RESEARCH MEMO

The Economic Costs of Cyber Risk

By Chris Nolan and Annie Fixler

June 28, 2021

Executive Summary

The SolarWinds cyber breach was likely the largest in U.S. history, though its full breadth and impact remain unknown. As early as October 2019, Russian hackers penetrated the Texas firm's software development environment so that when the company pushed patches to its customers, it inadvertently delivered Moscow's malware as well.[1] The hackers exfiltrated data from U.S. government agencies for more than a year before FireEye exposed the operation last December.[2]

While it could take months or even years to remove the compromised software and implement other remediation measures, and although the costs to the U.S. government alone could be in the hundreds of millions of dollars,[3] the breach was not as damaging as feared from an economic perspective, because its primary purpose appears to have been espionage. The breach did not cause large-scale business disruptions like those caused by Russia's NotPetya attack on Ukraine in 2017. That malware spread around the world, affecting tens of thousands of companies, costing some as much as hundreds of millions of dollars.[4]

The digital age has increased productivity and efficiency, but many firms are struggling to manage the downside risks that accompany it. Too many companies are prioritizing short-term growth and cost-cutting at the expense of cybersecurity. As the SolarWinds breach demonstrated, one company's cyber risk can have cascading economic and national security implications.

1. The United States and United Kingdom have attributed the SolarWinds operation to Russia's civilian foreign intelligence service, the SVR. Russia denies this. "'Flattered' Russian spy chief denies SolarWinds attack – BBC," *Reuters*, May 18, 2021. (https://www.reuters.com/technology/russian-spy-chief-denies-svr-was-behind-solarwinds-cyber-attack-bbc-2021-05-18); UK National Cyber Security Centre, Advisory, "Further TTPs associated with SVR cyber actors," May 7, 2021. (https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf)

2. A report from Palo Alto Networks notes that domain registration and command-and-control setup occurred as early as September 2019. However, that does not necessarily indicate that the hackers had established a foothold in SolarWinds' network. In October, the hackers were identified manipulating SolarWinds' code. "SolarStorm Supply Chain Attack Timeline," *Palo Alto Networks*, December 23, 2020. (https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline)

3. Dave Nyczepir, "SolarWinds' federal footprint is large, and compromise is a 'nightmare scenario' for affected agencies," *FedScoop*, December 14, 2020. (https://www.fedscoop.com/solarwinds-federal-footprint-nightmare)

4. Andy Greenberg, "The Untold Story of Notpetya, The Most Devastating Cyber Attack in History," *WIRED*, August 22, 2018. (https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world)

Chris Nolan is the qualitative research lead at Intangic, an insurtech firm that provides corporations with innovative solutions for rising intangible and digital asset risks. **Annie Fixler** is the deputy director of FDD's Center on Cyber and Technology Innovation. She works on issues related to the national security implications of cyberattacks on economic targets; adversarial strategies and capabilities; and U.S. cyber resilience.

Twenty years ago, after a wave of corporate scandals undermined public confidence in the securities market, Congress passed the Sarbanes-Oxley Act, requiring greater corporate financial disclosures.[5] The law strengthened investor protections and confidence through better accounting standards, improved internal controls and disclosure by companies and stronger external oversight. Poor cybersecurity is today's systemic risk, and the potential impact is even greater. Unlike the accounting malpractice and financial scandals of the 1990s and early 2000s that prompted congressional intervention, a single company with deficient cybersecurity could inflict substantial harm on the U.S. government, company shareholders (including retirees dependent on pensions), the public, and critical national infrastructure.

The insurtech firm Intangic developed a digital-risk rating system that uses a combination of financial data and externally observable malicious network activity to price actuarial risk across over 6,000 public corporations, including projected economic and shareholder value losses stemming from breach events. This memo employs the Intangic model to analyze two hypothetical breach scenarios: one targeting a large managed service provider, and a second one targeting a regional utility. The results demonstrate how the deficiencies of a single company can yield economic losses that exceed those caused by major natural disasters.

Confronting and correcting the issue of poor cybersecurity practices will require legislative and policy remedies. This memo prescribes enhanced corporate disclosures related to risk controls, cyber breaches, and vulnerabilities to improve the quality of information available to regulators and investors. Market forces can then incentivize corporate stakeholders to improve their company's resilience and security. The goal is to minimize the likelihood of cyber breaches on the scale of SolarWinds – or worse – in the future.

Underinvestment in Security Is Creating Systemic Risk

Digital technology is now the most valuable asset in the world. It plays a critical role in the function and growth of companies across every industry sector. Technology giants are the most valuable companies in the world today, replacing the energy and manufacturing firms that topped the rankings 25 years ago.

1995 Most Valuable Companies	2005 Most Valuable Companies	2021 Most Valuable Companies
1 GM	**1** Exxon	**1** Apple
2 Ford Motor	**2** GE	**2** Saudi Aramco
3 Exxon	**3** Gazprom	**3** Microsoft
4 Walmart	**4** Microsoft	**4** Amazon
5 AT&T	**5** Citigroup	**5** Google

Data source: Bloomberg

5. Sarbanes-Oxley was enacted in 2002 after high-profile corporate accounting scandals. The collapse of companies such as Enron, Tyco, and WorldComm resulted in massive losses and shook investor confidence. This prompted a major overhaul of accounting and disclosure standards. Sarbanes-Oxley improved the information available to investors about risks, thereby increasing investor protections and confidence. Josh Fruhlinger, "The Sarbanes-Oxley Act explained: Definition, purpose, and provisions," *CSO Online*, November 30, 2020. (https://www.csoonline.com/article/3598292/the-sarbanes-oxley-act-explained-definition-purpose-and-provisions.html)

The rate of change is not slowing down. As Microsoft CEO Satya Nadella explained in January, "What we have witnessed over the past year is the dawn of a second wave of digital transformation sweeping every company and every industry."[6] For example, car manufacturing is now so dependent on advanced technology that a global shortage of computer chips at the beginning of 2021 upended production schedules and temporarily shut down some auto plants. Ford, for example, saw a 17 percent drop in production in the first quarter of 2021 due to chip shortages.[7]

Every company now uses advance technology to generate more value. The combinations of hardware, software, data management tools, and other programs – collectively known as the technology "stack" – of companies today are increasingly complex. There are myriad, overlapping tools with redundant capabilities, and patches and updates are pushed out daily.

