless Malware Attacks Are Increasingly Common," Steadfast, August 3, 2020, https://www.steadfast.net/blog/fileless-malware-attacks-are-increasingly-common.

Threat actors can cause massive damage once inside a network, but the attacker needs an entry point to be able to bypass the network's security system. These entry points are called attack vectors. Clever programmers use analysis and online trends to create a process that exposes attack vectors, thus sourcing victims for cybercrime. Some of the most rudimentary methods have proven to be the most effective at scale. Phishing is a technique in which authors send a message (usually an email) designed to trick the recipients into divulging sensitive information or installing harmful software on their computer.[20] The sender email's address can be "spoofed" to look more legitimate, meaning the address attached with the message is not the actual email account of the phisher. For instance, an address may be spoofed so that it appears the email is from a trusted colleague or figure of authority.

Virtually all email users have been subject to phishing at one point, and it remains the most common way that malware is distributed.[21] Drive-by downloads are another attack vector that everyday internet users will encounter. This type of malware installs itself onto a computer without consent. They usually appear on websites, sometimes including legitimate ones.[22] As seen in the figure below, the most favored attack vectors are preventable, prototypical security issues like weak passwords and malware via spam emails.

[20] Rudra Srinivas, "Explainers: 4 Common Attack Vectors You Need to Know," CISO MAG | Cyber Security Magazine, February 1, 2022, https://cisomag.eccouncil.org/4-common-attack-vectors-you-need-to-know/.
[21] Ibid.
[22] Lucille Adams, "Common Malware Entry Points and How to Eliminate Them," Auslogics Blog, August 5, 2021, https://www.auslogics.com/en/articles/tag/malware/.

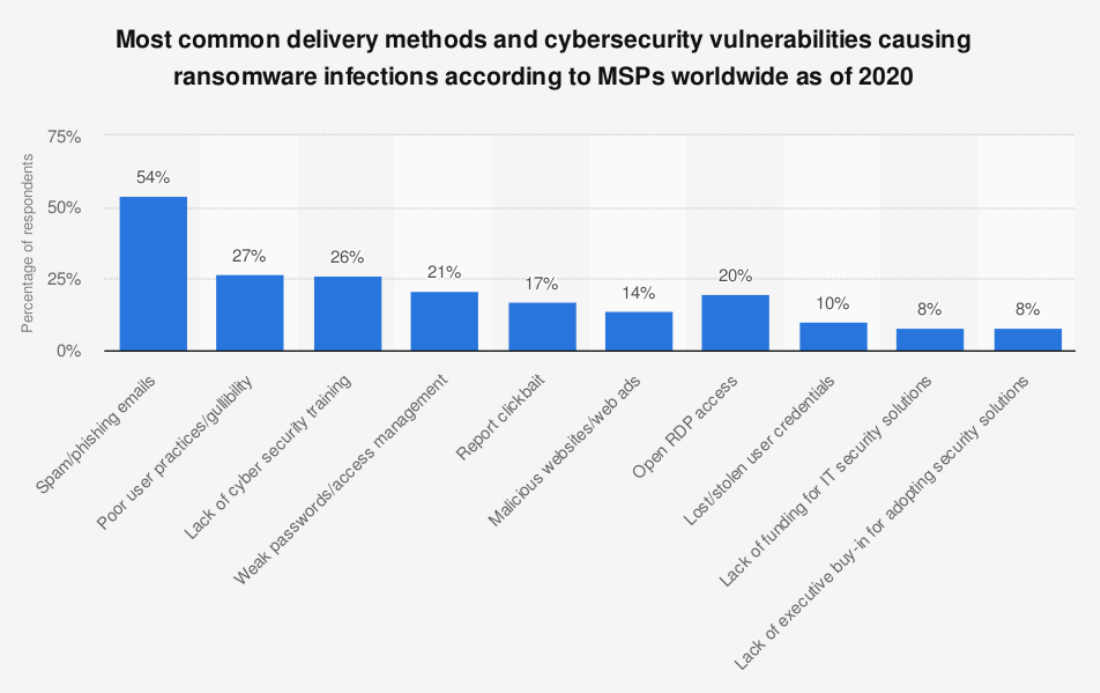

Figure 3: Statista, 202123

When cybercriminals are looking to target a corporation, they will deliberately collect information on employees and then use that data to launch tailored phishing attacks, set up a drive-by download, or find another way to weasel their malware onto the employee's desktop. Once the malware is resident, it can execute, spread, and start corrupting the data. Hackers also break into systems through compromised credentials, missing or poor encryption, and in some cases may be disgruntled or former employees themselves with intentional access to the system. The table below shows the most common action breaches.

