The Rising Threat to Consumer Data in the Cloud

White Paper on Data Breaches and the Security of Consumer Data on Corporate Systems, Servers, and Networks

Professor Stuart E. Madnick, Ph.D.

December 2022

Support for this study was provided by Apple.
The conclusions and opinions expressed are exclusively those of the author.

This paper details the growing and evolving threat to consumer data when stored and processed on corporate computer systems, servers, and networks. While those systems may reside on-premise, in corporate data centers, or in third-party cloud infrastructure, for simplicity we refer to consumer data storage and processing that does not take place on consumer devices as taking place "in the cloud."

Key Takeaways

As people live more of their lives online, they're sharing more personal data than ever. In 2017, just one in five interactions between consumers and companies took place online. By 2020, that percentage had skyrocketed to more than half.[1]

Cybercrime is a lucrative business. Corporate login credentials of administrators sell for as much as $120,000 on the dark web, creating strong economic incentives for hackers to target high-value companies and individuals.[2]

The proliferation of data has been accompanied by a dramatic rise in attacks. Globally, the total number of data breaches more than tripled between 2013 and 2021.[3,4]

Even organizations with strong security practices are vulnerable to threats. More than 60% of the 1,000 largest companies in the US have experienced a public data breach, and it is estimated that, on an annual basis, one in four of those companies will experience a corporate breach.[5] Globally, in 2021, over half of organizations in every country surveyed suffered a ransomware attack.[6]

Existing security measures are not being adopted widely enough. While best-practice security measures would protect organizations against the vast majority of current attacks, they aren't being adopted quickly, broadly, or consistently enough to decrease the threats to consumer data.

We are only as safe as the least secure company that has access to any of our data. Hackers can use data stolen from companies with weak security to target employees and systems at other companies, including those with strong security protocols.[4,7]

Corporations should rethink the data they collect and reduce the amount of data they can access and the duration of data retention to only what is necessary to conduct business. By doing so, companies can reduce the risk to users even if a breach occurs.

Executive Summary

Imagine that you are starting a family and you want to stay on top of your finances so you can manage your budget for your growing family. Because you have too many accounts for banking, loans, subscriptions, and bills to keep track of, you decide to sign up for a service that aggregates all your accounts in one place. When **you register your account online, you follow the instructions carefully**. You create a strong, unique password and set up multifactor authentication. You enter your bank account and loan information, home address, and other personal information. Your spouse also signs up, and you create a joint family account that combines your information.

A month later, you're alarmed to read that **the company that manages this service has been hacked**. When you log in to your account, an alert notifies you that your private information was compromised in the attack. **Suddenly, something that was supposed to help secure your family's future has become a source of undue stress and potential harm**.

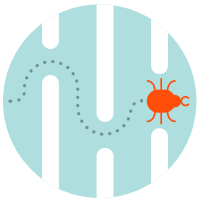
Unfortunately, scenarios like this are all too common. As people live more of their lives in the digital sphere, they are generating more — and more personal — data than ever before. From messages and photos to financial and health information, they are sharing and storing enormous amounts of private data online and in the cloud. **And that data represents an enticing target for malicious actors around the world**.

The Evolving Threat

Today, the threat posed by cybercriminals and hackers has never been greater. The theft and exploitation of consumer data is a booming business with low barriers to entry and potentially lucrative payouts for those involved. As a result, the proliferation of data has been accompanied in recent years by a dramatic rise in attacks across the globe. In the US alone, there were over 290 million victims of data breaches in 2021.[8]

There are steps that individuals can and should take to protect the security of their digital accounts, including the use of proper password hygiene and multifactor authentication. But as the scenario above demonstrates, the reality is that **a person can do everything right and their cloud data can still be just as vulnerable**. This is because consumer account security measures help protect individual accounts from being taken over but do not stop server-side data breaches. Unfortunately, malicious actors are not just directly targeting the people and accounts whose data they seek to exploit; increasingly, they are also **targeting the companies and servers that store those people's private data in bulk**.

The rise of corporate data breaches reflects a fundamental change in the digital landscape. In 2017, just one in five interactions between consumers and companies took place online. By 2020, that percentage had skyrocketed to more than half.[1] And while people clearly benefit from the ability to interact with businesses online, this rapid shift in behavior has **created even more opportunities for criminals to target consumers' personal data**.



