Data as a Liability: Cybersecurity Insurance and its Transatlantic Implications

Varoon Bashyakarla

2019 McCloy Fellowship on Global Trends
The American Council on Germany

Spring 2020

Table of Contents

Abstract

Cybersecurity is an unavoidable challenge of the twenty-first century, and cyber incidents are on the rise in both the United States and Germany. A growing number of firms in both countries have started offering cyberinsurance policies to protect against the costs associated with leaks, breaches, and hacks. The evolution of cyber risk, the market response of cyber insurance, and the possibility of a cyber catastrophe bear structural resemblance to the evolution of financial risk, the development of the mortgage industry, and the 2008 financial crisis. As observed in the aftermath of the ensuing economic meltdown, a large-scale cyber disaster is likely to induce isolationist tendencies in the United States and Germany. However, given the shared set of cybersecurity challenges besetting both countries, Berlin and Washington have a unique opportunity to preserve their respective national security, diplomatic, and economic interests while strengthening the transatlantic bond in the process.

> Cyber is the one thing that scares me to death. I cannot believe the amount of silent coverage that the industry affords. It's an accident waiting to happen...If you think about cyber as a potential loss scenario, there's no other loss that's anywhere near as

> potentially catastrophic. If you think about wind, or a quake, or a man-made disaster, or even a political uprising, you're never talking about more than about 10 per cent of the world. With cyber, it's the whole world in a nanosecond. The aggregation of exposure is mind-boggling.
>
> – Stephen Catlin, 45-year insurance industry veteran[1]

Introduction

The global migration to the cloud and the 'datafication' of communication has engendered an economic transformation across virtually every industry and facet of life: banking, trade, housing, labor, transportation, agriculture, education, law enforcement, finance, manufacturing, healthcare, travel, media, politics, retail, travel, grassroots organizing, dating, media, research, entertainment, art, and more. The benefits of these technological advancements – saved time and money, among others – are well-documented and widely understood. The internet and the opportunities it has created are lauded for these achievements, but at what cost have these benefits been realized?

The logic of mass data collection, the tendency towards quantification, and the normalization of surveillance established in the process have manifested themselves in a variety of forms that call the simplistic narrative of the internet as a panacean, democratizing force into question: disinformation propagated online via the ad-based business model of the internet,[2] elections swayed by micro-targeting of voters via illicitly harvested data,[3] and inequitable algorithmic decisions informed by data from the real world that mirrors and perpetuates underlying social, economic, and political inequalities rather than subverting them, among others.[4] A related phenomenon, which is growing increasingly difficult to ignore, is the lack of basic safeguards in mass-consumed tech products and services engineered and designed for markets that preference efficiency and convenience over privacy and security. As individuals, businesses, and governments continue sharing sensitive, often personal data with services connected to the internet, they expose both their digital and non-digital lives alike to a growing set of risks.

The associated damages are non-trivial. By the end of 2020, the number of internet-connected devices is projected to reach 30 billion,[5] and by 2021, cybercrime costs are expected to exceed $6 trillion annually as the number of internet users around the world reaches 6 billion by 2022.[6] The trade publication *Cybersecurity Ventures* notes, "This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined."[7] Data is an asset, but it is also a liability. If data is the new oil, as the platitude suggests, what is the digital equivalent of climate change?

Recognizing the considerable value of internet-based communications, and thus the potential harm that could result from cybersecurity incidents, some insurance companies have created cybersecurity insurance policies to preserve the benefits of the internet's technological leaps

1 Kent, "Catlin."
2 DiResta et al., "The Tactics and Tropes of the Internet Research Agency."
3 Kang and Frenkel, "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users."
4 "Machine Bias — ProPublica."
5 "Spotlight."
6 "Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion."
7 "Cybercrime Damages $6 Trillion by 2021."

while insulating against potential losses. The creation and adoption of cyberinsurance implicitly affirms the notion that technological development has, in short, made the world riskier as a result of novel cybersecurity vulnerabilities it has introduced. These escalating and destabilizing forces inevitably impact individual states and their relations with one another. Understanding both the threats to and the cybersecurity strategies of the United States and Germany may provide insights as to what implications cyber risk has for the transatlantic bond.

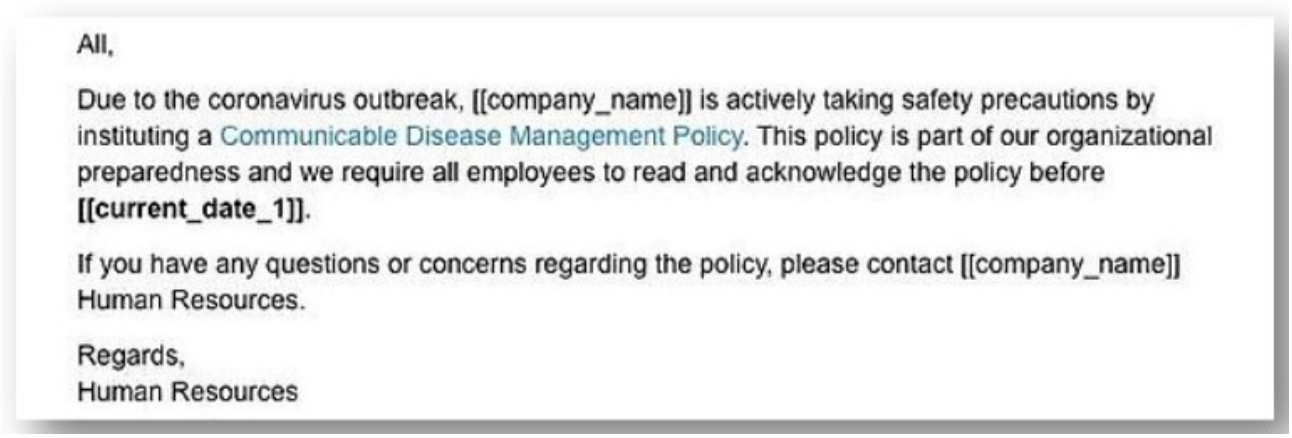
The Politicization of American and German Cyberspace: A Contemporary Snapshot

The first cybersecurity incident to attract mainstream media attention occurred in the United States in 1988, in which a researcher created a 99-line program that rendered computers unusable by slowing them down. The author of the Morris worm was the first person convicted under the Computer Fraud and Abuse Act in the USA, which prohibits unauthorized computer access.[8] Thirty-two years later, cyber incidents have grown more sophisticated than their experimental antecedents. In practice, culprits often go unpunished because attribution is exceptionally difficult and because the playing field is now global.

Shared Challenges

Today, both the United States and Germany regularly experience a number of cyber incidents of political consequence. The SARS-CoV-2 crisis has spurred what might be the largest wave of cyberattacks that cohere around a common theme ever observed at a time when people are turning to the internet for answers amidst uncertainty, when employees are working remotely in record numbers, and when IT teams are scrambling to meet a new host of demands.[9] The German Federal Office of Information Security released a statement warning of a surge in malware (purportedly claiming to provide coronavirus-related information on websites with COVID-19-related keywords), phishing emails, and doctored websites supposedly from state aid and healthcare institutions designed to intercept login credentials, and of fraudulent online shops ostensibly selling protective gear. As a result, cybercriminals, the statement warns,[10] may gain access to online banking accounts, collect sensitive information belonging to companies, and encrypt valuable data – rendering it inaccessible – before blackmailing the victims and decrypting the data.[11] In the southwest state Baden-Würtemberg, state criminal police have issued warnings of fraudsters contacting firms by phone and instructing them to seek emergency aid on falsified websites.[12] Similar cyberthreats have been noted in the US.[13]

8 “The History of Cyber Attacks - a Timeline.”
9 “Coronavirus Now Possibly Largest-Ever Cyber Security Threat.”
10 “BSI - Presseinformationen Des BSI - Cyber-Kriminelle Nutzen Corona-Krise Vermehrt Aus.”
11 “Covid-19 Coronavirus-Cybersecurity and Information Security Developments Summary 15 May.Pdf.”
12 “LKA-BW.”
13 Choudhury, “Cybercriminals Are Exploiting Fears of the Pandemic to Steal Personal Information.”


All,

Due to the coronavirus outbreak, [[company_name]] is actively taking safety precautions by instituting a Communicable Disease Management Policy. This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before **[[current_date_1]]**.

If you have any questions or concerns regarding the policy, please contact [[company_name]] Human Resources.

Regards,
Human Resources

An example phishing email seemingly sent from a company to its employees. Clicking on the link in the email prompts the download of malicious software. Social engineering of this kind has skyrocketed around the world during the coronavirus pandemic.[14]

Russia is a common adversary of both US and German cybersecurity. In April 2015, members of the Bundestag received an email from the "@un.org" domain, suggesting it was from the United Nations. The email, ostensibly about Ukraine's economy based on its subject line, contained malware that quietly collected credentials and spread across the Bundestag's network. Over the course of weeks, the Bundestag's website, online services, and IT infrastructure all became inaccessible. An analysis later found that 16 GB in total, including entire inboxes of Bundestag members, had been sent to a foreign server. Germany's Federal Prosecutor recently issued an arrest warrant for Dmitry Badin, a Russian national believed to be part of the GRU's elite hacking division. The FBI already had Badin on its 'Wanted' list for his role hacking the World Anti-Doping Administration while investigating a doping scheme and for his role in the DNC hacks shortly before the 2016 presidential election in the US, where Russia is known to have interfered with American political affairs.[15] Based on the findings of seventeen intelligence agencies, the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security stated that "The U.S. Intelligence Community is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations."[16]

Starting in 2017, both the US and Germany were involved in the infamous NotPetya ransomware campaign targeting Microsoft systems and demanding payment in Bitcoin. The White House called NotPetya "the most destructive and costly cyber-attack in history."[17] Beiersdorf, a German skin company lost about $43 million due to disruptions caused by the ransomware.[18] Meanwhile, the German pharmaceutical company Merck was forced to pause production of some drugs and observed losses totaling $870 million. FedEx, via a European subsidiary, sustained $400 million in damages, and NotPetya cost Mondelēz – the parent company of Oreo – about $188 million.[19] Experts maintain that NotPetya is the brainchild of the Kremlin, which the White House estimates to have caused $10 billion in losses around the world.[20]

14 "Coronavirus Phishing Emails: How to Protect against COVID-19 Scams | NortonLifeLock."
15 "Who Is Dmitry Badin, The GRU Hacker Indicted By Germany Over The Bundestag Hacks?"
16 "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security."
17 "Statement from the Press Secretary."
18 "State Secrets: Germany Is Just Fine with the NotPetya Cyberattack but Its Allies Aren't."
19 "The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED."
20 "Statement from the Press Secretary."