[23] Joseph Johnson, "Leading Cause of Ransomware Infection 2020 | Statista," Leading cause of ransomware infection 2020, February 2021, https://lb-aps-frontend.statista.com/statistics/700965/leading-cause-of-ransomware-infection/.

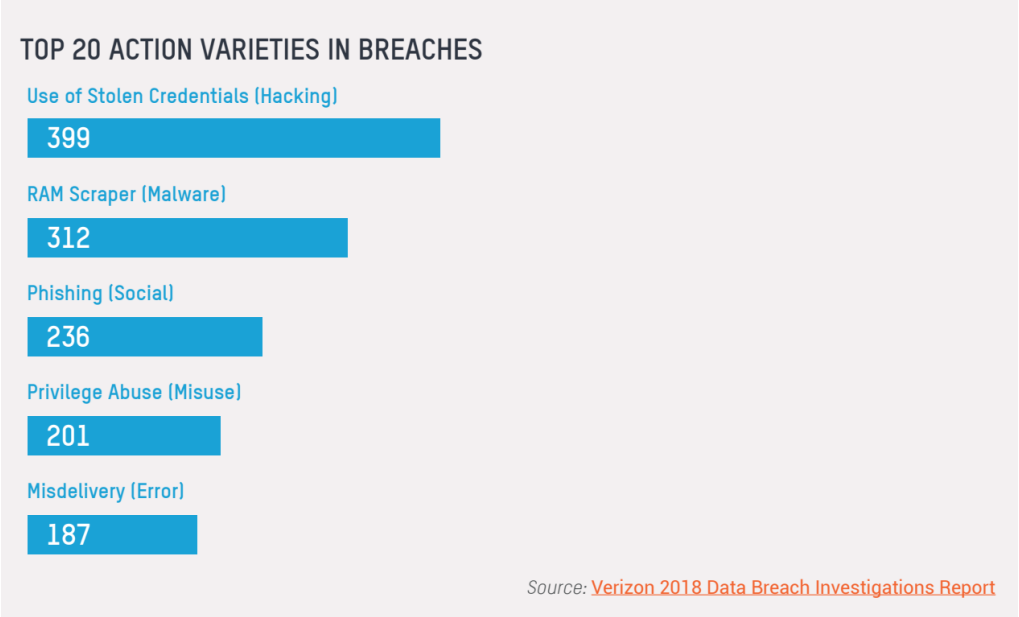

Figure 4: Verizon Data Breach Investigation Report[24]

Theft at the organizational level requires additional skill and more technical knowledge than stealing from individuals. The damage from an "ordinary" cyberattack that preys on a single person is usually limited in scope to monetary losses, access to social media accounts, and medical or personal information. These types of attacks are conducted at-scale on a large group of users and typically do not single out any one person. Top-notch cybercriminals tend to target organizations because of the higher potential payout. Once an organization's computer network is compromised, hackers seek valuable private data as well as money. This data may include client lists, program source code, trade secrets, unpublished patent applications, budgets, and a trove of other nonpublic information. Organizational losses from cyberattacks include money, data, amid other impairments and are therefore much harder to quantify. Indirect repercussions may arise in the form of a disparaged brand or reputation, increased regulation, lessened interest from would-be acquirers, and the opportunity cost of spending resources in an effort to return to the status quo. The pervasive and

[24] "Verizon Data Breach Investigations Report 2018 - PhishingBox," 2018, https://www.phishingbox.com/downloads/Verizon-Data-Breach-Investigations-Report-DBIR-2018.pdf.

insidious effects companies suffer from cyberattacks corroborate the critical role that cybersecurity plays in the corporate environment.

III. The M&A Process and Cybersecurity

Corporate dealmaking shattered records in 2021, fueled by low interest rates, abundant cash in the pockets of buy-side institutions, and companies' efforts to address shifts in strategy post-pandemic. Global mergers and acquisitions hit the mark of $5.7 trillion, up more than 60% year-over-year.[25]