A Vulnerable Ecosystem

The landscape has shifted in another important way as well. As hackers become more determined, they are also becoming more sophisticated. They are evolving their methods and finding more ways to defeat security practices that once held them back. Consequently, **even organizations with the strongest possible security practices are vulnerable to threats in a way that wasn't true just five years ago**.

For instance, **if hackers want to infiltrate a company with robust security practices, they might start by targeting a different organization with relatively weak security**. They can then steal credentials or information that helps them target employees or systems at the first company. This is precisely what has led to a breach at some organizations in recent years, including companies that cybersecurity experts herald for strong security and privacy protections.[4,9]

This is just one example of the tactics at play. But what it demonstrates is that **the data ecosystem has become so vast and interconnected that people are only as safe as the least secure company that interacts with any company that has access to their data**. That "least secure company" does not even need to have access to the consumer data.

To maximize user security, every organization that collects any consumer data would need to adopt much more stringent security protocols. Unfortunately, most still haven't, and **most of the organizations that are working on it are not moving nearly fast enough**.

This challenge isn't going away. In fact, it's only getting worse. More sensitive personal data is stored remotely over the internet (in "the cloud") every day, and hackers are working to find new ways to exploit it. We have reached a point where **not only are criminals becoming more innovative and dangerous, the data perimeter is also becoming more expansive and harder to defend**.

A More Secure Future

Given these dynamics, how should organizations respond? What can they do in a world where consumers can do everything right, businesses can implement best-in-class security practices, and yet data breaches remain a threat?

There is no silver-bullet solution, but there are clear steps that can greatly help.

First, **organizations must continue to develop new protections against evolving threats**. Measures like biometric authentication and passwordless sign-in have been incredibly valuable, and next generations of even more advanced security innovations will surely arrive in the future. It's not enough, however, for organizations to offer these measures to their users; they must also apply them rigorously to their own employees, especially those whose job responsibilities require any kind of privileged access to sensitive data or systems.

But while organizations continue to innovate against new threats, they must also face reality: **as long as organizations have troves of readily accessible consumer data, inventive hackers will aim to find ways to bypass security measures**. And hackers only need one successful attack to potentially trigger a catastrophic data breach.

This is why, in addition to fighting to limit the frequency of attacks, **organizations must act decisively to minimize the impact if a breach does occur**. That means interrupting a breach early and, more importantly, rethinking and reducing the amount of customer data they can access and retain in the first place. Organizations should collect data only when necessary, reduce the duration of data retention, and encrypt the data stored in the cloud. That way, even if hackers manage to access corporate networks, there will be less data they can exploit — and significantly less risk to users around the world.

By the Numbers

290 million

In 2021, in the US alone, there were over **290 million** victims of a data breach.[8]

1.1 billion

There were 5,212 confirmed breaches in 2021,[4] which exposed **1.1 billion** personal records across the globe.[10]

4 of 5

Four out of five Americans have had their private information exposed at least once.[11]

12 billion

The website "Have I Been Pwned?" reports that, as of October 2022, almost **12 billion** online customer accounts and their data have been compromised in data breaches.[12]

3

On average, an American's private information has been exposed in **at least three** breaches.[11]

+381%

The number of data breaches **more than tripled** between 2013 and 2021.[3,4]

+60%

Over **60%** of the 1,000 largest companies in the US have experienced a public data breach, and it is estimated that on an annual basis one in four of those companies will experience a corporate breach.[5]

4 of 5

Over **four out of five** surveyed organizations impacted by a data breach experienced multiple breaches.[13]

Over half

Data breaches occur around the world. In 2021, **over half** of organizations in every country surveyed suffered a ransomware attack.[6]

$120,000

Corporate login credentials of administrators can sell for as much as **$120,000** on the dark web.[2]

Contents

About the author

Dr. Stuart E. Madnick is the John Norris Maguire (1960) Professor of Information Technology, Emeritus, in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and the Founding Director of *Cybersecurity at MIT Sloan*: *the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity.* His involvement in cybersecurity research goes back to 1979 when he co-authored the book *Computer Security*, one of the first books on this subject.

Prof. Madnick holds a Ph.D. in Computer Science and has been a faculty member at MIT since 1972. He served as the head of MIT's Information Technologies Group for more than 25 years. In addition to cybersecurity, he has broad expertise in software engineering, database technology, software project management, and strategic use of information technology, as well as their applications to businesses and other large organizations as reflected in more than 400 books, papers, and other publications.