The image above shows what victims of the original version of the 2017 Petya ransomware saw. NotPetya is believed to have been orchestrated by the Kremlin, a shared adversary of American and German cybersecurity. German companies (including DHL and Beiersdorf), American organizations (including Mondelēz and a number of hospitals), and other entities around the world sustained major losses. NotPetya caused systems responsible for radiation monitoring at Chernobyl to go offline and brought drug production at Merck to a standstill. In total, the ransomware cost an estimated $10 billion in losses globally.[21]

State-specific Cybersecurity Incidents

Despite responding to the same global events and sharing cybersecurity adversaries, the United States and Germany have unique histories of cybersecurity incidents that reflect their specific vulnerabilities, risk profiles, and strategic positioning. The following examples are a mere smattering of recent cyber events intended to illustrate the variety, breadth, and depth of the cyber issues confronting each state.

One of the most widely publicized cyber incidents in recent US history was the attack on the Office of Personnel Management. As Josephine Wolff, Assistant Professor of Cybersecurity Policy at The Fletcher School at Tufts University and author of *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches,* wrote in her book, "In the 2015 breach, fingerprint data for 5.2 million people and background investigation information for 21.5 million current and former government employees were stolen, including responses to questions on the lengthy Standard Form 86 (SF-86) used for security clearances." The attack was waged by the People's Liberation Army – the Chinese armed forces – and likely conferred a variety of benefits to the Chinese government: identifying undercover American agents stationed in China, blackmailing government employees, guessing their passwords, and impersonating individuals to conduct further attacks. Cyberespionage of this sort has been a particular challenge of American businesses as foreign adversaries attempt to "gain insight into their competitors' commercial strategies, international trade negotiations, and proprietary intellectual property belonging to foreign companies." In 2014, Sony sustained a massive data breach in which all the data on over half of its servers was wiped, including "employee salary information, Social Security numbers, and performance reviews," shaming high-profile executives and Hollywood producers in the process.[22] In 2017 alone, the United States observed 477 breaches of health data affecting over 5.5 million patient records,[23] and data from American hospitals has been held hostage for ransom by hackers.[24] Cybersecurity incidents are not always the result of malicious foreign actors with nefarious aims,

21 "Petya (Malware)."
22 Wolff, Josephine, *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*.
23 "2017 Breach Report."
24 "Ransomware Attack Prompts Hancock Health to Pay $50,000 to Hackers."

however; they can result from domestic actors,[25] even when operating with good intentions, as well. One source for this report who runs a highly politicized non-profit and who requested anonymity disclosed a dramatic increase in the number of security incidents resulting from domestic actors after the inauguration of Donald Trump. Furthermore, a number of consumer apps that collect sensitive data, for instance, were largely ignored security-wise until they were understood to constitute national security risks. Grindr, a gay dating app that connects users based on geographic proximity, is owned by a Chinese company. The use of the app by American military personnel may be revealing the location of American troops to Beijing and is currently under the scrutiny of the Committee on Foreign Investment in the United States.[26] Similarly, the smartphone app Strava – which enables users to record, track, and share workouts – released a global map of users' workout locations in November 2017. The map displayed every workout ever uploaded to the platform, inadvertently disclosing the location of secret army bases.[27] Earlier that year, Equifax, one of three major credit reporting agencies in the US, failed to secure the personal data of 140 million Americans, compromising their names, credit card numbers, addresses, social security numbers, birth dates, and more in the process. Days after the breach was identified and before the company publicly announced the breach, executives sold millions of dollars worth of stock in the company, though Equifax claims these transactions were unrelated to the breach.[28]

Data breaches in Germany also span a diversity of targets, motives, and consequences. In 2019, a twenty-year-old lone German hacker confessed to leaking the personal details – including family pictures, personal phone numbers, credit card details, party documents, and addresses – of prominent German journalists, celebrities, and hundreds of politicians from all political parties with the exception of the far-right Alternativ für Deutschland. The data was posted on Twitter as an Advent calendar and had amassed 18k followers before being shut down, and Chancellor Angela Merkel was among the victims. Notably, government networks were not compromised in the hack.[29] In 2014, researchers studying a botnet infected with malware discovered a collection of 16 million email addresses and passwords belonging primarily to users in Germany; months later, authorities uncovered an additional set of 18 million credentials. The perpetrators, believed to be based in the Baltics, are thought to have used these email and password combinations to access users' online shopping accounts, thus granting them access to financial data.[30] In cases like these, the differentiation between culprits and victims, lawbreaking and immorality is unambiguous, but these distinctions are not always easy to draw. In one of the most widely publicized scandals in recent years, hackers illegally accessed millions of documents, which were subsequently leaked to a journalist at *Süddeutsche Zeitung*. These documents formed the basis of the Panama Papers, a staggering expose of wealthy elites around the world harnessing fraud and tax evasion for financial gain.[31] A number of breaches compromising consumer data have also occurred. In August 2019, customers of a MasterCard loyalty program had their home addresses, payment card information, phone numbers, and other pieces of personal data posted online.[32] While writing this report, it was discovered 3 million Germans had their personal data exposed after CAM4, an adult live streaming service, failed to secure one of its databases. Some of the records contained users' first and last names, email addresses, username, device information, chat transcripts, and payment logs,[33]

25 Frias, "The Ex-Amazon Employee Accused of Hacking into the 5th-Largest Credit-Card Company in the US Posted about It Online, the FBI Says."
26 "Exclusive."
27 "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases | Technology | The Guardian."
28 Haselton, "Credit Reporting Firm Equifax Says Data Breach Could Potentially Affect 143 Million US Consumers."
29 Welle (www.dw.com), "German Hacker behind Massive Political Data Leak Identified | DW | 08.01.2019."
30 "E-Mail-Passwörter Gestohlen: 18 Millionen Datensätze - DER SPIEGEL."
31 "New Panama Papers Leak Reveals Mossack Fonseca's Chaotic Scramble."
32 "Mastercard Reports Data Breach to German and Belgian DPAs."
33 "CAM4 Adult Cam Site Exposes 11 Million Emails, Private Chats."

underscoring the fact that cyberincidents occur not only for the purpose of profit and competitive advantages (e.g., sensitive national security information, valuable intellectual property, trade secrets, etc.) but also simply for reputational damage and humiliation, too.

Tensions

At times, German and American cybersecurity interests and actions have clashed, and outstanding tensions between the two countries on matters of cyber policy remain. In 2013, German news magazine *Der Spiegel* reported that an American intelligence unit of the CIA and NSA had evidently monitored Chancellor Angela Merkel's cellphone "for more than a decade" via a clandestine listening station at the American embassy in Berlin. The news led to a stern call from Merkel to then-President Barack Obama, questions over the transatlantic free trade agreement, and a strained relationship between the two states. Merkel's spokesperson, Steffen Seibert, called the findings a "grave breach of trust".[34] Today, the rollout of 5G, the next generation of network connectivity, remains a contentious issue. While the US has banned Shenzhen-based Huawei as a 5G provider, Germany has yet to do so; in response, the United States has threatened to withhold intelligence from Germany should Germany use Huawei[35] since the firm may act as an extension of the Chinese state security apparatus, enabling Beijing to eavesdrop on the network and monitor the data flowing across it.[36]

Cyber Insurance and Risk Management

The staggering personal, business, and national security-related costs of cybersecurity incidents has spawned a nascent and rapidly growing cybersecurity insurance industry to limit the fallout of leaks, breaches, and hacks. The sector is larger, more robust, and further developed in the United States than in Germany, though cyberinsurance offerings in both countries are burgeoning.

Insurance and the Transatlantic Connection: A Historical Note

The history of insurance encompasses the a number of political affairs from the US and Germany. Most notably, in 1885, Chancellor Otto von Bismark effectively launched the world's first health insurance system. Frederick Ludwig Hoffman, a German born in 1865 who emigrated to the United States at the age of nineteen after years of attempting to escape poverty in Germany, stridently opposed these "ideas of government control and state socialism" from Germany, as he articulated later in his life.[37] Shortly after his arrival in the US, he discovered a proclivity for statistics and the promise it held for improving working conditions and for ameliorating social injustices. A German-turned-American commenting on European social policies – which he deemed paternalistic at a time when anti-German sentiments surged in the wake of World War I – he staunchly defended American institutions from alleged socialist threats. An autodidact, Hoffman became a statistician for the Prudential Insurance Company of America and after naturalizing, served as President of the American Statistical Association.[38] Repulsed by German welfare efforts, he left an indelible mark on the evolution of insurance in the US.

Today, Hoffman's legacy is mixed. He grew interested in measuring differences between blacks and whites, and his first book, *Race Traits and Tendencies of the American Negro*, "used statistics to demonstrate the supposed biological degeneracy of blacks and the innate superiority of the 'Anglo-Saxon' race".[39] At the same time, his statistical insights were transformational. Hoffman

34 "Cover Story: How NSA Spied on Merkel Cell Phone from Berlin Embassy - DER SPIEGEL."
35 Barnes and Satariano, "U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist."
36 Chazan, "Trump's Ambassador to Germany Hits out at Berlin over Huawei."
37 Hoffman, "Scientific Racism, Insurance, and Opposition to the Welfare State."
38 "Frederick L. Hoffman (1865–1946) | Amstat News."
39 Hoffman, "Scientific Racism, Insurance, and Opposition to the Welfare State."

was among the first to discover a connection between asbestos and lung disease among workers, and he even contended that a link exists between tobacco and cancer in 1915. Despite his contributions to public health, his research justified decisions to withhold insurance from black Americans and his steadfast opposition to progressive insurance policies "set a precedent for the commercial insurance industry's role in blocking universal health coverage for the rest of the century."[40]

Although the state of American and German healthcare is an ancillary observation, the influence of Hoffman's work on present-day debates about American healthcare and the intersection of physical and cyber health like the aforementioned coronavirus-related cyber abuse notwithstanding, Hoffman's work raises a fundamental issue as yet unresolved in the case of cyberinsurance. Hoffman's views were steeped in racialized views of the time, as evinced in his belief that "that black lives were so precarious that the entire race was uninsurable," but they beg the question of what qualities would deem an organization too risky to underwrite with cyberinsurance.[41] Moreover, on whom does the onus of cybersecurity rest? Hoffman found state-organized health insurance repugnant. Are individuals, individual companies, or governments solely responsible for their own cybersecurity? In the cyber world in which cyberattacks regularly constitute political maneuvers with precise targets, however, does cyber defense function as a quasi-public good? Where do national protections end and individual responsibilities begin?