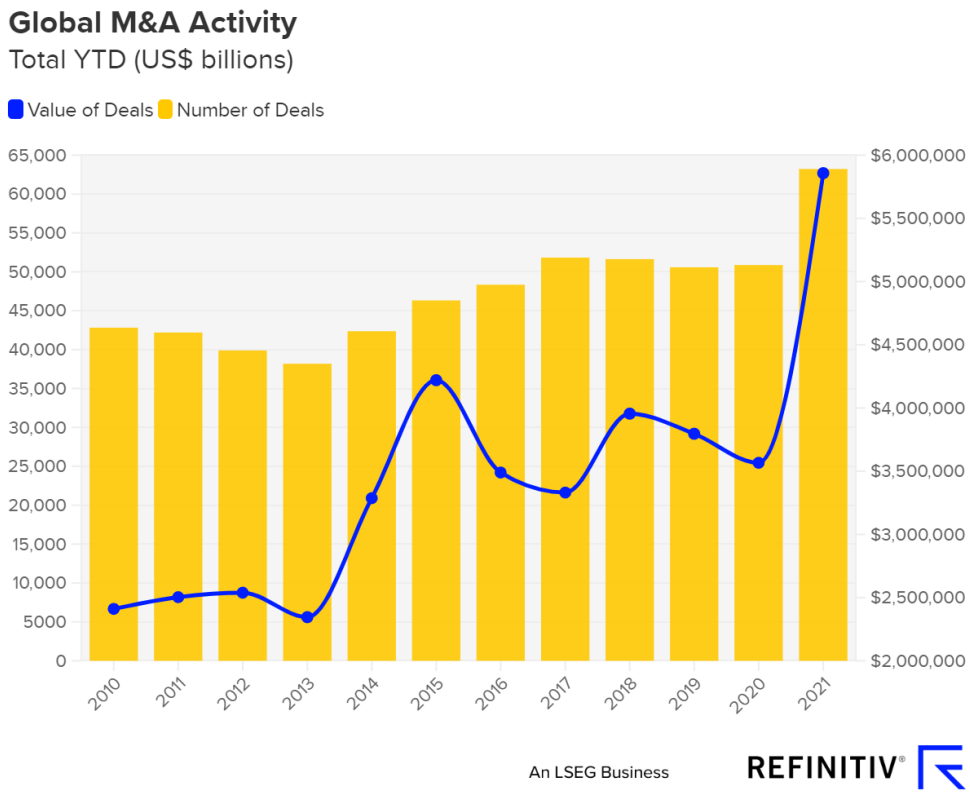

Figure 5: Refinitiv Deals Intelligence[26]

[25] Kristin Broughton, "M&A Likely to Remain Strong in 2022 as Covid-19 Looms over Business Plans," The Wall Street Journal (Dow Jones & Company, December 23, 2021), https://www.wsj.com/articles/m-a-likely-to-remain-strong-in-2022-as-covid-19-looms-over-business-plans-11640255406.

[26] Matthew Toole, "Dealmakers Ring out 2021 as the Year of M&A," Refinitiv Perspectives, January 12, 2022, https://www.refinitiv.com/perspectives/market-insights/dealmakers-ring-out-2021-as-the-year-of-

Corporate strategy teams complete mergers to expand market share, reduce competition, diversify the product line, or increase efficiency via recognizing synergies. Whether the deal is a merger, divestiture, or acquisition, there's an evaluation process that touches Financial, Legal, Business, Human Resources, and Information Technology.[27] This process is known as "due diligence" and allows for a complete investigation of the entity and the opportunity for a prolonged assessment of risk. Companies on either side of a transaction typically hire an investment bank to represent them and provide advisory regarding important decisions. On a buy-side engagement, an investment bank will set a preliminary valuation, quantify the strategic fit of the target through synergy opportunities, craft a bidding strategy, determine the appropriate way to finance the transaction, and negotiate the terms of the deal. On the sell-side, the bank will assemble marketing materials, structure the bid process, set valuation expectations, and act as the liaison between the management teams (and the buy-side bank) during due diligence.

"M&A can be a breeding ground for cyberattacks and data breaches", says Rohan Singla, a Risk Advisory employee at Grant Thornton.[28] Awareness of a target's cybersecurity history (both documented and undocumented incidents) is critical in order to make a well-informed bid. Additionally, that information is pertinent when contemplating upgrades or investments in cybersecurity post-merger. Today more than ever, the risk of data breaches includes not only the risk of a network breach but also the risk of the entire enterprise being undermined via business activities that rely on digital connectivity and accessibility.[29] Software company Forescout polled over

ma/#:~:text=Corporate%20dealmakers%20let%20rip%20in,private%20equity%20investors%20and%20SPACs.

[27] "Cybersecurity in Merger and Acquisition Report | Forescout," The Role of Cybersecurity in Mergers and Acquisitions Diligence, 2019, https://www.forescout.com/resources/cybersecurity-in-merger-and-acquisition-report/.

[28] "Cybersecurity in M&A Strategy," Cybersecurity in mergers and acquisitions | Grant Thornton, July 13, 2021, https://www.grantthornton.com/library/articles/advisory/2021/cybersecurity-in-ma-strategy.aspx.

[29] James Kaplan, Ray A. Rothrock, and Friso Van Der Oord, "The Board's Role in Managing Cybersecurity Risks - Proquest," accessed April 15, 2022, https://www.proquest.com/docview/1986317468.