In addition to his research work in academia, he has extensive experience in the development of information systems for industry and has co-founded several high-tech firms.

Glossary

Corporate data breaches: unauthorized use or theft of business or consumer information from an organization's corporate network or systems (including any that the organization is running in a third-party cloud).

Encrypted data: data that has been transformed into a code to protect its contents. To decipher the code and access the data, users or organizations need a key (or a password) that makes the data "readable."

End-to-end encryption: a type of encryption that ensures only the sender and receiver of data can access and modify that data.

Fast ID Online (FIDO): a broadly supported authentication standard for passwordless sign-in that relies on public/private key pairs in place of passwords to log in to websites and apps across platforms.

Insider threats: malicious or unauthorized use of privileges by one or several of an organization's employees. For example, an employee misusing their login credentials to steal consumer information and sell it on the dark web.

Multifactor authentication: a requirement that a user successfully present two or more pieces of authentication to access a website or application. Entering a password followed by entering a code received in a text message or email is a common form of multifactor authentication.

Phishing: social engineering attacks in which a bad actor pretending to be part of a legitimate company, or someone the recipients know, sends a fraudulent message to a large number of recipients to trick them into revealing sensitive information.

Phone phishing (or vishing) attacks: social engineering attacks in which a bad actor uses a phone call or leaves a voice mail to trick someone into revealing sensitive information or paying money. When these attacks are delivered via text messages, as opposed to phone calls, they are referred to as smishing attacks.

Ransomware: bad actors taking control of an asset and demanding a ransom in exchange for the asset's return or to prevent its public exposure. For example, a bad actor encrypting sensitive confidential data such as private photos and messages and asking the victim for a ransom in order to decrypt the data.

Social engineering: bad actors relying on social interactions to manipulate people into divulging confidential information or stealing their money.

Spear phishing: phishing messages that are carefully crafted so that you believe that they are legitimate and are often accomplished by using detailed personal information that was previously stolen. For example, a message from a company's CEO to its CFO requesting the transfer of funds to an outside organization.

The Current Landscape of Consumer Data and Data Breaches

KEY TAKEAWAYS

- **As we create and share more personal data, the risk of data breaches is growing. In fact, the number of yearly reported data breaches more than tripled between 2013 and 2021.[3,4] In 2021, in the US alone, there were over 290 million victims of data breaches.[8]**
- **Data breaches occur across the world. In a 2021 survey, more than half of surveyed organizations in every country suffered a ransomware attack.[6]**
- **Victims of data breaches often suffer significant financial and emotional harm, and may eventually lose trust in organizations tasked with protecting their data. As of October 2022, almost 12 billion online customer accounts and their data have been compromised in data breaches.[12]**

As long as companies continue to collect an ever-expanding amount of information about their customers, those same companies will remain prime targets for cyber attacks.

Today, we are living more of our lives online than ever before. In recent years, digital technology has transformed how we communicate with our families and friends. It has fundamentally changed how many of us work. And, increasingly, it is reshaping how we engage with businesses as consumers. In 2020, more than half of all interactions between consumers and companies took place online, up from just one in five in 2017.[1]

This shift has fueled an explosion of consumer data across the globe. From photos and messages to location, health, and financial information, we now store vast amounts of consumer data in the cloud. At the same time, the rise of digital commerce means that we are providing more and more personal information to the businesses we interact with online – sometimes without our explicit permission or knowledge — that is often stored in corporate networks and systems. Many of these businesses believe "the more data the better," especially given the decreasing costs of data storage.[14] However, they neglect an important cost: the cost to the company and the impact on the consumers if that data is stolen.

In many cases, this data serves legitimate purposes, adding convenience and efficiency to the consumer experience. But it also creates an enormous amount of risk. Now, when someone orders food for delivery or hails a ride, they are not simply using a digital service: they are also providing their data to those companies.[15] While there are many benefits to these services, consumers, whether they realize it or not, are also trusting the company that provides the service to safeguard their private information, such as their location or address, phone number, email, payment and billing information, and transaction history. Indeed, they are also — almost always unknowingly — trusting every company that the service provider relies on in turn.