Procuring technology is the easy part. Managing it well is what separates more secure companies from their weaker peers. A misconfiguration in any one tool can create serious security vulnerabilities. Technology management and cybersecurity impact financial performance just like return on equity, return on investment, free cash flow, or any other traditional metric.

Ransomware breaches are economically and financially damaging because they impact things that directly impact the balance sheet, such as productivity and cost efficiencies. The cost of the ransomware payment – the issue that receives most of the attention – is minor compared to the cost of repairing the breach, the loss of revenue, the erosion of profit margins, and the shareholder (and reputational) losses that typically linger for several quarters or even years.[8]

Gaps in Cyber Risk Disclosures

In 2018, the Securities and Exchange Commission (SEC) issued guidance stating that cybersecurity risk is material to a company's financial health and business operations, but did not require publicly traded companies to disclose cyber risks or cyber incidents.[9] The guidance acknowledges that companies may require time to discern the implications of an incident, and recommended that companies that suffer a cyber breach amend prior disclosures during their investigation into the breach. In practice, however, most companies do not provide additional

6. Todd Bishop, "Microsoft profits jump 33% as CEO Satya Nadella cites a 'second wave of digital transformation,'" *Geek Wire*, January 26, 2021. (https://www.geekwire.com/2021/microsoft-profits-jump-33-ceo-satya-nadella-cites-second-wave-digital-transformation)

7. Claudia Assis, "Ford's 'massive' first-quarter beat overshadowed by chip-shortage headwinds," *MarketWatch*, April 29, 2021. (https://www.marketwatch.com/story/fords-massive-first-quarter-beat-overshadowed-by-chip-shortage-headwinds-11619712630).
In early May, Kia and Hyundai announced temporary shutdowns of plants in South Korea because of the chip shortage. Kia had previously announced and then reversed a temporary shutdown of a plant in Georgia in April. Michael E. Kanell, "Kia's Georgia plant stays open despite global semiconductor shortage," *The Atlanta Journal-Constitution*, April 9, 2021. (https://www.ajc.com/ajcjobs/kias-georgia-plant-stays-open-despite-global-semiconductor-shortage/3MCYYMTJ4BDZ5IBCOAVPOHHJHA); "Hyundai, Kia to suspend plants next week on chip shortages," *Yonhap News Agency* (South Korea), May 14, 2021. (https://en.yna.co.kr/view/AEN20210514005600320?section=market/economy)

8. The FBI's annual report, for example, notes that cost estimates of ransomware exclude "estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim." U.S. Federal Bureau of Investigation, Internet Crime Complaint Center, "Internet Crime Report 2020," 2020, page 20. (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)

9. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Securities and Exchange Commission, 83 Federal Register 8166, February 26, 2018. (https://www.federalregister.gov/documents/2018/02/26/2018-03858/commission-statement-and-guidance-on-public-company-cybersecurity-disclosures)

information in subsequent reports. As a result, it can appear to investors that a breach never happened or had a negligible impact.

The SEC guidance also recognizes that cyber policies and procedures are important elements of overall risk management. As such, the guidance encourages companies to adopt comprehensive policies, to conduct self-assessments of their compliance with their own policies, and to self-assess their controls and procedures to ensure information is provided to senior leadership for the purpose of disclosures and certifications. Yet there has never been a disclosure of this kind, which suggests that companies are not actually conducting rigorous self-assessments – or they are not reporting. On the whole, companies are not following the SEC guidance.[10]

Even when companies disclose breaches, they often are not fully transparent about the financial impact. Companies use terms such as "ongoing expenses" and "materially adverse impact on financial performance" in the wake of significant breach events.[11] This lack of transparency limits investors' understanding of the extent of the damage from the incident.

Insurance-Related Disclosures

While cyber insurance coverage can be an important risk management tool for enterprises, many organizations have nonexistent or insufficient coverage, and underwriters struggle to price policies properly due in part to the challenge of accurately modeling the likely frequency and severity of breaches. Thus, cyber insurance cannot effectively compensate for deficient cybersecurity practices.

The Foundation for Defense of Democracies (FDD) has explored the value of cyber insurance in improving resilience and aiding recovery from cyberattacks.[12] To date, however, companies affected by malicious cyber incidents have found limited success filing claims. The insurance has either been insufficient, as in the case of Norsk Hydro,[13] or providers have denied claims, as in the case of Target's $138 million claim following a 2013 breach.[14] Litigation between insurers and claimants (such as Maersk, Merck, and Mondelez) over the NotPetya malware attack of 2017 also reveals the limitations of insurance in the case of attacks by nation-state actors. In general, even when insurance provides relief from a cyberattack, the payment rarely covers the damage inflicted, especially the indirect costs such as operational shutdowns and loss of potential revenue.[15] In short, cyber insurance is not yet providing companies with the essential

10. This conclusion is based on Intangic's observation of the market and is confirmed by a report from a coalition consisting of SecurityScorecard, the Cyber Threat Alliance, the National Association of Corporate Directors, Diligent, and IHS Markit. "The State of Cyber-Risk Disclosures of Public Companies," *SecurityScorecard, National Association of Corporate Directors (NACD), Cyber Threat Alliance, IHS Markit, and Diligent*, March 2021. (https://s3.amazonaws.com/ssc-corporate-website-production/documents/resources/the-state-of-cyber-risk-disclosures-of-public-companies.pdf)

11. Intangic's data indicate that on the whole, companies that provide a dollar-based disclosure of the effects of a cyber breach are likely to suffer smaller financial and economic losses as a result of the breach than companies that do not.