Cyberinsurance in Practice

In theory, cyberinsurance operates just like other forms of insurance – value generated from risk pooling and prudent underwriting to hedge against expected losses with commensurate premiums. Cyberinsurance offerings on the market are often the combination of several constituents: errors and omissions (product failures, performance issues, errors), media liability (personal injury, intellectual property infringement excluding patents), network security (business interruptions, extortion, unauthorized access, malware dissemination, destruction of data assets), privacy (rogue employees, lost devices).[42]

Opinions on cyberinsurance vary. One source, a CTO of a large American organization targeted in a massive, publicized cyberattack, who asked to remain anonymous affirmed that cyberinsurance coverage had helped his organization significantly. When the need arises, cyberinsurance provides a post-incident buffer to the affected organization by limiting dependence on government aid, by mitigating financial and reputational loss, and by facilitating the recovery process. Another source, a cybersecurity consultant for small and medium-sized organizations, stated, "Getting cybersecurity insurance is not one of my recommendations for [the organizations I work with]. They are better off investing in preventative steps like staff education." The industry does not yet appear to have reached a consensus.

Cyberinsurance is still in its infancy suffers from a number of drawbacks, three of which stand out among the rest. First, cybersecurity insurance suffers from a lack of data and standards. In short, creating insurance policies requires that insurers and underwriters have robust, actuarial data on what works and what does not, what conditions correspond to what outcomes. Sprinklers in the late 1800s were observed to help extinguish fires, but since pipe sizes and sprinkler placement varied, results were mixed. In 1895, fire and sprinkler insurance representatives met to review the matter and settled on specific standards for sprinkler installation, which the sprinkler industry adopted and which fire insurance underwriters mandated.[43] Similar standards do not yet exist for cyberinsurance. Insurance companies price premiums given information about the likelihood of a

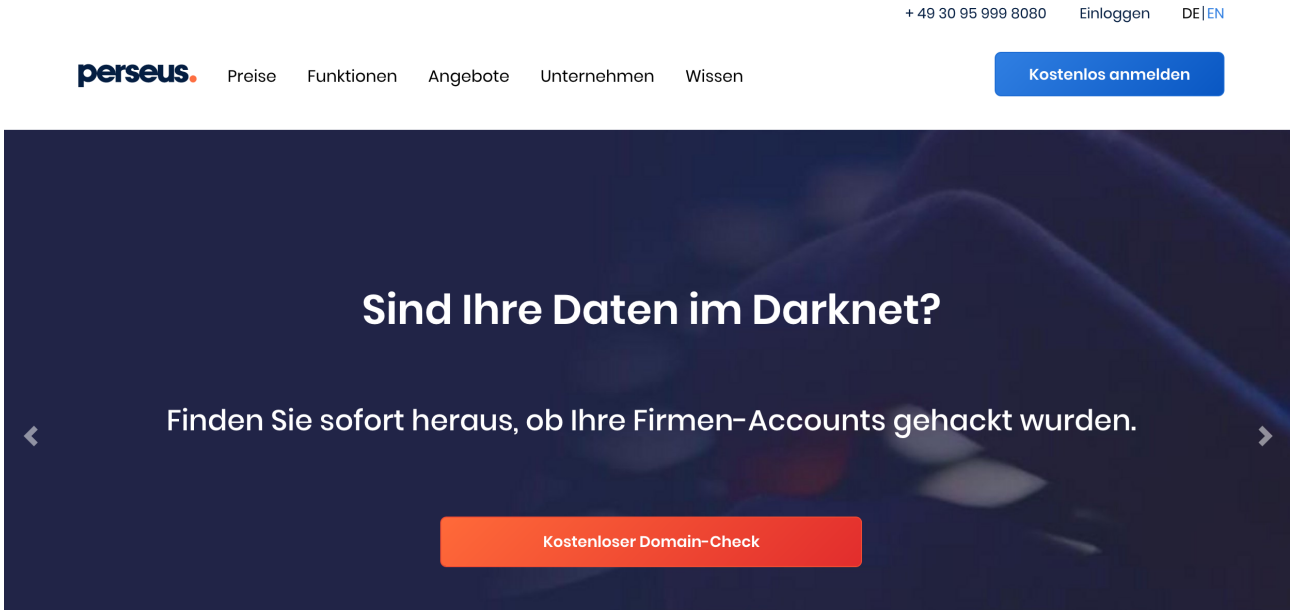
40 Hoffman.
41 O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*.
42 Fauntleroy, Wagner, and Odell, "Cyber Insurance - Managing Cyber Risk."
43 Fauntleroy, Wagner, and Odell.

loss and the corresponding cost of that loss, and the complexities involved in cyberinsurance cannot be understated. Evaluating the value of a company's assets to a foreign adversary, estimating the marginal impact of enabling two-factor authentication, and assessing the risk of a highly mobile team losing a device may all seem like basic exercises in principle but require robust, calibrated data to properly ascertain their risks in an actuarially sound manner. Firms simply cannot make these predictions and price their products without the requisite benchmarks in place. Second, most cyberinsurance policies include a war exclusion, meaning insuring organizations will not be held liable if a cyber incident occurs as a result of an act of war. This definition, however, remains unclear, partly because cyberwar remains a nebulous concept. Mondelēz held a cyberinsurance policy from Zurich Insurance before losing over $180 million as a result of the NotPetya ransomware. When the US government cited Russia as the perpetrator of the NotPetya attack, Zurich Insurance claimed that the event was an act of war and thus outside the scope of the insurance policy (recalling Hoffman's provocations about who, ultimately, is liable). Mondelēz is suing Zurich Insurance, and Merck, which lost over $700 million, is suing more than 20 insurance companies over the war exclusion indemnity.[44] Lastly, many cybersecurity insurance firms lack adequate reinsurance to balance concentrations of cyber risk.

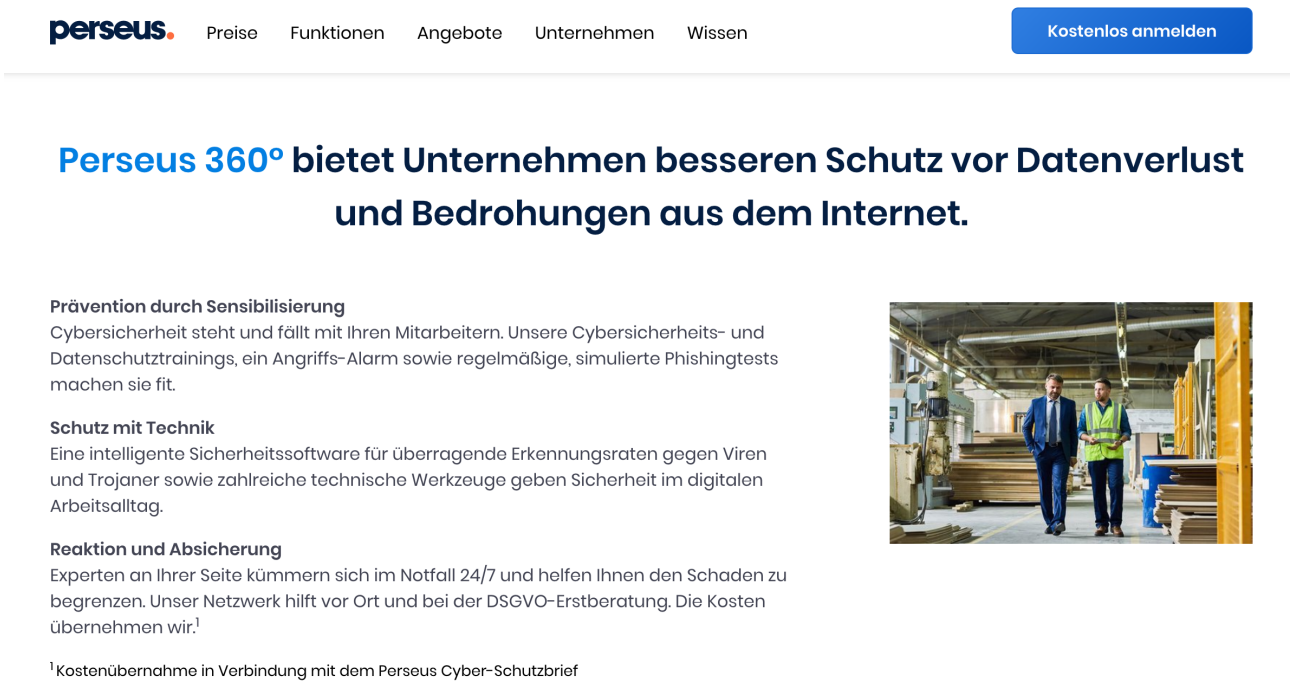
A Glimpse at the Cyberinsurance Industry

Perseus, a Berlin-based cybersecurity startup, and CNA Financial Corporation, a multinational, 123-year-old firm based in Chicago, both offer cyberinsurance products. A review of their products and services indicates what similar providers in the industry offer. Perseus is a private company founded in 2017 and has fewer than 50 employees. The company released a cyberinsurance product designed for small and medium-sized businesses in the fall of 2017 to meet the lack of cyber protection plaguing German companies. The firm claims to employ a system "starting with an AI-based security scoring model that continuously calculates and updates risk scores, automatically suggests measures to prevent breaches and adjusts risk scores based on the security technology used."[45] Promotional materials about the company's insurance product state that, in the event of a cyber incident, the firm will send IT forensics experts on site, complete a damage assessment, determine the losses to the company, cover the costs associated with data recovery and malicious software removal, pay the fees associated with an external audit, assist the company in shoring up its defenses after an attack, and document the whole process. The annual indemnity limit per company is capped at 50,000 EUR.[46]

44 Satariano and Perlroth, "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong."
45 "(41) Perseus Cyber Security: About | LinkedIn."
46 "Cyber Cover for Reimbursement after Cyber Attacks | Perseus."



The landing page of Perseus, a German cybersecurity firm that offers cyber coverage for small and medium-sized enterprises, asking "Is your data in the dark web?"[47]



This promotional splash from Perseus reads "Perseus 360° offers companies better protection against data loss and threats from the internet." The text outlines the company's three-pronged approach that encompasses employee cybersecurity training, technical tools to detect cyber threats, and expert help in the case of an emergency. With protection from the Perseus Cyber Cover, the texts reads, "We'll cover the costs."[48]

In comparison to Perseus, CNA Financial is a much larger, public company with more than 5,000 employees and clients spread across 150 countries.[49] At the end of 2019, it ranked sixth in dollar-volume of direct premiums written,[50] and when taking cyber insurance as part of a larger insurance package into account, CNA boasts 6.5% of market share, making it the second-largest

47 "360° cyber security for small and medium sized businesses | Perseus."
48 "360° cyber security for small and medium sized businesses | Perseus."
49 "Rely-On-NetProtect_CNA.Pdf."
50 "Rankings."

package cyber insurer.[51] According to the company's website, CNA's offerings are "built on nearly two decades of cyber insurance expertise".[52] The firm offers its cyberinsurance to companies with at least two years of operating history and annual revenues of up to $10 billion.[53]

CNA

Cyber

Cyber Risk Solutions

CNA is proud to offer a market-leading suite of cyber liability insurance products and risk control resources. Our solutions are anchored by more than 15 years of cyber coverage expertise and are designed for companies with two or more years of operating history and revenues up to $10 billion* with no revenue threshold for excess placements.