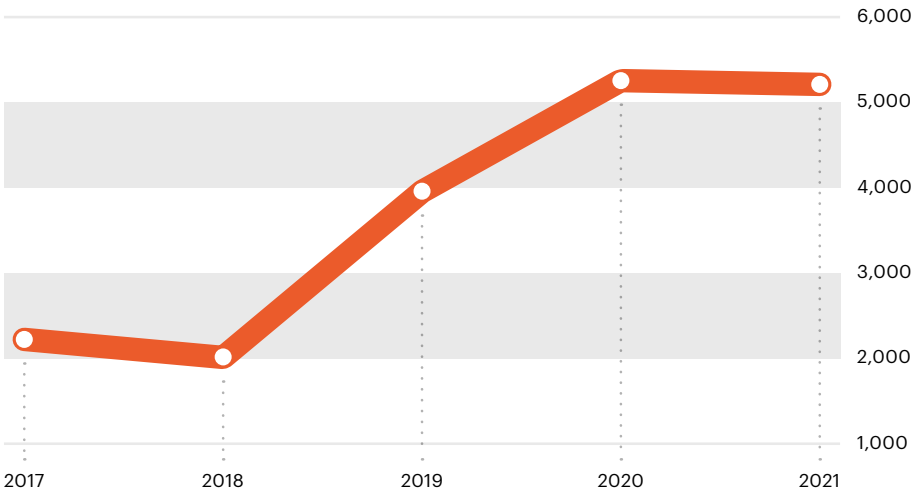
This is not an abstract concern. Every day, hackers are getting bolder and more creative. They are continually finding new ways to infiltrate corporate systems and steal valuable data. As long as companies continue to collect an ever-expanding amount of information about their customers, those same companies will remain

prime targets for cyber attacks. And this means that even consumers who take all the right precautions to protect themselves and their personal data in the cloud will, through no fault of their own, remain vulnerable to having their data stolen from third parties.

Many companies are working hard to protect themselves from breaches, implementing different strategies to help keep the data in their possession secure. But the rapidly growing amount of data collected and stored,[16] combined with the increasingly sophisticated tactics of hackers across the globe, can present an insurmountable challenge. The proliferation of consumer data on corporate systems has been accompanied by a dramatic rise in attacks: In the US alone, there were over 290 million victims of data breaches in 2021.[8] While companies implement different strategies to prevent these data breaches, bad actors constantly evolve their tactics and patterns to gain access to this valuable data.

The threat of corporate data breaches continues to grow with each passing year.

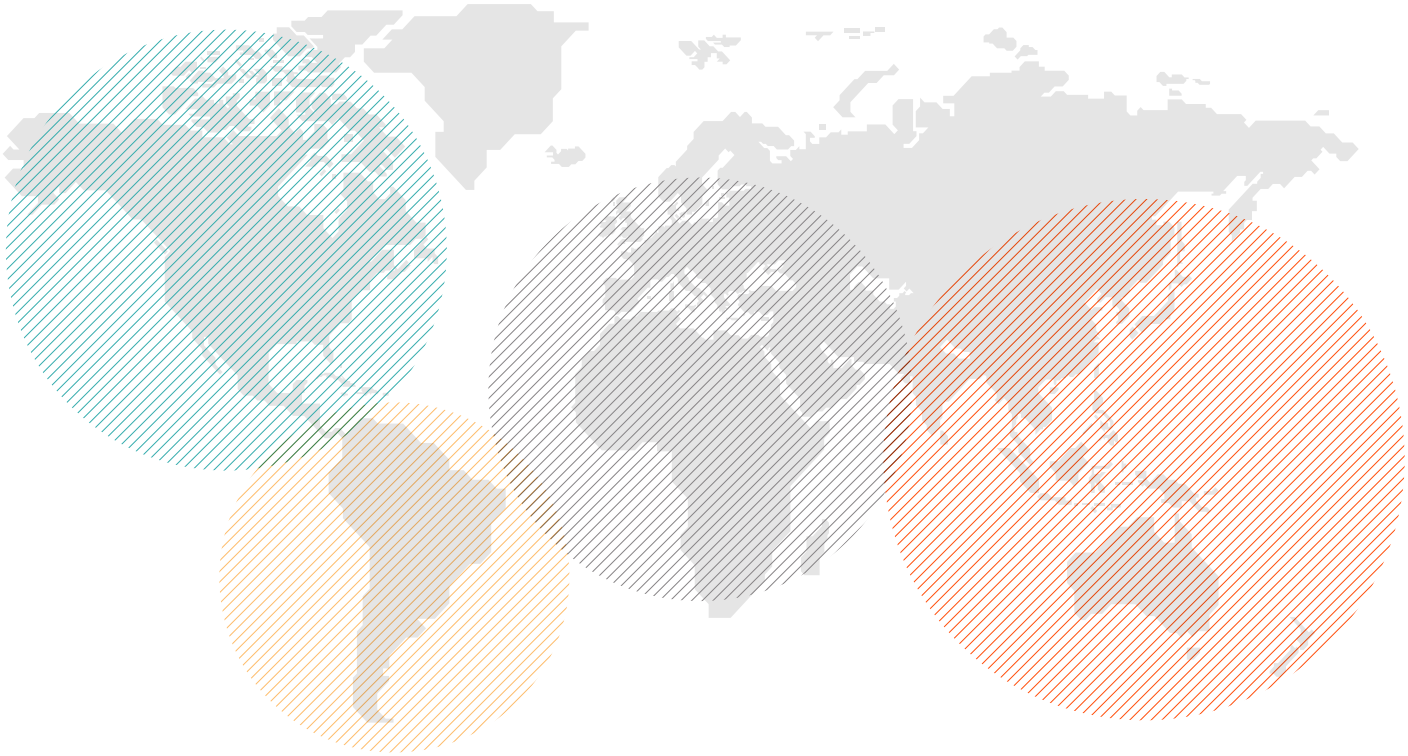
Reported Data Breaches Over Time[3,4,19]