12. Nour Aburish, Annie Fixler, and Michael Hsieh, "The Role of Cyber Insurance in Securing the Private Sector," *Foundation for Defense of Democracies*, September 13, 2019. (https://www.fdd.org/analysis/2019/09/11/cyber-insurance); Trevor Logan, "The Time for Cyber Insurance," *Foundation for Defense of Democracies*, September 2, 2020. (https://www.fdd.org/analysis/2020/09/02/the-time-for-cyber-insurance)

13. Jeff Stone, "Norsk Hydro's cyber insurance has paid just a fraction of its breach-related losses so far," *CyberScoop*, October 28, 2019. (https://www.cyberscoop.com/cyber-insurance-norsk-hydro-lockergoga-attack)

14. Andrew Simpson, "Federal Judge Sides with Chubb in Denial of Target's Data Breach Bank Claims," *Insurance Journal*, February 10, 2021. (https://www.insurancejournal.com/news/national/2021/02/10/600678.htm)

15. For more information about the challenges in the cyber insurance industry, see: U.S. Government Accountability Office, "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market," May 20, 2021. (https://www.gao.gov/products/gao-21-477)

risk-transfer function that other forms of corporate insurance (such as property and casualty insurance) typically provide. This will likely change as the insurance industry's approach to digital risk improves, including through the use of better actuarial models and more sophisticated underwriting solutions, such as parametric insurance.

Modeling Cyber Risk

Despite the rising frequency and increased costs of business-interruption events such as ransomware, technology risk remains largely unregulated. Markets and regulators need to identify objectively and transparently whether companies are properly managing digital technology and related risks.

Until now, a paucity of data on breaches has hampered cyber risk modeling. Most risk assessments are based only on disclosed cyber breaches, which account for only a fraction of total incidents. According to Mandiant's Security Effectiveness Report, 53 percent of attacks infiltrate corporate networks without detection.[16] Of the remaining 47 percent, companies disclose only those breaches in which customers' personally identifiable information (PII) is stolen or ransomware causes an obvious disruption in service, as those are the situations requiring action pursuant to current data-breach notification laws. Companies are otherwise unlikely to volunteer information, thus preventing investors, insurers, the government, and U.S. taxpayers from getting an accurate picture of the impact.

Instead of relying on an incomplete dataset, it is possible to model digital risk based on financial disclosures and externally observable malicious network traffic. Using only publicly available information, Intangic has built a digital-risk rating system and actuarial model to estimate the economic and financial costs of cyber risks. A licensed third-party index provider audits these company risk ratings. Published results demonstrate that across every industry sector, companies with one- or two-star ratings suffer breaches more frequently than firms with four- or five-star ratings.[17] This is the rating system Intangic uses in its actuarial model for insurance purposes. The individual company ratings are not public, though corporate customers have access to their own ratings. The results of the ratings have also been measured against the stock market for over four years and are published monthly in the form of a publicly available index covering the U.S., UK, and EU markets.

Intangic updates the results of these assessments every month and validates them against externally verifiable information. The company's data science lab then runs over a million tests per month to validate the risk ranking for companies. These predictive results are measured against the following factors to demonstrate accuracy:

- Negative changes in enterprise value on an overall and sector-specific basis
- Negative changes in income statement, cash flow statement, or balance sheet
- Probability of debt default (credit ratings)
- Probability of negative earnings surprise due to poor cyber hygiene
- Predictive value of the economic-loss model post-breach

16. "Deep Dive Into Cyber Reality: Mandiant Security Effectiveness Report 2020," *FireEye*, 2020. (https://www.fireeye.com/current-threats/annual-threat-report/security-effectiveness-report.html)

17. Intangic also indexes cyber performance on a geographic and sector-specific basis to ensure fair comparisons and to account for macroeconomic and cyclical impacts on operations. Similar to how credit ratings, investment bank research, sovereign risk, and ESG (environmental, social, and governance) ratings are validated, Intangic's assessments are time-stamped and validated by an independent auditor.

Because operational performance impacts stock prices over the long run, Intangic's cyber ratings are measured against the stock market. As of November 2020, over the past three years, companies with "good" scores on Intangic's digital-risk rating system outperformed "bad" ones by 46 percent in the United States and by 60 percent in the European Union. The model thus enables investors to make informed financial decisions, allows insurers to price premiums based on risk, and helps companies make better decisions about their own digital transformations, including risk transfer and security expenditures.

Intangic's ratings also serve as an early-warning system for significant cyber incidents. Companies with poor cyber risk ratings are more likely to suffer a cyberattack and are less prepared to recover from one. By detecting the highest-risk companies (those with one- or two-star ratings), the model can anticipate where remediation of vulnerabilities may be necessary to avoid a breach and how company resources can be best allocated to mitigate vulnerabilities and lower the probability of an event.

For example, for one year leading up to the SolarWinds breach announcement, Intangic's ratings model ranked SolarWinds as a high-risk company because, relative to its peers, the company had:

- high expenses related to mergers and acquisitions but low annual research-and-development spending, suggesting the company prioritized short-term growth over continued technological development, including security;
- high network and technological complexity[18] and weak liquidity, indicating that if the company suffered a cyber incident, it would lack the financial capacity to remediate the issue effectively; and
- more externally observable malicious network activity.

For SolarWinds, in particular, the fact that thousands of companies and numerous U.S. government agencies bought, deployed, and relied upon SolarWinds software made the company an increasingly attractive target for hackers.

Operational disruption and downtime are the costliest effects of cyberattacks. When a company's disruption causes cascading effects on its customers, Intangic's model estimates an economic impact on par with that of recent catastrophic weather events. Such events provide an approximation of what to expect in terms of operational downtime from losses of electricity and other utilities as well as transportation and logistics services.