NetProtect 360®
This cyber liability policy provides access to underwriting acumen and risk management strategies that combine people, controls, technology and insurance into a comprehensive solution to help businesses remain prepared and competitive.

EPS Plus
Designed for professional services firms, this policy provides many of the cyber liability solutions of NetProtect 360®, along with offering essential E&O Liability coverage.

Epack Extra®
Designed for smaller clients, Epack Extra® combines into a single modular form with Professional Liability coverage, including Directors & Officers, Employment Practices Liability, Fiduciary, Miscellaneous Professional Liability, Network Security and Privacy Injury Liability and Media.

Endorsements
Select from a wide range of options to extend coverage on existing forms or access additional Cyber Liability coverages.

Leading coverages designed for:

- Business Services
- Construction
- Financial Institutions
- Healthcare
- Manufacturing
- Professional Services
- Real Estate
- Retail
- Technology

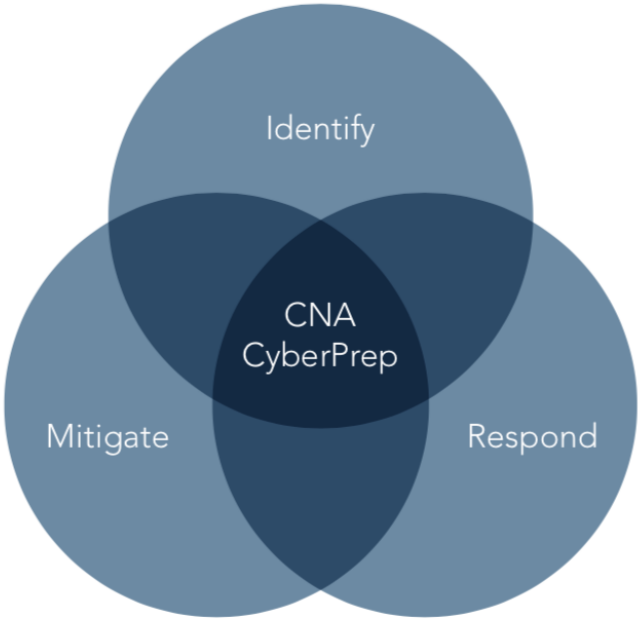
Coverage	NetProtect 360®	EPS Plus	Epack Extra
Media	X	X	X
Network Security, Privacy and Regulatory Proceeding (incl. fines)	X	X	X
E&O (Tech, MPL)		X	X
Privacy Event Expense	X	X	X
Extortion	X	X	X
Privacy Regulation Investigation	X	X	X**
Crisis Response	X	X**	X**
PCI Loss	X**	X**	X**
Business Interruption and Extra Expense	X	X	X**
Dependent Business Interruption and Extra Expense	X**	X**	X**
Network Restoration	X	X	X**
Bricking	X	X**	X**
Reputational Harm	X**	X**	X**
Network Failure	X**	X**	X**
Dependent Network Failure	X**	X**	X**
Voluntary Shutdown	X**	X**	X**
E-Theft, Social Engineering and Telephone Fraud	X**	X**	X**

An overview of CNA Financial Corporations cyber liability insurance products. CNA NetProtect 360, the basic plan shown in the table, covers "losses for network extortion, business interruption expenses, loss or damage to a network and e-theft."[54] The table outlines a number of different incidents covered. 'PCI Loss' refers to the loss of payment card information, and 'Bricking' refers to an electronic device that becomes totally unusable, often as a result of broken firmware, the software that makes hardware function as intended.[55]

51 "Top 10 Cyber Insurance Companies in the US | Insurance Business."
52 "CNA Cyber Risk Solutions | CNA."
53 "CNA+Cyber+Liability+Risk+Solutions.Pdf."
54 Hunt, "Top Companies Offering Cyber Insurance."
55 "CNA+Cyber+Liability+Risk+Solutions.Pdf."

CNA CyberPrep

CNA CyberPrep is available to all CNA cyber policyholders, providing them with a network of cybersecurity professionals and services to actively identify, mitigate and respond to their cyber risks. CNA CyberPrep is modeled on industry-leading cybersecurity frameworks for standards, guidelines and best practices, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and is rooted in strong partnerships with highly regarded cybersecurity professionals.



Identify

Identify current cybersecurity posture: A select group of vendors and services help insureds identify the strengths and weaknesses of their cybersecurity posture, while also providing recommendations for further cybersecurity steps.

Mitigate

Mitigate potential cybersecurity risk: Cybersecurity recommendations are put into action by additional vendors and services, which help insureds enhance their cybersecurity posture by mitigating potential cyber risk. Services include next generation anti-virus protection, incident response planning and testing, policy and procedure development and testing, password management, employee education and multi-factor authentication.

Respond

Respond to cyber incident: Security incidents are often high-pressure situations. CNA's incident response vendors have a deep understanding of critical steps to minimize an incident's impact and provide help after one occurs. These vendors include breach/privacy counsel, forensic investigation and remediation firms, notification vendors, credit monitoring vendors and public relation firms.

CNA cyberinsurance policyholders gain access to CNA's "CyberPrep" product, summarized in this promotional image. Completing these preparatory steps likely reduces the chance of a cyber incident occurring. For extra fees, clients can pay for CNA to facilitate a number of additional services: third-party penetration testing to stress test the client's defenses, security awareness training, and password management, among others.[56]

56 "CyberPrep+Brochure.Pdf."

The Transatlantic Implications of Cybersecurity Risk and Cyberinsurance

As these abridged case studies suggest, the emerging cyberinsurance market is mixed and seeks to minimize the harms from a variety of threats and sources of exploitation: domestic and international adversaries, human behavior and psychology, technical deceit, lucrative black and gray markets for personal data, political developments that feed uncertainty, and more. Understanding what these developments might mean broadly and for the US and Germany specifically is a daunting task that, in truth, feels somewhat presumptuous. The unknown unknowns aside, the known unknowns alone are enough to question the soundness of any attempt to predict how cybersecurity and cyberinsurance will progress. Many of today's cyber risks are novel and can be difficult to articulate *ex ante*. For starters, the attack surface in question is not only multifaceted, but it is also dynamic and responsive to exogenous political, economic, social, technological, environmental, and legal developments. The technical and social engineering that inform cybersecurity strategy is highly specialized and complex. Even present-day understanding of cyberattacks may be lagging – at best– or misconceived – at worst – since solutions to meet cybersecurity challenges are founded upon an acknowledgement and identification of existing problems. In reality, however, the best cyberattacks are ones that are never discovered in the first place.

A more tractable approach, therefore, might be to ascertain *how* cyber risk and cyberinsurance is likely to affect the transatlantic connection even if the exact nature of *what* might happens remains uncertain. This report suggests that the evolution of cybersecurity risk (and efforts to insulate against it with cyberinsurance) bears structural resemblance to the evolution of financial risk; understanding how financial risk and related incidents – like the 2008 financial crisis – shaped US-German relations provides hints as to how cyber risk and related incidents may do so as well. In this vein, the following sections substantiate the similarities between financial and cyber risks and speculates what these parallels might mean for US-German relations in the event of a large-scale cyber incident.

Cyber Risk and Financial Risk: The Sociocultural Context

One of the most basic similarities between the evolution of financial and cyber risk relates to people in the industry. In recent years, there has been a pronounced migration of employees leaving the financial industry – specifically investment banking – for careers in the technology industry. As the Los Angeles-based startup company Comparably summarized in a blog post, "Tech is the new finance. All over the world, people are increasingly forgoing banking for jobs with tech companies..."[57] In a *Forbes* article entitled "6 Ways To Seamlessly Transition From A Career In Finance To Tech", one tech founder noted, "the reality is that Google battles Goldman for recruiting top talent."[58] The numbers concur. The *Wall Street Journal* notes that 2013 was the first year Stanford's Graduate School of Business sent more graduates to tech than to finance, a pronounced reversal of students' preference for finance from just two years before,[59] reflecting trends at other top American business schools.[60] This pattern does not simply apply to newly-minted college and business school graduates; seasoned financial professionals are also flocking to tech. In 2017, *Business Insider* profiled a "banker-turned-Googler" named Sameer Syed who "hosts a quarterly roundtable called Wall Street to Silicon Alley, a group that helps financiers transition into the world of tech. Syed said that since he's switched industries, he's been inundated with requests from people looking to make a similar change."[61] Adam Zoia, CEO of the recruiting firm Glocap Search commented, "Since the financial crisis, finance as a status career has diminished and the relative

57 "Study: What the C-Suite Earns (A Look at Executive Pay in Tech) – Comparably Blog."
58 "6 Ways To Seamlessly Transition From A Career In Finance To Tech."
59 Korn, "Elite Grads in Business Flock to Tech."
60 "Why Lawyers and Bankers Are Leaving Their Jobs (and Where They're…."
61 "A Banker-Turned-Googler Explains How to Translate Finance Experience into Tech - Business Insider."

attractiveness has shifted significantly in favor of tech," in a CNBC article headlined "Why Silicon Valley wants Wall Street's best."[62] Executives are evidently also part of the influx of tech workers. A representative of an executive search firm revealed in 2015, "Seven out of 10 conversations I have with investment bankers now end with them asking me to keep them in mind for jobs in technology. That almost never happened five years ago." While this body of evidence is all from the US, *Bloomberg* claims that "The trend is worldwide."[63]

Finance is also a strong reference for American and German technological risk is because cultural attitudes towards risk manifest themselves similarly in both industries; Americans, in short, tolerate more risk than Germans do. Germans tend to be fiscally conservative relative to Americans, and they are far more circumspect and privacy-conscious when sharing personal data with private companies. These conventions are apparent among the individual preferences of Germans and Americans. Compared to Germans, Americans have a higher tolerance for financial risk. Princeton University economic historian summed up this point in stating, "The Germans are much more worried than the Americans, for example. They think they need to prepare for every eventuality, that bad things can hit them and that they need to be ready for that."[64] In fact, the first savings bank in the world opened in 1778 in Hamburg, and even today, German tabloids tend to denounce low interest rates as harmful to savers, not beneficial to investors. Indeed, Germans "continue to regard stock markets with disdain, and still put their faith in the good old-fashioned Sparkasse," a reference to the Savings Bank. Kai Uwe Peter, Managing Director of Berliner Sparkasse, noted "Saving is seen as the morally right thing to do. It is more than a simple financial strategy." The household savings rate in German "is remarkably stable over time, unaffected by economic crises and interest rate changes" and, at roughly 10% of disposable income, is about twice as much as that of the United States.[65]

Germans are similarly risk-avoidant regarding tech matters of privacy, corporate surveillance, and related cyber incidents. Cyber criminals thrive in environments in which users entrust their personal data to companies online; more data sharing creates more opportunities to undermine cybersecurity and, of course, more chances to profit from any intercepted information – whether financially or otherwise.