2,700 American business executives and IT decision makers. The study found that 73% of respondents considered an undisclosed data breach to be an immediate deal breaker in their company's M&A strategy.[30]

Network breaches have become so routine for dealmakers that for most transactions it's not a question of if, but when. In the same aforementioned poll, 53% of respondents reported that their organization faced a critical cybersecurity issue or incident during an M&A deal that put the transaction in jeopardy. [31] High-profile companies especially elevate their risk when the merger announcement is published in the press release. The accompanying media coverage can alert hacking collectives that want to exploit a window of opportunity that exists during the amalgamation process. The Cyber Division of the Federal Bureau of Investigation published a notification to private industry in November 2021. In the statement, the Bureau wrote "Between March and July 2020, at least three publicly traded US companies actively involved in mergers and acquisitions were victims of ransomware during their respective negotiations."[32] Firms must shore up their defenses and develop response tactics prior to screening companies during the initial stages of M&A.

The expansive consequences of an attack mean that cybersecurity management can no longer be delegated to the IT department. The issue needs to be addressed holistically, requiring the teamwork of both directors and management. Even as companies increase their investments in security, directors and C-suite executives are often not sufficiently prepared to deal with cybersecurity issues. In some cases, insufficient spadework and complacency may bring about legal repercussions against the directors, who owe fiduciary duties of care and loyalty to the corporation and its shareholders. Case law is developing and testing the courts' interpretation of directors' duty of oversight, which delineates that they must continually monitor many things,

[30] "Cybersecurity in Merger and Acquisition Report | Forescout," The Role of Cybersecurity in Mergers and Acquisitions Diligence, 2019, https://www.forescout.com/resources/cybersecurity-in-merger-and-acquisition-report/.
[31] Ibid.
[32] Federal Bureau of Investigation, "Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims," November 2021, https://www.ic3.gov/Media/News/2021/211101.pdf.

among them cybersecurity risk. Following Target Corp.'s data breach in 2013, shareholders filed a class-action lawsuit against directors and company officers alleging negligence of fiduciary duties for failing to adequately oversee the security of data.[33] Target appointed a special litigation committee to investigate the breach. The committee found no "actionable claims" against Target in its report. Target is incorporated in Minnesota and because of this, the judge ruled according to Minnesota law which heavily weighs a board's litigation committee's findings.[34] The case was ultimately dismissed, but the precedent cases show that the legal framework is evolving to include cybersecurity in the duty of care. Based on the shifting judicial rulings, directors should be very conscious that their legal duties may require an understanding of what the basic cybersecurity posture constitutes for their respective corporation.

IV. Conclusion and Best Practices

As organizational cybersecurity needs adapt to increasing threats, members of the corporate and M&A world must educate themselves on the specific risks cyberattacks pose to their line of work. A robust cybersecurity framework does not provide the same feelings of achievement and success for most people that accompany other business activities like beating projections, making the sale, finishing a project, or completing an acquisition. This absence of positive feedback creates the perilous problem that many breached firms realize in retrospect; an underestimation and ignorance of risk from the top-down. To avoid this situation, corporations should undertake preventative measures before considering any M&A transaction. This encompasses awareness from firm leaders, adequate defense systems, and an exhaustive framework for how to deal with cyber incidents when they happen.

[33] "Settlement of Target Data Breach Consumer Class Action Is Derailed on Appeal," Data Protection Report (Norton Rose Fulbright, April 27, 2018), https://www.dataprotectionreport.com/2017/02/settlement-of-target-data-breach-consumer-class-action-is-derailed-on-appeal/.

[34] Sam Gross, "Caremark Liability in the Digital Age: Corporate Directors' Oversight Duties in the Data Privacy Domain," Legaltechcenter.net, accessed April 15, 2022, https://legaltechcenter.net/files/sites/159/2020/05/Caremark-Liability-in-the-Digital-Age.pdf.

As the Russia-Ukraine War escalates in Eastern Europe, U.S. President Joe Biden has asked American companies to strengthen their online defenses as a matter of national security in a March advisory.[35] The plea comes as Russian hackers scan the networks of US companies looking to wage a second war in the cyber realm.[36] This threat will continue long after the Russia-Ukraine War is resolved. Awareness of cybersecurity's ever-expanding role cannot be overlooked, both on the world stage and in the boardroom.

[35] Joseph Biden, "Statement by President Biden on Our Nation's Cybersecurity," The White House (The United States Government, March 21, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/.
[36] Rishi Iyengar, "US Warns Businesses to Prepare for Russian Cyberattacks. Here's How They Can Do That," CNN (Cable News Network, March 23, 2022), https://www.cnn.com/2022/03/23/tech/cyberattack-businesses-russia/index.html.