Studies of the impact of Hurricane Sandy in 2012 on small- and medium-sized businesses (SMBs) in New York, New Jersey, and Connecticut, and of the impact of 2017's Hurricane Harvey on SMBs in the Houston area, show not only widespread operational disruption but also long-term costs. For example, Sandy impacted one-third of all firms in the greater New York metro area.[19] Firms reporting losses due to utility disruption on average lost $5,000

18. A company's network complexity can be assessed externally by examining the number of nodes and alternative paths within its computer network. Factors that can adversely impact network complexity include acquisition of new companies (including complex systems integration) and the addition of digital tools such as customer-facing apps within a network. Such tools may improve convenience for customers, but they can also render a network more difficult to defend.

19. Benjamin L. Collier, Andrew F. Haughwout, Howard C. Kunreuther, and Erwann O. Michel-Kerjan, "Firms' Management of Infrequent Shocks," *Journal of Money, Credit and Banking*, December 3, 2019. (https://onlinelibrary.wiley.com/doi/epdf/10.1111/jmcb.12674); Benjamin Collier, Lawrence Powell, Marc A. Ragin, and Xuesong You, "Financing Severe Climate Risk: Evidence from Businesses During Hurricane Harvey," Unpublished Paper, January 7, 2021. (Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3741812)

per employee. Meanwhile, Hurricane Harvey cost an estimated 55,000 to 75,000 jobs over the short term,[20] and half of the surveyed firms had not fully recovered one year later. Eight percent reported that their businesses would never recover, and 9 percent closed permanently.[21]

Like cyberattacks, extreme weather events also impact firms' future risk management plans.[22] Forty percent of firms impacted by Harvey reported increasing their savings and/or credit, a process of de-risking that negatively impacts overall GDP growth. Twenty-five percent of firms impacted by those two hurricanes increased their insurance coverage even though insurance was of little help to companies impacted by the hurricanes.[23]

Disruptive cyber incidents can cause similar short- and long-term damage. In fact, cyber incidents can exact an even greater economic cost than extreme weather events, because the bulk of the economic losses from weather events are from property damage.[24] Intangic's model focuses on digital assets such as software, which are much more valuable for most companies in terms of revenue generation, cost efficiency, and profit growth. The indirect effects of a cyberattack often include increased strain on the financing and credit worthiness of affected companies and increased debt. These impacts linger for at least several months and, in some cases, years following the event, whereas property damage can often be more easily remedied.

Scenario Analysis: Cascading Effects of Cyber Incidents

The following scenarios depicting hypothetical cyberattacks illustrate how a single company's deficiencies can create systemic risks and losses. These scenarios are not improbable. Similar attacks have already occurred.

Scenario #1 – Managed Service Providers: SMBs are the source of nearly half of all private-sector jobs in the United States.[25] Unlike Fortune 500 companies, which often have advanced, in-house cyber defense capabilities, SMBs usually have limited defenses.

As companies have accelerated digitization efforts in recent years, they have often outsourced information technology (IT) functions to managed service providers (MSPs), increasing their operational reliance on these

20. Keith Phillips and Christopher Slijk, Federal Reserve Bank of Dallas, San Antonio Branch, "Short-Term Job Growth Impacts of Hurricane Harvey on the Gulf Coast and Texas," accessed June 7, 2021. (https://www.dallasfed.org/research/forecast/~/media/documents/research/forecast/harvey.pdf)

21. Benjamin L. Collier, Andrew F. Haughwout, Howard C. Kunreuther, and Erwann O. Michel-Kerjan, "Firms' Management of Infrequent Shocks," *Journal of Money, Credit and Banking*, December 3, 2019. (https://onlinelibrary.wiley.com/doi/epdf/10.1111/jmcb.12674); Benjamin Collier, Lawrence Powell, Marc A. Ragin, and Xuesong You, "Financing Severe Climate Risk: Evidence from Businesses During Hurricane Harvey," Unpublished Paper, January 7, 2021. (Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3741812)

22. Ibid.

23. Seventy-four percent of businesses with property insurance, 72 percent with business interruption insurance, and 52 percent with flood insurance said their policies did not cover any of their losses from Sandy. Of firms impacted by Sandy, 39 percent took on debt to finance their recovery, while 15 percent received insurance payments. The results from the Hurricane Harvey recovery were similar, with only 15 percent of firms using insurance payouts to cover their losses, with the rest having to tap savings, increase debt, or take on new equity financing. As 74 percent of firms reported that Harvey increased their financing needs to address damage and business-interruption losses, insurance played a small role in the overall recovery.

24. U.S. Department of Commerce, National Oceanic and Atmospheric Administration, National Hurricane Center, "Costliest U.S tropical cyclones tables updated, January 26, 2018. (https://www.nhc.noaa.gov/news/UpdatedCostliest.pdf)

25. U.S. Small Business Administration, Press Release, "Advocacy Releases 2020 Small Business Profiles For The States And Territories," June 5, 2020. (https://advocacy.sba.gov/2020/06/05/advocacy-releases-2020-small-business-profiles-for-the-states-and-territories)

third parties. Growing digital interconnectedness makes it increasingly difficult to distinguish a corporate network from that of a supplier, partner, or customer. The expansion of telework during the COVID-19 pandemic has only increased the attack surface by expanding remote access into enterprise IT networks.[26]

Vendors are a known risk, according to specialty insurer Beazley.[27] In addition to the SolarWinds breach, several large MSPs suffered breaches within the past two years.[28] In the decade-long "Operation Cloud Hopper," hackers infiltrated MSPs to bypass the cyber defenses of dozens of companies to steal intellectual property and confidential business data.[29] By compromising one MSP in New York, for example, hackers gained access to clients across the financial, telecommunications, manufacturing, automotive, energy, and other sectors.[30]