Germany long led the world on matters of data protection law and privacy, and due in large part to historical reasons,[66] Germany has championed the cause of informational self-determination after a landmark court ruling from 1983 established "the individual's right to allow or block the sharing of their personal information with any public or private entity."[67] Under the European Union's General Data Protection Regulation (GDPR) that has been in effect since May 2018, data controllers are required to disclose data breaches within 72 hours of discovery.[68] The GDPR imposes harsh fines on egregiously offending companies – up to 20 million Euros or 4% of the firm's *global* revenue from the previous year, whichever is greater.[69] As two experts note of German values, "Fear of the private sector and, even more so, government abuse of personal data is widespread," and this fear extends to the personal data collected online.[70] The *New York Times* states simply, "Germany is one of the most privacy-sensitive countries in the world."[71] Starting in 2013,

62 Chokshi, "Why Silicon Valley Wants Wall Street's Best."
63 "Why Bankers Are Leaving Finance for No-Salary Tech Jobs - Bloomberg."
64 "Why Are Germans so Obsessed with Saving Money? | Financial Times."
65 "Why Are Germans so Obsessed with Saving Money? | Financial Times."
66 "Germany - The Privacy, Data Protection and Cybersecurity Law Review - Edition 6 - TLR - The Law Reviews."
67 "Handelsblatt Explains."
68 "Art. 33 GDPR – Notification of a Personal Data Breach to the Supervisory Authority | General Data Protection Regulation (GDPR)."
69 "What Are the GDPR Fines?"
70 "Echoes of History."
71 Miller and O'Brien, "Germany's Complicated Relationship With Google Street View."

for example, Google Street View showed a jumble of blurred images where residents wished that their homes not be shown, and now Google must inform the public before driving down streets to collect Street View images.[72] In a pan-European analysis of the Internet of Things (IoT) industry that seeks to connect household devices to the internet (e.g., smart toothbrushes, internet-connected beds, intelligent toasters, etc.), Accenture found dampened enthusiasm for IoT tech among German firms since "people in Germany are more sensitive to data protection and privacy issues."[73]

Americans, by contrast, largely still seem to trust their personal data to private companies and continue to share intimate details about their lives publicly online. In a nationally-representative sample of about 1,100 Americans, a March 2020 survey conducted by *The Verge* found that over half of respondents said they trusted their data to eight of the eleven companies in question. (Only Instagram, Twitter, and Facebook – the worst performer of the group – received less than a 50% share of users who trust their data to these platforms.)[74] There is, however, some evidence emerging that American attitudes towards companies that collect and monetize their data is starting to resemble the more wary views of their German counterparts.[75]

Cyber Risk and Financial Risk: The Macroeconomic Perspective

The banking industry and its associated financial risks are a strong model for a study of the technology industry and cyber risks because of their macroeconomic parallels. Much of the innovation in financial engineering (derivatives trading, speculation, etc.) starting in the 1950s came from the United States.[76] Many of the technological advancements enabling data-intensive, internet-based businesses to flourish similarly originated in the US. Accordingly, the United States has set global financial and technological precedents with respect to risk tolerance as American-born financial and technological systems have embedded themselves in international economic structures.

In 2005, the Chief Economist of the International Monetary Fund, Raghuram Rajan, authored a prescient paper titled "Has Financial Development Made the World Riskier?" in which he identified warning signs of the 2008 financial crisis. The abstract states:

> Developments in the financial sector have led to an expansion in its ability to spread risks...On net, this has made the world much better off...Concurrently, however, we have also seen the emergence of a whole range of intermediaries, whose size and appetite for risk may expand over the cycle...As a result, under some conditions, economies may be more exposed to financial-sector-induced turmoil than in the past.[77]

Fifteen years later, despite different mechanisms of securitization and financialization at play, the logic of this argument seems readily applicable to cyber risk.

In both the financial and cyber cases, statistical models are constructed to predict the probability of undesirable outcomes, and prices adjust to reflect the associated risks. Mortgages associated with a higher probability of default (for example, as a result of a poor credit score) cost more, and companies with a high probability of witnessing a cyber incident (for example, as a result of belonging to an at-risk industry like healthcare) pay higher cyberinsurance premiums.[78] In the case of the housing crisis, banks, regulators, and other financial actors underestimated the risk of mortgage defaults (and the domino effect of defaults en masse). In *Financial Engineering: The*

72 Miller and O'Brien.
73 "Milojevic - 2017 - Digital Industrial Transformation with the Interne.Pdf."
74 "The Verge Tech Survey 2020: How People Feel about Apple, Google, Facebook, and More - The Verge."
75 "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information | Pew Research Center."
76 "BHoFE.Png (PNG Image, 1958 × 2273 Pixels) - Scaled (34%)."
77 Rajan, "Has Financial Development Made the World Riskier?"
78 "110 Must-Know Cybersecurity Statistics for 2020 | Varonis."

Evolution of a Profession, authors Tanya Beder and Cara Marshall wrote in 2012 of the financial crisis that "...it is clear risk measurement and risk management failed to identify some exposures...Revising risk measurement methodologies and risk management techniques will be an important focus of the financial engineering community over the next decade."[79] Might the causes of systemic risk miscalculation in financial systems, which defined the 2008 crisis, also induce underestimates of cyber risk underlying technological systems?

This report maintains yes, both the financial sector pre-crisis and digital tech services accumulating personal data today operate on systemic undervaluations of risk because of the economic incentives to do so via externalized costs on common goods. One of the consequences of the aforementioned migration of workers from finance to tech is that that the same principles of internalizing benefits, underestimating risks, devising regulatory schemes largely shaped by the private sector, and externalizing the costs characteristic of the financial crisis has simply spread to and intensified in the technology industry. In an interview for the *Inside Job*, banker and academic Andrew Sheng argued, "A financial engineer builds dreams and, when those dreams turn out to be nightmares, other people pay for it," alluding to the trillions of dollars spent to stabilize markets around the world as a result of stakeholders who overlooked and externalized excessive risk onto taxpayers, including the $700 billion Emergency Economic Stabilization Act of 2008 (in which American taxpayers saved commercial banks) and the 70 billion EUR cost to German taxpayers.[80] The externalized cost that private financial actors failed to account for was excess financial risk, which was then paid for by the public.

In the case of technological systems, the negative externality is the privacy and security cost that the market fails to internalize when cyber incidents occur. Firms that collect personal data internalize the benefits generated by their business models. However, when a leak, breach, or hack occurs, the cost is often not born by the company whose systems were compromised or who failed to protect users' data, but rather by the users themselves. Even for cyber incidents that result in outcomes as conventional and established as identity theft, subsequent obstacles to accessing basic services (e.g., applying for a loan or a job) can present overwhelming costs to users; indeed, even when most savvy victims elect to – for instance – freeze their credit, the cost of doing so is still borne directly by them, not the offending data controller.[81]

Moreover, outside the context of traditional cases like identity theft, it is even clearer that victims, not the responsible organization, assume the costs of cyber incidents. Ransomware, for example, is a type of malicious software designed to hold assets ransom. Users who fall victim to ransomware that exploits software and renders their data inaccessible, for example, will often pay the ransom if regaining access to their data is important enough to them. (In October 2015, FBI agent Joseph Bonavolonta said, "To be honest, we often advice people just to pay the ransom" acknowledging the fact that victims have virtually no recourse.)[82] As Wolff notes, "In the absence of centralized financial intermediaries who could be held responsible or forced to bear the costs of ransomeware thefts, the financial burden for these incidents fell completely on the individuals and organizations who were targeted."[83] In other words, the costs associated with cybersecurity incidents are shouldered by victims themselves, not the systems that allowed them to be victimized.

In even more extreme cases, the manner in which cyber incidents externalize costs onto users and not the entities holding their data grows even more obvious. In the case of Ashley Madison, a website for people seeking extramarital affairs, the company faked a "Trusted Security

79 Beder and Marshall, *Financial Engineering*.
80 Hellwig, "Germany and the Financial Crises 2007 – 2017."
81 Grant, "What to Do When Personal Identity Theft Becomes a Professional Problem."
82 Wolff, Josephine, *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*.
83 Wolff, Josephine.

Award" on its website and touted its security credentials before being hacked and leaking the "names, photos, profile information, email addresses, credit card numbers, and billing addresses of many of the site's 37 million users."[84] While two suicides were putatively connected to the hack, individuals affected by the breach "were permitted to claim up to $3,500...to cover documented losses stemming from the breach."[85] The pattern from one cyber incident after another is well-established – financial compensation fails to adequately recompense victims for their privacy and security-related costs, which are in turn externalized onto individuals to bear on their own.

Similar to the manner in which banks imposed public debt on the public when the risks associated with their private debts proved intractable, entities guilty of poor security practices introduce financial costs and negative externalities onto individuals' privacy and security when cyber incidents occur. Robert S. Taylor, former principal deputy general counsel of the Department of Defense, summarizes the matter succinctly: "Cybersecurity is a common good; lax cybersecurity imposes negative externalities on other economic entities and on private citizens. Failure to account for these negative externalities results in underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment."[86]

Cyber Risk and Financial Risk: Too Big To Fail

A major impetus behind the American bailout of financial institutions was the recognition that some had simply proved to be too indispensable, too interconnected, too big to fail; large tech companies, firms running critical infrastructure, and others whose services mediate other online services similarly exhibit signs of being 'too big to fail.'

As Nick Srnicek writes in *Platform Capitalism*, many of the largest companies in the world today are platforms. Facebook and Google are two-sided market platforms that connect advertisers and consumers, for example. Amazon and eBay provide online marketplaces for buyers and sellers. Airbnb does not own any accommodations but links guests and hosts. Uber does the same for riders and drivers. These companies are ultimately valuable because of their data. As one scholar noted of Srnicek's work, "Platforms place themselves in a position in which they can monitor and extract all the interactions between these groups. This positioning is the source of their economic and political power."[87]

There are a few noteworthy implications of platforms and their strategic positioning. The first set of consequences relate to the centrality they enjoy as platforms. Platforms benefit from network effects that allow them them to operate from positions of market dominance that feed monopolistic behavior. Any Airbnb competitor, for instance, will have to contend with the fact that existing buyers and sellers are already on Airbnb. When promising competitors do manage to grow, however, they are more likely than ever before to be acquired – the second upshot of platforms' power. Between 2008 and 2013, big data-related mergers and acquisitions doubled globally – outpacing all other industries – and the trend appears to be continuing unabated.[88] In some cases, firms are acquired for their data, and sometimes they are refashioned into products built on top of the dominant company's infrastructure. This centrality and tendency to acquire smaller firms render companies already deeply integrated into economic systems even more critical. What happens such companies succeed in accumulating massive amounts of data and suffer a cyber attack?

One such example is Equifax, which – as one of *three* major credit reporting agencies in the United States – enjoys an obvious indispensability. From Equifax's own, company-furnished profile that was taken down after the breach but archived online, "The company organizes, assimilates and

84 Wolff, Josephine.
85 Wolff, Josephine.
86 "How to Measure Cybersecurity."
87 "The Challenges of Platform Capitalism."
88 "LSE Lit Fest 2017."

analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers."[89] In 2017, Equifax lost the names, social security numbers, birth dates, home addresses, and more belonging to 147 million people. As one fraud analyst commented, "On a scale of 1 to 10 in terms of risk to consumers, this is a 10."[90] A *New York Times* opinion columnist bemoaned, "Equifax, you had one job. Your only purpose as a corporation, the reason you were created and remain a going concern, is to collect and maintain people's most private financial data."[91] In the court proceedings it was revealed that among other basic security lapses, Equifax protected the online portal used to manage credit disputes for 182,000 people with the password 'admin' in addition to storing unencrypted user data on a public server online, free for viewing by any attacker.[92] In the aftermath of the Equifax breach, as the *New York Times* published "Experts said it was highly unlikely that any regulatory body would shut Equifax down over this breach. As one of the nation's three major credit-reporting agencies, which store and analyze consumers' financial history for credit decisions, it is likely to be considered too central to the American financial system."[93]

Ultimately, the Federal Trade Commission sued Equifax, and the $700 million settlement (less than 25% of the firm's annual revenue) allowed the company to "not have to publicly admit wrongdoing" and earmarked $31 million to compensate victims.[94] Considering the fact that the breach affected 147 million people, if each affected person were to file a claim, each victim would receive only 21 cents, setting up a disappointing Catch-22. The more victims who file their claims, the stronger the message to Equifax about victims' value for their private data. At the same time, the more claimants, the less money each victim receives, lowering the incentive for people to invest the time into filing the claim in the first place, enabling Equifax to claim that victims do not value their privacy. The *Times* noted how this structure externalized costs onto users in printing "This Catch-22 is reminiscent of Equifax's entire business, where the data brokers wield all the power and operate with impunity, and customers have very little recourse."[95] Another writer noted, "The more data a company has on us, the less likely it is that a breach will put the company in any real danger, because its very size protects it."[96] This phenomenon, the centrality of certain data-rich services and infrastructures, the market-dominant position of some companies, and the associated consolidation of power is the definition of 'too big to fail.'

Cyber Risk and Financial Risk: The Transatlantic Bond

For all these reasons, the evolution of financial risk offers a strong model through which cyber risk can be studied. A 'cyber catastrophe' – as the industry calls it – is the cybersecurity equivalent of a financial crisis-scale event and could take many forms, like a major earthquake drowning Amazon Web Service's servers into the ocean, bringing 15% of all American websites down, violating service level agreements, interrupting business claims, and launching a cascade of crises with exponentially greater costs. While there are clear business incentives to minimize such risks and while companies like Amazon have undoubtedly engineered robust redundancies in their data centers, the fact remains that unanticipated incidents like NotPetya (estimated to have caused $10 billion in damage worldwide alone) or WannaCry ($4 billion)[97] may be looming on the horizon. In this vein, what lessons does the financial crisis have for the American-German transatlantic

89 "Company Profile | About Us | Equifax."
90 Bernard et al., "Equifax Says Cyberattack May Have Affected 143 Million in the U.S."
91 Manjoo, "Seriously, Equifax?"
92 O'Flaherty, "Equifax Lawsuit."
93 Manjoo, "Seriously, Equifax?"
94 Warzel, "Opinion | Equifax Claims May Not Get You $125."
95 Warzel.
96 Manjoo, "Seriously, Equifax?"
97 "Total WannaCry Losses Pegged at $4 Billion - Reinsurance News."

connection given the possibility of a cyber catastrophe? Understanding how the financial crisis impacted transatlantic relations may shed light on the implications of its cyber analogue.

The financial crisis prompted a paradigm shift in the framework governing US-German relations. The US and Germany adopted different responses to the crisis, which in turn invited a comparison of their economic judgement. First, while both the United States and Germany approved economic stimulus packages, leaders in each country defended their decisions differently. The American response –led by the Bush and Obama Administrations – justified the stimulus by citing the need to support demand in the economy, while German politicians did so by appealing to the need to remain competitive in the global market. Secondly, the American and German stimulus packages differed as well. The American stimulus focused on tax cuts, investments in infrastructure, and state aid. Germany, having already invested heavily in infrastructure, instead used the stimulus to support *kurzarbeit,*[98] a reduced working-hour program to help companies retain employees as opposed to firing them.[99] These differences may appear inconsequential on the surface, but they directly contributed to different economic outcomes in the two countries.

As the aftermath of the financial crisis demonstrated, "Germany emerged as a world champion of the economic rebound."[100] The strength of the German economy's countercyclical measures grew apparent when, between 2008 and 2009, American unemployment grew 4.5 percentage points, while German unemployment over the same period remained relatively stable. While American firms fired employees and then rehired new employees once they had the means to do so, the existence of *kurzarbeit* allowed German firms to avoid the high fixed costs of searching for and hiring new employees in the aftermath of the crisis.[101] According to Nicholas Kulish, former Berlin bureau chief for the *New York Times*, the preparedness of the German economy reflects that it "made the short-term sacrifices necessary for long-term success that Germany's European partners did not. And it will reinforce the widespread conviction among policy makers that they handled the financial crisis and the painful recession that followed it far better than the United States, which, they never hesitate to remind, brought the world into this crisis."[102] The end result, as Klaus Larres, Senior Fellow in the Center of Transatlantic Relations at Johns Hopkins University's School of Advanced International Studies, and Ruth Wittlinger, Professor in the School of Government and International Affairs at Durham University, wrote in *German-American Relations in the 21st Century: A Fragile Friendship*, "The fallout from the financial crisis has been an even greater divergence of domestic economic preferences between Germany and the United States than this had previously been the case."[103]

This divergence of preferences matter, according to Professor at the Chair for Comparative European Governance Systems at Chemnitz University of Technology because "the financial crisis has significantly changed the parameters of the bilateral relations between Germany and the US in the context of wider EU–US transatlantic relations."[104] As he notes, the advantages of Germany's coordinated response "resulted in increasing skepticism towards US-style liberal market capitalism" in which economic actors are simply more subject to the vicissitudes of the market.[105] American skepticism towards its European counterparts over the same time period also seems to have grown. Former presidential counsellor and National Security Advisor Zbigniew Brzezinski, while reflecting on the European sovereign debt crisis, admonished, "Europe's lack of global ambitions makes for

98 "Silvia - 2011 - Why Do German and U.S. Reactions to the Financial .Pdf."
99 "Defying Others, Germany Finds Economic Success - The New York Times."
100 "Global Debt Disaster: What the Financial Crisis Means for Germany - DER SPIEGEL."
101 "Silvia - 2011 - Why Do German and U.S. Reactions to the Financial .Pdf."
102 "Defying Others, Germany Finds Economic Success - The New York Times."
103 "German-American Relations in the 21st Century: A Fragile Friendship - Google Books."
104 Schweiger, "The Global Financial Crisis and the Euro Crisis as Contentious Issues in German-American Relations."
105 Schweiger.

excessive reliance on America and makes the American public more skeptical of Europe."[106] This mutual skepticism, particularly given the strains imposed on transatlantic relations by the Trump Administration, has resulted in looking inwards and a renewed focus on domestic needs, competences, and goals on both sides of the Atlantic against an unavoidable backdrop of interdependence. Larres and Wittlinger encapsulate the spirit of this dynamic in their reflections:

> Since the onset of the global financial crisis a growing economic realism has taken hold in German-US relations. This has become ever more prominent in the context of the global financial crisis as domestic constituencies have become more narrowly focused on their economic self-interest and on maintaining what they perceive as their national comparative advantage. However, due to the strong linkages between the German and the US economy, the respective national constituencies cannot ignore bilateral trade relations and economic cooperation as an important factor in maintaining their domestic comparative advantage.[107]

Similar dynamics are emerging in transatlantic cybersecurity relations. Both German exports and cybersecurity strategy have been growing increasingly independent from the United States. In the 1970s, "up to 14 percent of German exports went to the US," and in 2010, the share of US-bound exports was a meager 6.8 percent.[108] Last year, only 8.8 percent German exports were sent to the US. While this shift seems attributable to rising demand from countries like China and Brazil, this change is symbolic of the fact that German exports (which drives its economic growth with roughly half of Germany's economy driven by its export of goods and services)[109] are becoming less reliant on the United States. Germany's cybersecurity strategy is similarly seeking independence from the United States, a trend that commenced in the aftermath of the Snowden revelations. In August 2018, Germany shared plans for a joint project between the interior and defense ministries "to fund research on cyber security and to end its reliance on digital technologies from the United States, China and other countries."[110] Interior Minister Horst Seehofer stated in 2018, "It is our joint goal for Germany to take a leading role in cyber security on an international level."[111] Amidst a growing realization that American firms dominate the cloud market and a push for more homegrown, European alternatives,[112] Angela Merkel stated in an October 2019 speech that Europe's reliance on cloud solutions from American firms may have consequences "that we can't fully predict yet today."[113]

While the US and Germany may be focused on domestic economic and cybersecurity matters above transatlantic ones, they remain important partners for one another, and the set of challenges confronting both countries may actually foster enhanced cooperation. The United States is Germany's largest trading partner outside the European Union,[114] and as the US State Department describes, "EU Member States are collectively the United States' biggest trading partner, and Germany, as Europe's largest economy, is at the heart of that relationship."[115] Additionally, both states are crucial investment partners for each other. Similarly, the United States and Germany face many of the same cyber adversaries, including China, Russia, and Iran. Cyberespionage of both the private and public sector remain a key concern for both countries. Cybersecurity – an inevitable challenge of twenty-first century statecraft – presents Washington and Berlin a unique opportunity

106 "German-American Relations in the 21st Century: A Fragile Friendship - Google Books."
107 "German-American Relations in the 21st Century: A Fragile Friendship - Google Books."
108 "Global Debt Disaster: What the Financial Crisis Means for Germany - DER SPIEGEL."
109 "Germany Trade Statistics | WITS."
110 "Germany, Seeking Independence from U.S., Pushes Cyber Security Research."
111 "Germany, Seeking Independence from U.S., Pushes Cyber Security Research."
112 Stupp, "EU Wants Homegrown Cloud Services to Rival Amazon, Microsoft."
113 "Bundeskanzlerin | Aktuelles | Rede von Bundeskanzlerin Merkel Beim Deutschen Maschinenbaugipfel Des Verbandes Deutscher Maschinen- Und Anlagenbau e.V. Am 15. Oktober 2019 in Berlin."
114 "Facts about German Foreign Trade."
115 "U.S. Relations With Germany - United States Department of State."

to respond to common set of dynamic, global circumstances cooperatively in a capacity that can both advance their respective national interests and strengthen the transatlantic relationship.