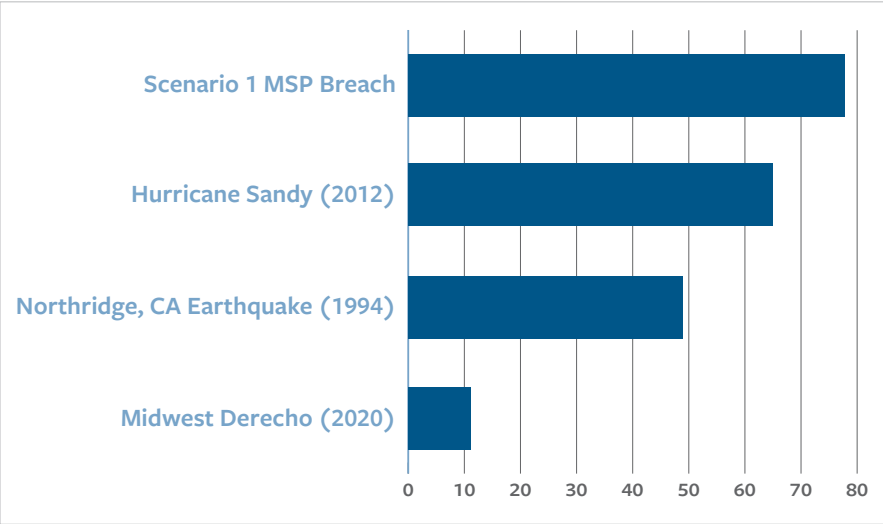
Unfortunately, MSPs do not always adequately protect their own technology and that of their customers. There are critical IT service providers with below-average security ratings whose vulnerabilities heighten the probability of a successful malware attack.[31] This is the "third-party paradox": The corporate drive for greater efficiency and cost savings has created additional cyber-related vulnerabilities that most companies had not considered when they elected to outsource.[32]

Because MSPs have privileged access to the backend IT infrastructure of the customers they serve, SMBs with strong cybersecurity can still be affected by a breach targeting their vendors. According to Intangic data, if a customer is operationally dependent upon a service provider, a disruption affecting that provider may also compromise the customer, regardless of its cyber rating.

Imagine the following:[33] An MSP succumbs to phishing attacks. Once the hackers gain access to the MSP's internal systems, the hackers inject malware into the backend systems of the MSP's customers. This breach lasts for several months without detection, as none of the MSP's systems detect malicious activity.

26. "Beazley: Ransomware Attacks Increasingly Paired With Data Breach," *Claims Journal*, March 24, 2020. (https://www.claimsjournal.com/news/national/2020/03/24/296164.htm)
27. Ibid.
28. Dan Swinhoe, "Wipro breach highlights third-party risk from large IT services providers," *CSO Online*, April 17, 2019. (https://www.csoonline.com/article/3389685/wipro-breach-highlights-third-party-risk-from-large-it-services-providers.html); Lawrence Abrams, "IT giant Cognizant confirms data breach after ransomware attack," *Bleeping Computer*, June 17, 2020. (https://www.bleepingcomputer.com/news/security/it-giant-cognizant-confirms-data-breach-after-ransomware-attack)
29. U.S. Department of Justice¸ Press Release, "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," December 20, 2018. (https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion)
30. John Carlin, David Newman, and Amy Josselyn, "DOJ Indictment Alleges Theft of Hundreds of Gigabytes of Corporate and Government Data in Attacks Targeting Managed Service Providers," *Morrison & Foerester LLP*, January 10, 2019. (https://www.lexology.com/library/detail.aspx?g=1068fd0a-8388-4453-aa7b-6872a5c96536)
31. "The Cyberhedge Cyber Governance Indices are market-based proof that cyber governance impacts shareholder value," *Intangic*, March 25, 2021. (https://cyberhedge.com/indices). Companies with one or two stars in the Intangic Cyber Governance Index have a greater probability of experiencing a ransomware attack, considered "high-risk." Multiple large MSPs currently have a one- or two-star rating.
32. Intangic first referred to the third-party paradox in an analysis of the 2019 WiPro breach. "Organizations," *CYBERHEDGE Research*, Volume 2, September 2019. (https://Intangic.com/insights/research/volume-2-september-2019)
33. The plausibility of this scenario and the other in this paper is based on Intangic's ratings and data. The scenarios are based on similar events that occurred previously, albeit on a smaller scale. For more, see the appendix.

Figure 1: Economic Losses from Disasters ($ in billions)



The hacking group then launches a coordinated ransomware attack on the MSP and many of its customers, resulting in significant business disruption for more than three days.[34] This impacts 600 SMBs[35] across the industrial, chemical, energy, IT, and communications sectors. Impacted companies span every region of the United States and every major industry sector.

In such a scenario, Intangic forecasts that the economic losses would approach $80 billion, costing tens of thousands of jobs.[36] The exact figure ($77.8 billion) is equal to 31 percent of the Dow Jones Industrial companies' annual net income.[37] This estimate exceeds the economic damage inflicted by Hurricane Sandy (approximately $65 billion).[38] See Figure 1.

Scenario #2 – Critical Infrastructure: The risk of a disruptive cyberattack on critical infrastructure is rising. Hackers have successfully breached electric utilities.[39] Within the electricity sector, hackers are particularly focused on companies that manage generation, transmission, or distribution of energy across the country, according to industrial cybersecurity firm Dragos as well as the Government Accountability Office.[40] Hackers have already developed ransomware specifically designed for industrial control systems upon which critical infrastructure often depends.[41]

34. A business disruption for more than three days is considered a long business interruption.

35. This is a realistic number given the size of a large MSP's customer base. Consider just the publicly known number of companies impacted by the SolarWinds breach.

36. The dollar value of an economic loss is calculated based on a percentage of a company's annual operating income. Job-loss figures for each scenario are estimated based in part on the job-loss figures attributed to larger-scale business disruptions caused by recent severe hurricanes, such as Harvey.

37. The market-value loss experienced by these companies would be even greater, with an aggregate hit to equity value of $285 billion, according to the Intangic model. The dollar figures in this and the other hypothetical scenario are based on independently validated data on the financial and economic impact of cyber breaches on individual companies to date. These are not hypothetical estimates.