Conclusion

The challenges and opportunities created by cybersecurity concerns in the twenty-first century are novel. By 2022, the number of internet users is projected to reach 6 billion, and this connectivity affords internet users the chance to dramatically boost business productivity, to lower communication costs with people all around the world, to share stories and hopes and dreams with almost anyone they choose.[116] As the industry powering the Internet of Things develops, the data connected users share will no longer be confined to information they actively grant internet companies (e.g., credit card details) or data they emit (e.g., location histories via smartphones).

Digital footprints of the twenty-first century will encompass even more intimate details than those today as internet-connected devices are introduced into the home and private spaces: the smart bed that collects data on users' sleeping habits, the toaster that flags an overconsumption of carbohydrates, the smart watches that sense increased heart rates before its users meet with their superiors at the office. This data is incredibly valuable, and it is both an asset and a liability. As Ginni Rometty, Chair, President, and CEO of IBM opined:

> We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world.[117]

More digitization, more extensive collections of personal and behavioral data, and more critical infrastructures that rely on the cloud create many opportunities, but they also expose new dependencies on technologies that – as the past illustrates – may very well be riddled with vulnerabilities. For the United States and Germany, a nascent cyberinsurance industry seeks to contain these risks by insuring firms against losses associated with cybersecurity incidents. Though this industry is new and its future difficult to predict, the evolution of cyber risk bears striking resemblance to the evolution of financial risk with respect its global relevance, with respect to contrasting German and American risk tolerances, with respect to the externalities they risk imposing on the public, and with respect to the dynamics surrounding 'too big to fail.' Using developments in the financial sector as a guide, these similarities suggest that the United States and Germany may be inclined towards pursuing more isolationist cybersecurity strategies.

At the same time, the United States and Germany share many of the same cybersecurity challenges. Mutual national security, diplomatic, and economic interests in thwarting threats of cyberespionage from foreign adversaries have created a space to not only preserve but to also enhance the American – German transatlantic bond.

116 "Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion."
117 Morgan, "Is Cybercrime the Greatest Threat to Every Company in the World?"

References

"6 Ways To Seamlessly Transition From A Career In Finance To Tech." Accessed May 17, 2020. https://www.forbes.com/sites/laurencebradford/2017/07/26/6-ways-to-seamlessly-transition-from-a-career-in-finance-to-tech/#2ea2e104e944.

"(41) Perseus Cyber Security: About | LinkedIn." Accessed May 17, 2020. https://www.linkedin.com/company/perseuscyberclub/about/.

"110 Must-Know Cybersecurity Statistics for 2020 | Varonis." Accessed May 17, 2020. https://www.varonis.com/blog/cybersecurity-statistics/.

"360° cyber security for small and medium sized businesses | Perseus." Accessed May 17, 2020. /en/, https://www.perseus.de/en/.

Healthcare Innovation. "2017 Breach Report: 477 Breaches, 5.6M Patient Records Affected," January 29, 2018. https://www.hcinnovationgroup.com/cybersecurity/news/13029724/2017-breach-report-477-breaches-56m-patient-records-affected.

"A Banker-Turned-Googler Explains How to Translate Finance Experience into Tech - Business Insider." Accessed May 17, 2020. https://www.businessinsider.com/banker-googler-resume-advice-2017-4?r=DE&IR=T.

"Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information | Pew Research Center." Accessed May 17, 2020. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

"Art. 33 GDPR – Notification of a Personal Data Breach to the Supervisory Authority | General Data Protection Regulation (GDPR)." Accessed May 17, 2020. https://gdpr-info.eu/art-33-gdpr/.

Barnes, Julian E., and Adam Satariano. "U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist." *The New York Times*, March 17, 2019, sec. U.S. https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html.

Beder, Tanya S., and Cara M. Marshall. *Financial Engineering: The Evolution of a Profession*. John Wiley & Sons, 2011.

Bernard, Tara Siegel, Tiffany Hsu, Nicole Perlroth, and Ron Lieber. "Equifax Says Cyberattack May Have Affected 143 Million in the U.S." *The New York Times*, September 7, 2017, sec. Business. https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

"BHoFE.Png (PNG Image, 1958 × 2273 Pixels) - Scaled (34%)." Accessed May 17, 2020. https://ritholtz.com/wp-content/uploads/2015/02/BHoFE.png.

"BSI - Presseinformationen Des BSI - Cyber-Kriminelle Nutzen Corona-Krise Vermehrt Aus." Accessed May 17, 2020. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Cyber-Kriminell_02042020.html.

"Bundeskanzlerin | Aktuelles | Rede von Bundeskanzlerin Merkel Beim Deutschen Maschinenbaugipfel Des Verbandes Deutscher Maschinen- Und Anlagenbau e.V. Am 15. Oktober 2019 in Berlin." Accessed December 6, 2019. https://www.bundeskanzlerin.de/bkin-de/aktuelles/rede-von-bundeskanzlerin-merkel-beim-deutschen-maschinenbaugipfel-des-verbandes-deutscher-maschinen-und-anlagenbau-e-v-am-15-oktober-2019-in-berlin-1681952?mod=article_inline.

"CAM4 Adult Cam Site Exposes 11 Million Emails, Private Chats." Accessed May 17, 2020. https://www.bleepingcomputer.com/news/security/cam4-adult-cam-site-exposes-11-million-emails-private-chats/.

Chazan, Guy. "Trump's Ambassador to Germany Hits out at Berlin over Huawei," November 25, 2019. https://www.ft.com/content/94000e8a-0f8c-11ea-a7e6-62bf4f9e548a.

Chokshi, Trusha. "Why Silicon Valley Wants Wall Street's Best." CNBC, July 30, 2014. https://www.cnbc.com/2014/07/30/careers-bankers-leave-wall-street-for-technology-industry.html.

Choudhury, Saheli Roy. "Cybercriminals Are Exploiting Fears of the Pandemic to Steal Personal Information." CNBC, April 15, 2020. https://www.cnbc.com/2020/04/15/coronavirus-cybercriminals-are-targeting-people-through-phishing-scams.html.

"CNA+Cyber+Liability+Risk+Solutions.Pdf," n.d. Available for download from https://www.cna.com/web/guest/cna/ps/products/CT-AnyCyberLiabilityProdML

"CNA Cyber Risk Solutions | CNA." Accessed November 22, 2019. https://www.cna.com/web/guest/cna/ps/products/CT-AnyCyberLiabilityProdML.

"Company Profile | About Us | Equifax." Accessed May 17, 2020. https://web.archive.org/web/20170813165113/https://www.equifax.com/about-equifax/company-profile/.

"Coronavirus Now Possibly Largest-Ever Cyber Security Threat." Accessed May 17, 2020. https://www.computerweekly.com/news/252480238/Coronavirus-now-possibly-largest-ever-cyber-security-threat.

"Coronavirus Phishing Emails: How to Protect against COVID-19 Scams | NortonLifeLock." Accessed May 17, 2020. https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html.

"Cover Story: How NSA Spied on Merkel Cell Phone from Berlin Embassy - DER SPIEGEL." Accessed May 17, 2020. https://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

"Cyber Cover for Reimbursement after Cyber Attacks | Perseus." Accessed May 17, 2020. https://www.perseus.de/en/functions/cyber-cover/.

Cybercrime Magazine. "Cybercrime Damages $6 Trillion by 2021," February 21, 2018. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

"CyberPrep+Brochure.Pdf," n.d. Available for download from /produkt/cyber-schutzbrief/, https://www.perseus.de/produkt/cyber-schutzbrief/

"Defying Others, Germany Finds Economic Success - The New York Times." Accessed May 17, 2020. https://www.nytimes.com/2010/08/14/world/europe/14germany.html.

DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. "The Tactics and Tropes of the Internet Research Agency," December 18, 2018. http://dataspace.princeton.edu/jspui/handle/88435/dsp01fb494c31z.

Bertelsmann Foundation. "Echoes of History: Understanding German Data Protection." Accessed May 17, 2020. https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/.

"E-Mail-Passwörter Gestohlen: 18 Millionen Datensätze - DER SPIEGEL." Accessed May 17, 2020. https://www.spiegel.de/netzwelt/netzpolitik/e-mail-passwoerter-gestohlen-18-millionen-datensaetze-a-962419.html.

"Exclusive: Told U.S. Security at Risk, Chinese Firm Seeks to Sell Grindr Dating App." *Reuters*, March 27, 2019. https://www.reuters.com/article/us-grindr-m-a-exclusive-idUSKCN1R809L.

"Facts about German Foreign Trade," n.d., https://www.bmwi.de/Redaktion/EN/Publikationen/facts-about-german-foreign-trade.pdf?__blob=publicationFile&v=9

Fauntleroy, J. C., Ryan R. Wagner, and Laura A. Odell. "Cyber Insurance - Managing Cyber Risk:" Fort Belvoir, VA: Defense Technical Information Center, April 1, 2015. http://www.dtic.mil/docs/citations/ADA623798.

"Fitness Tracking App Strava Gives Away Location of Secret US Army Bases | Technology | The Guardian." Accessed May 17, 2020. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

"Frederick L. Hoffman (1865–1946) | Amstat News." Accessed May 17, 2020. https://magazine.amstat.org/blog/2018/10/29/sih-hoffman/.

Frias, Lauren. "The Ex-Amazon Employee Accused of Hacking into the 5th-Largest Credit-Card Company in the US Posted about It Online, the FBI Says." Business Insider. Accessed May 17, 2020. https://www.businessinsider.com/how-the-fbi-caught-paige-a-thompson-alleged-capital-one-hack-2019-7.

"German-American Relations in the 21st Century: A Fragile Friendship - Google Books." Accessed May 17, 2020. https://books.google.de/books?id=Zy_gDwAAQBAJ&pg=PT16&lpg=PT16&dq=impact+of+financial+crisis+on+US+-+German+relations&source=bl&ots=OqTcX21nCx&sig=ACfU3U2CYmWnrMJw4fYETxMa2WPAkFCBMw&hl=en&sa=X&ved=2ahUKEwiY0OS_lrjpAhUNsKQKHVjPBooQ6AEwBXoECAoQAQ#v=onepage&q=financial%20crisis&f=false.

German Hacker behind Massive Political Data Leak Identified | DW | 08.01.2019." DW.COM. Accessed May 17, 2020. https://www.dw.com/en/german-hacker-behind-massive-political-data-leak-identified/a-46991625.

"Germany - The Privacy, Data Protection and Cybersecurity Law Review - Edition 6 - TLR - The Law Reviews." Accessed May 17, 2020. https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210039/germany.

"Germany, Seeking Independence from U.S., Pushes Cyber Security Research." *Reuters*, August 29, 2018. https://www.reuters.com/article/us-germany-cyber-idUSKCN1LE1FX.

"Germany Trade Statistics | WITS." Accessed May 17, 2020. https://wits.worldbank.org/CountryProfile/en/DEU.