38. Doyle Rice and Alia E. Dastagir, "One year after Sandy, 9 devastating facts," *USA Today*, October 29, 2013. (https://www.usatoday.com/story/news/nation/2013/10/29/sandy-anniversary-facts-devastation/3305985)

39. Morgan Chalfant, "Hackers breached US electric utilities: analysts," *The Hill*, August 2, 2018. (https://thehill.com/policy/cybersecurity/399999-analysts-say-hackers-breached-us-electric-utilities); Rebecca Smith, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It," *The Wall Street Journal*, January 10, 2019. (https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112)

40. Morgan Chalfant, "Hackers breached US electric utilities: analysts," *The Hill*, August 2, 2018. (https://thehill.com/policy/cybersecurity/399999-analysts-say-hackers-breached-us-electric-utilities); U.S. Government Accountability Office, "Electricity Grid Cybresecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution System," March 2021. (https://www.gao.gov/assets/gao-21-81.pdf)

41. "New ransomware targets critical infrastructure," *Intangic*, February 10, 2020. (https://Intangic.com/insights/daily/2020/02/10/new-ransomware-targets-critical-infrastructure)

The merging of operational technology (OT) and IT has also drastically increased the cyber threat surface for companies. OT systems are increasingly controlled by IT systems for remote maintenance of large, physical devices,[42] leaving them vulnerable to insider threats and external hackers breaching the IT environment. For example, while the FBI and Department of Homeland Security confirmed that the May 2021 DarkSide ransomware attack did not breach Colonial Pipeline's OT networks, the company "proactively disconnected certain OT systems to ensure the systems' safety."[43] As Dragos notes, sometimes "halting operations becomes the safest choice" because of the dependency of OT systems on IT networks.[44]

OT systems have no built-in cybersecurity mechanisms. They often have a lifespan measured in decades rather than the months or years of IT systems. This matters because older OT systems were not designed to include cybersecurity. Indeed, no one anticipated their connection to IT systems and the wider internet. For example, 70 percent of large power transformers in the United States are at least 25 years old and were not designed for the digital age.[45]

With the increased adoption of Internet of Things devices by utility companies, industrial control systems have become more connected and thus more vulnerable to attack. The rollout of new digital tools for managing both the grid and downstream digital services for customers have introduced greater complexity and vulnerability to IT networks. The greater the number of direct customer-interface points, the more potential entry points for threat actors.

Electric utilities generally have stronger cybersecurity than other sectors,[46] particularly municipally owned water utilities, which are notoriously vulnerable.[47] Electric utilities, however, feel the same business pressures to expand profit margins and to grow through acquisition. Acquisition increases the probability of attack, because the process of merging the companies' networks tends to have an adverse impact on cybersecurity in the short term.[48]

Security teams across the utility sector are often stretched thin as they cope with the expanded threat environment that comes with not only the merging of OT and IT, but also the risks that come with a remote workforce. In short, while the cyber defense capabilities of companies in the electricity sector are often more sophisticated than those of their peers in other sectors, there is still a range of capabilities, and some companies are less secure than others.[49]

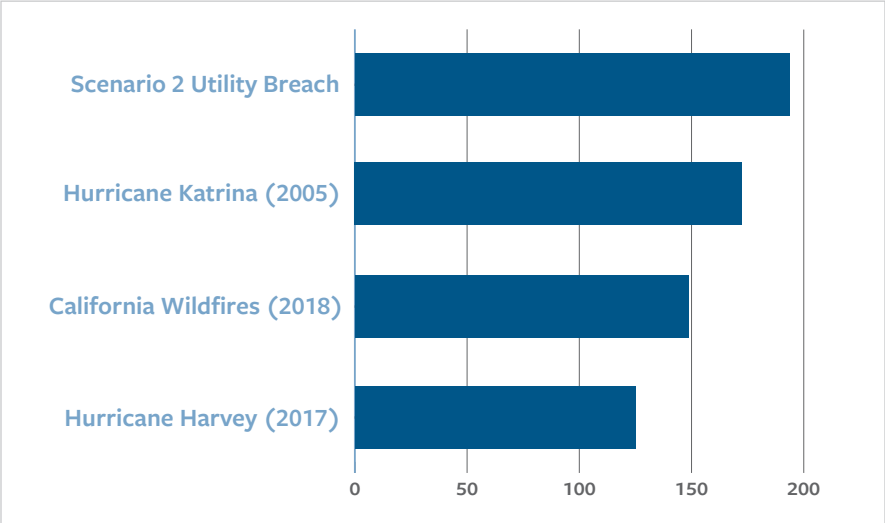
42. Richelle Elberg, "Affordable connectivity driving smart water and gas," *Smart Energy*, October 29, 2019. (https://www.smart-energy.com/magazine-article/affordable-connectivity-driving-smart-water-and-gas); Samantha F. Ravich, "Hackers Threaten Our Water Supply," *RealClearPolicy*, June 17, 2020. (https://www.realclearpolicy.com/articles/2020/06/17/hackers_threaten_our_water_supply_496397.html)
43. U.S. Cybersecurity and Infrastructure Security Agency, "Alert (AA21-131A): DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks," May 11, 2021. (https://us-cert.cisa.gov/ncas/alerts/aa21-131a)
44. Mike Hoffman and Tom Winston, "Recommendations Following the Colonial Pipeline Cyber Attack," *Dragos*, May 19, 2021. (https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack)
45. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, "Large Power Transformers and the U.S. Electric Grid," June 2012, page v. (https://www.energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf)
46. Cyberhedge (Intangic's predecessor) found that the utilities and financial sectors ranked highest on cyber governance metrics. Utilities include electric, gas, and privately owned water companies. Cyberhedge, Press Release, "Cyberhedge Releases New Cyber Governance Rankings by Sector," September 10, 2019. (https://www.prnewswire.com/news-releases/cyberhedge-releases-new-cyber-governance-rankings-by-sector-300915198.html)
47. Mark Montgomery and Annie Fixler, "Cybersecurity and your water: Hacker attempted to poison Florida city's water supply," *The Hill*, February 23, 2021. (https://thehill.com/opinion/cybersecurity/540009-cybersecurity-and-your-water-hacker-attempted-to-poison-florida-citys)
48. Lindsey O'Donnell, "CISA Warns of Security Flaws in GE Power Management Devices," *Threatpost*, March 22, 2021. (https://threatpost.com/cisa-security-flaws-ge-power-management/164961)
49. Chris Nolan and Ryan Dodd, "Cyber Governance Alert: GE," *Cyberhedge*, June 26, 2020. (https://cyberhedge.com/insights/alert/ge)

It is not difficult to imagine a major regional electric utility in the United States making a series of choices that puts it at increased risk of an attack with economically devastating consequences. Such a company might have long struggled with its digital transformation process and the merging of OT and IT. With a short-term-oriented business strategy, its CEO and board might pursue growth through acquisition to pad the balance sheet, acquiring a smaller regional competitor. While integrating the complex IT and OT systems of the acquired company's network and getting a handle on new digital tools, an overwhelmed security team might fail to implement security patches.

During this period, a sophisticated hacker group might detect vulnerabilities in the company's cyber defenses and launch a campaign. If the hackers obtain the login credentials of a key employee, they would gain administrator-level access to all internal network functions, including OT. The hackers could then launch a business-disruption attack on the regional utility, paralyzing its internal systems, including the command-and-control function for the grid itself. Even if the company were able to regain control of the network, repel the hackers, and restore operations relatively quickly, Intangic projects that a breach that disrupts power generation across the grid for five days would cause an economic loss of $193.5 billion.[50] This is equivalent to approximately 30 percent of the Department of Defense's 2021 budget.[51]

Disruption of a major regional electric utility would likely affect 1,500 SMBs across sectors ranging from healthcare and energy to industrials. The impacted area would depend on the location of the utility but could cross multiple state lines. More than 100,000 jobs might be lost as a result.[52]

Figure 2: Economic Losses from Disasters ($ in billions)



Recommendations

Improving poor cybersecurity practices will require comprehensive legislative and policy remedies. Greater disclosure of cyber breaches and vulnerabilities would improve the quality of information available to regulators and investors about market risks. This transparency would increase investor confidence in the ability of public companies to protect their most valuable assets – technology and intellectual property. Greater transparency would also help address systemic risk and strengthen security controls, enhancing national resilience against a range of cyber threats. As with all regulation of industries, the government will need to determine the right combination of requirements and incentives to achieve greater transparency regarding the economic costs of cyber incidents. The following recommendations focus on requirements, acknowledging that tax or other incentives may be necessary

50. This number is the value of the economic loss. The market loss alone would be $683,102,827,638.
51. U.S. Government Accountability Office, "Defense Budget: Opportunities Exist to Improve DOD's Management of Defense Spending," February 24, 2021. (https://www.gao.gov/products/gao-21-415t)
52. This estimate is based on the number of jobs lost from recent large-scale weather events, such as Hurricane Harvey.

to encourage the adoption of best practices. Transparency alone will not eliminate cyber breaches, but better disclosure will reduce their frequency and can lessen the severity of breaches when they occur.

1. **Pass a National Breach-Notification Law:** One year ago, the congressionally mandated Cyberspace Solarium Commission (CSC) concluded that, inter alia, Congress ought to pass a national data-breach notification law. The commission observed that the current "patchwork" of state laws is not serving the American people, and that a federal law (which supercedes state laws) would "standardize consumers' expectations and provide regulatory certainty" to businesses.[53] Currently, breach-notification laws focus on notification of customers when PII is compromised. Breaches of this nature, however, represent a fraction of total breaches. As noted, ransomware attacks rarely result in the compromise of PII, so under current law, many companies need not disclose being the victim of a highly disruptive attack. For example, few of the 100 companies affected by the SolarWinds breach need to answer to either regulators or customers. Without a federal breach-notification law that includes disruption as a criterion for disclosure, American citizens may never understand the full economic effects and market impact of the breach.

2. **Amend Sarbanes-Oxley to Include Cybersecurity Reporting Requirements:** Congress should amend Sarbanes-Oxley to codify the SEC's 2018 guidance, specify corporate responsibility requirements for cybersecurity, and require management assessments of cyber risk.[54] The CSC also recommended codifying this SEC cybersecurity language. Using Sarbanes-Oxley as a guide, mandating self-disclosure of vulnerabilities can incentivize companies to re-examine their own security controls just as Sarbanes-Oxley forced companies to re-evaluate financial controls.[55] The new language should require disclosure of the financial and operational impact (in dollar terms) of breaches when they occur.

3. **Require Dollar-Based Risk and Breach Disclosures:** Dollar-based breach disclosures should be required as part of any mandatory breach notification. Financial and economic loss estimates should be provided in the reporting periods immediately following breaches.

   Dollar-based risk disclosure should also be part of a company's proactive disclosure of risk factors. Risk assessments alone are not sufficient to protect investors or provide market-based incentives for companies to achieve consistently higher levels of security. Rather, when companies disclose financial estimates associated with risks – as is consistent with the practice for any significant financial risk – investors better understand how well companies are managing risk. This transparency will help create market incentives for companies to invest in security. Such disclosures would also help investors understand which losses may be covered by cyber insurance, analogous to how a company would disclose dollar-based costs stemming from damage from other unforeseen events.