"Global Debt Disaster: What the Financial Crisis Means for Germany - DER SPIEGEL." Accessed May 17, 2020. https://www.spiegel.de/international/business/global-debt-disaster-what-the-financial-crisis-means-for-germany-a-779306.html.

Grant, Kelli B. "What to Do When Personal Identity Theft Becomes a Professional Problem." CNBC, January 8, 2019. https://www.cnbc.com/2019/01/07/how-identity-theft-causes-problems-at-work.html.

"Handelsblatt Explains: Why Germans Are so Private about Their Data." Accessed May 17, 2020. https://www.handelsblatt.com/today/handelsblatt-explains-why-germans-are-so-private-about-their-data/23572446.html.

Haselton, Todd. "Credit Reporting Firm Equifax Says Data Breach Could Potentially Affect 143 Million US Consumers." CNBC, September 7, 2017. https://www.cnbc.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html.

Hellwig, Martin. "Germany and the Financial Crises 2007 – 2017," 2007, 60. https://www.riksbank.se/globalassets/media/konferenser/2018/germany-and-financial-crises-2007-2017.pdf

Hoffman, Beatrix. "Scientific Racism, Insurance, and Opposition to the Welfare State: Frederick L. Hoffman's Transatlantic Journey." *The Journal of the Gilded Age and Progressive Era* 2, no. 2 (2003): 150–90.

Lawfare. "How to Measure Cybersecurity," August 26, 2019. https://www.lawfareblog.com/how-measure-cybersecurity.

Cybercrime Magazine. "Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion," July 19, 2018. https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/.

Hunt, Janet. "Top Companies Offering Cyber Insurance." The Balance. Accessed November 9, 2019. https://www.thebalance.com/top-companies-offering-cyber-insurance-4171528.

Department of Homeland Security. “Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security,” October 7, 2016. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

Kang, Cecilia, and Sheera Frenkel. “Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users.” *The New York Times*, April 4, 2018, sec. Technology. https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html.

Kent, Jonathan. “Catlin: Cyber ‘scares Me to Death’ | The Royal Gazette:Bermuda Business.” The Royal Gazette. Accessed November 20, 2019. http://www.royalgazette.com/re-insurance/article/20190503/catlin-cyber-scares-me-to-death.

Korn, Melissa. “Elite Grads in Business Flock to Tech.” *Wall Street Journal*, November 6, 2013, sec. Management. https://www.wsj.com/articles/more-business-graduates-opt-for-tech-over-wall-street-1383697758.

“LKA-BW: Warnmeldung für Unternehmen: Betrügerische Datenerlangung im Zusammenhang mit COVID-19 Soforthilfeanträgen.” Accessed May 17, 2020. https://www.presseportal.de/blaulicht/pm/110980/4558678.

LSE Review of Books. “LSE Lit Fest 2017: Platform Capitalism by Nick Srnicek,” February 24, 2017. https://blogs.lse.ac.uk/lsereviewofbooks/2017/02/24/lse-lit-fest-2017-platform-capitalism-by-nick-srnicek/.

“Machine Bias — ProPublica.” Accessed May 17, 2020. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Manjoo, Farhad. “Seriously, Equifax? This Is a Breach No One Should Get Away With.” *The New York Times*, September 8, 2017, sec. Technology. https://www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html.

“Mastercard Reports Data Breach to German and Belgian DPAs.” Accessed May 17, 2020. https://www.bleepingcomputer.com/news/security/mastercard-reports-data-breach-to-german-and-belgian-dpas/.

Miller, Claire Cain, and Kevin J. O’Brien. “Germany’s Complicated Relationship With Google Street View.” *Bits Blog* (blog), April 23, 2013. https://bits.blogs.nytimes.com/2013/04/23/germanys-complicated-relationship-with-google-street-view/.

“Milojevic - 2017 - Digital Industrial Transformation with the Interne.Pdf,” n.d. https://www.accenture.com/_acnmedia/pdf-49/accenture-digital-industrial-transformation-with-the-internet-of-things.pdf

Morgan, Steve. “Is Cybercrime the Greatest Threat to Every Company in the World?” CSO Online, July 26, 2017. https://www.csoonline.com/article/3210912/is-cybercrime-the-greatest-threat-to-every-company-in-the-world.html.

"New Panama Papers Leak Reveals Mossack Fonseca's Chaotic Scramble." Accessed May 17, 2020. https://www.icij.org/investigations/panama-papers/new-panama-papers-leak-reveals-mossack-fonsecas-chaotic-scramble/.

O'Flaherty, Kate. "Equifax Lawsuit: 'Admin' As Password At Time Of 2017 Breach." Forbes. Accessed May 17, 2020. https://www.forbes.com/sites/kateoflahertyuk/2019/10/20/equifax-lawsuit-reveals-terrible-security-practices-at-time-of-2017-breach/.
O'Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown, 2016.

"Petya (Malware)." In *Wikipedia*, May 5, 2020. https://en.wikipedia.org/w/index.php?title=Petya_(malware)&oldid=954988467.

Rajan, Raghuram G. "Has Financial Development Made the World Riskier?" Working Paper. National Bureau of Economic Research, November 2005. http://www.nber.org/papers/w11728.

"Rankings," January 12, 2014. https://www.iii.org/publications/commercial-insurance/rankings.

"Ransomware Attack Prompts Hancock Health to Pay $50,000 to Hackers." Accessed May 17, 2020. https://www.indystar.com/story/news/crime/2018/01/17/hancock-health-paid-50-000-hackers-who-encrypted-patient-files/1040079001/.

"Rely-On-NetProtect_CNA.Pdf," n.d. Available for download from https://www.cna.com/web/guest/cna/ps/products/CT-AnyCyberLiabilityProdML

Satariano, Adam, and Nicole Perlroth. "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong." *The New York Times*, April 15, 2019, sec. Technology. https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html.

Schweiger, Christian. "The Global Financial Crisis and the Euro Crisis as Contentious Issues in German-American Relations." *German Politics* 27, no. 2 (April 3, 2018): 214–29. https://doi.org/10.1080/09644008.2018.1429411.

"Silvia - 2011 - Why Do German and U.S. Reactions to the Financial .Pdf," n.d. Available for download from https://www.berghahnjournals.com/view/journals/gps/29/4/gps290404.xml

" Covid-19 Coronavirus-Cybersecurity and Information Security Developments Summary 15 May.Pdf," n.d. Available for download from https://www.allenovery.com/en-gb/global/news-and-insights/publications/covid-19-coronavirus-global-merger-review-update

"Spotlight: Securing the 'Internet of Things,'" February 27, 2018. https://internethealthreport.org/2018/spotlight-securing-the-internet-of-things/.

"State Secrets: Germany Is Just Fine with the NotPetya Cyberattack but Its Allies Aren't." Accessed May 17, 2020. https://www.handelsblatt.com/today/politics/state-secrets-germany-is-just-fine-with-the-notpetya-cyberattack-but-its-allies-arent/23581222.html?ticket=ST-6020163-9TRtfe72tCodOHY6GqFA-ap5.

The White House. "Statement from the Press Secretary." Accessed May 17, 2020. https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

"Study: What the C-Suite Earns (A Look at Executive Pay in Tech) – Comparably Blog." Accessed May 17, 2020. https://www.comparably.com/blog/what-the-c-suite-earns-a-look-at-executive-pay-in-tech/.

Stupp, Catherine. "EU Wants Homegrown Cloud Services to Rival Amazon, Microsoft." *Wall Street Journal*, October 24, 2019, sec. WSJ Pro. https://www.wsj.com/articles/eu-wants-homegrown-cloud-services-to-rival-amazon-microsoft-11571909400.

IPPR. "The Challenges of Platform Capitalism: Understanding the Logic of a New Business Model," September 20, 2017. https://www.ippr.org/juncture-item/the-challenges-of-platform-capitalism.

"The History of Cyber Attacks - a Timeline." Accessed May 17, 2020. https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm.

"The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED." Accessed May 17, 2020. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

"The Verge Tech Survey 2020: How People Feel about Apple, Google, Facebook, and More - The Verge." Accessed May 17, 2020. https://www.theverge.com/2020/3/2/21144680/verge-tech-survey-2020-trust-privacy-security-facebook-amazon-google-apple.

"Top 10 Cyber Insurance Companies in the US | Insurance Business." Accessed May 17, 2020. https://www.insurancebusinessmag.com/us/news/cyber/top-10-cyber-insurance-companies-in-the-us-195463.aspx.

"Total WannaCry Losses Pegged at $4 Billion - Reinsurance News." Accessed May 17, 2020. https://www.reinsurancene.ws/total-wannacry-losses-pegged-4-billion/.

"U.S. Relations With Germany - United States Department of State." Accessed May 17, 2020. https://www.state.gov/u-s-relations-with-germany/.

Warzel, Charlie. "Opinion | Equifax Claims May Not Get You $125." *The New York Times*, July 29, 2019, sec. Opinion. https://www.nytimes.com/2019/07/29/opinion/equifax-settlement.html.

"What Are the GDPR Fines?," July 11, 2018. https://gdpr.eu/fines/.

"Who Is Dmitry Badin, The GRU Hacker Indicted By Germany Over The Bundestag Hacks?," May 5, 2020. https://www.bellingcat.com/news/2020/05/05/who-is-dmitry-badin-the-gru-hacker-indicted-by-germany-over-the-bundestag-hacks/.

"Why Are Germans so Obsessed with Saving Money? | Financial Times." Accessed May 17, 2020. https://www.ft.com/content/c8772236-2b93-11e8-a34a-7e7563b0b0f4.

"Why Bankers Are Leaving Finance for No-Salary Tech Jobs - Bloomberg." Accessed May 17, 2020. https://www.bloomberg.com/news/articles/2015-03-15/bankers-embracing-zero-salary-in-tech-may-make-peers-obsolete.

The Muse. “Why Lawyers and Bankers Are Leaving Their Jobs (and Where They’re….” Accessed May 17, 2020. https://www.themuse.com/advice/why-lawyers-and-bankers-are-leaving-their-jobs-and-where-theyre-going.

Wolff, Josephine. *You’ll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*. The MIT Press, 2018.

Acknowledgements

Thank you to the American Council on Germany for its generous support of this project and to the numerous sources interviewed, many of whom shared sensitive information for the sake of this research.

About the Author & Communications

Varoon Bashyakarla is a data scientist at Tactical Tech, a Berlin-based NGO, where his work explores how personal data is used for political influence. His past statistical undertakings led him to a variety of domains: public health, public safety, sports, finance, and cybersecurity. Varoon started his career as a data scientist in Silicon Valley and was previously a Fellow at the inaugural Eric and Wendy Schmidt Data Science for Social Good Fellowship and a Transatlantic Digital Debates Fellow. He holds a double degree in Statistics and Economics from Yale University.

Questions, comments, suggestions, and critiques are all welcome.

vbashyakarla [at] protonmail [dot] com