53. U.S. Cyberspace Solarium Commission, "Final Report," March 11, 2020, page 94. (https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view)
54. Ibid., page 83.
55. Mandatory disclosures alone may not change cyber risk. One study found that a year after disclosing an internal-controls weakness under Sarbanes-Oxley requirements, 59 percent remedied it, likely as a result of a concern about market reaction and litigation risk. However, after three years, 30 percent continued to disclose the same weakness. John Coates and Suraj Srinivasan, "SOX Ten Years After: A Multidisciplinary Review," *Harvard Business School*, January 12, 2014. (https://dash.harvard.edu/bitstream/handle/1/12175242/Srinivasan_Suraj_J2_SOX%20After%20Ten%20Years%20-%20A%20Multidisciplinary%20Review.pdf?sequence=1)

4. **Require Third-Party Cyber Assessments:** By using available technologies such as security validation, it is possible to assess the general cyber health of any company in real time. Such an assessment can identify not only what security controls exist but also how effective the controls are at protecting a company's digital assets. The disclosure of security controls and their effectiveness and related weaknesses is already recommended in the 2018 SEC guidance and should be mandated. These disclosures should occur quarterly to reflect the rapidly changing nature of corporate IT networks. The combination of mandatory disclosures and third-party assessments would parallel quarterly financial reporting coupled with external credit ratings that help investors make informed decisions.

5. **Provide Cyber Hygiene Guidance for SMBs:** Poor technology management leads to underperformance in the market. This is costly for investors and businesses alike. SMBs, however, may not have in-house cybersecurity expertise. The U.S. government, private cybersecurity firms, risk management firms, and cyber insurers should offer clear cyber hygiene guidance to SMBs that explains things such as National Institute of Standards and Technology (NIST) security controls[56] in terms these businesses can easily understand. Evaluating SMBs' implementation of this guidance should become part of third-party cyber assessments.

Conclusion

Cyber vulnerabilities pose a systemic risk to the U.S. economy. Through the right mix of policy and standard-setting, the U.S. government can help create a market with more informed risk-taking and more resilient companies. With better information, market forces can incentivize investments in security and better technology management to reduce risk. It is possible to improve the functioning of the insurance market and equip investors with the information to reward good, and punish poor, cyber risk management. To do so, the market needs dollar-based estimates of digital risk. Collectively, information from independent external assessments, disclosures from companies of cyber breaches and risk controls, and more transparency paint an accurate picture of this risk. The ultimate goal is to incentivize enterprise cyber resilience and, by extension, create greater national resilience against all forms of cyber threats.

56. U.S. Department of Commerce, National Institute of Standards and Technology, "Cybersecurity Framework," accessed June 7, 2021. (https://www.nist.gov/cyberframework)

Appendix: Objective Metrics With Dollar Value

For the scenarios included here, Intangic used its actuarial model to calculate the economic impact of hypothetical incidents. Previously, Intangic's model accurately predicted the financial and economic impact of operational disruption. The model wields externally verifiable data, including market and financial results. It has proven accurate in distinguishing between high- and low-risk companies in all industries in the United States, United Kingdom, and European Union.

For example, before Pitney Bowes suffered a significant (over three-day-long) ransomware attack in October 2019, Intangic (then Cyberhedge) rated the company as a two-star. Immediately following the breach in October, the Intangic model estimated the attack would result in a $25 million to $35 million operational and financial impact on the company. Pitney Bowes then disclosed a $29 million hit to free cashflow and a $19 million reduction in earnings before interest, taxes, debt, and amortization (EBITDA) in February 2020.[57]

Travelex is another example of the Intangic model's accuracy in predicting financial and economic losses. A cyberattack stopped Travelex's operations in late 2019. Due to loss of cash, the company never fully recovered and filed for bankruptcy. On January 10, 2020, Intangic projected $450 million in market losses. One month after the breach, Travelex announced that it had lost $443.8 million.[58]

In February 2020, after ISS World suffered a ransomware incident, the company's management sought to reassure investors of the event's limited impact, noting there was "no indication that any customer data or systems have been breached." Operational disruptions such as ransomware, however, are more financially costly and take longer to recover from than customer-data breaches. At the time, Intangic (then Cyberhedge) warned its clients that the impact of the incident would have "little to do with customer data loss and everything to do with business disruption."[59]

Six months later, the reported damage exceeded one-third of the company's annual operating income. After six months, the company announced that it had regained a "vast majority" of its operations and disclosed the financial cost of the attack.

In February 2020, Intangic projected $356 million in economic losses resulting from the breach. In June 2020, ISS World disclosed $255 million in losses, with additional costs likely in 2021 as IT assets are rebuilt.[60]

These ransomware events share two key similarities:

1. The cost of repairing systems after a breach is always much higher than initially estimated.

2. The damage suffered by companies and their shareholders is much greater than the direct costs such as software repair and replacement, which companies normally highlight. These costs are a fraction of the true economic and financial losses caused by operational disruption.

57. For more information on this case, see: "Pitney Bowes latest ransomware breach further evidence of persistently poor cyber governance," *Cyberhedge*, May 12, 2020. (https://cyberhedge.com/insights/daily/2020/05/12/pitney-bowes-latest-ransomware-breach-further-evidence-of-persistently-poor-cyber-governance)
58. For more information on this case, see: "Update to Rapid Response: Travelex/Finablr," *Cyberhedge*, March 24, 2020. (https://cyberhedge.com/insights/rapid-response/travelex-finablr-upd)
59. "ISS reports ransomware attack, incurs losses from business disruption," *Cyberhedge*, February 26, 2020. (https://www.cyberhedge.com/insights/daily/2020/02/26/iss-reports-ransomware-attack-incurs-losses-from-business-disruption)
60. "Rapid Response: ISS World," *Cyberhedge*, September 1, 2020. (https://cyberhedge.com/insights/rapid-response/iss-world)

About Intangic

Intangic (formerly Cyberhedge) is an insurtech company that provides corporations with innovative solutions for rising intangible and digital asset risks. With offices in Washington, DC, Barcelona, Berlin, and Luxembourg, Intangic is backed by a leading global investor in cybersecurity, Paladin Capital Group, and the Luxembourg Future Fund, backed by the Société Nationale de Crédit et d'Investissement and the European Investment Fund. For more information, visit www.intangic.com.

About FDD's Center on Cyber and Technology Innovation

The Foundation for Defense of Democracies (FDD) is a Washington, DC-based, nonpartisan policy institute focusing on foreign policy and national security. CCTI seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats and opportunities to national security posed by the rapidly expanding technological environment. For more information, please visit www.fdd.org/ccti.