NOTE:
The Number of Confirmed Data Breaches Analyzed by Verizon refers to the total number of confirmed data breaches included in the sample and analyzed by Verizon in its annual Data Breach Investigations Report. Verizon may cull the number of breaches analyzed based on its data quality standards. Further, the number of data breaches presented here represents a lower bound of actual breaches, and numbers are affected by reporting requirements, a lack of standardization in reporting, and other limitations of the analysis across regions and years.

The threat of corporate data breaches continues to grow with each passing year. In total, the number of data breaches reported annually more than tripled between 2013 and 2021, one study found.[3,4] While breaches at large companies garner the most public attention, this challenge affects organizations of every size. Research shows that hackers often find success targeting smaller companies, which may lack the resources or expertise to defend themselves. In 2020 and 2021, data breaches at small companies globally increased by 152% compared with 2018 and 2019. By comparison, breaches at large companies increased by 75% over the same period.[17,18]

Examples of Data Breaches by Region



Northern America

Yahoo! (US)
2013-2014
Collectively, **3 billion** user accounts[20,21]

Equifax (US)
2017
147 million records[25]

Desjardins (CA)
2017-2019
9.7 million individuals' records[29]

First American Financial (US)
2019
Over **885 million** sensitive documents[33]

Capital One (US)
2019
Over **100 million** customers[37]

Latin America and the Caribbean

Massive Data Leak in Brazil (BR)
2021
Over **220 million** citizens' records[22]

Registro Nacional de las Personas (AR)
2021
Up to **45 million** citizens[26]

Government of Costa Rica (CR)
2022
670 gigabytes of sensitive data[30]

Instituto Agrario Dominicano (DR)
2022
Over **1 terabyte** of government data allegedly stolen[34]

Europe, Middle East and Africa

Dailymotion (FR)
2016
85 million user accounts[23]

Ticketmaster (EU)
2018
9.4 million customers[27]

Careem (AE)
2018
14.6 million customer records[31]

Pegasus Airlines (TR)
2022
Almost **23 million** flight data files[35]

TransUnion (ZA)
2022
54 million customer records[38]

Asia Pacific

Tianya Club (CN)
2011
40 million user records[24]

Cathay Pacific (HK)
2014-2015
9.4 million customer records[28]

Aadhaar (IN)
2018
Up to **1.1 billion** citizens' records[32]

SingHealth (SG)
2018
1.5 million patient records[36]

Optus (AU)
2022
9.8 million customer records[39]

Developments in Consumer-Level Authentication Over Time

Enhancing Security to Protect Users

Many of the techniques hackers use to gain unauthorized access to consumer data could have been prevented by organizations deploying well-understood security practices. Today, most attacks rely on techniques that could be prevented by organizations consistently using widely available security mechanisms for their employees and contractors. These mechanisms include multifactor authentication, ensuring that passwords are complex, having a reasonable anti-malware posture, minimizing who has access to confidential data and large data stores, and keeping corporate systems up-to-date with operating system patches.[40] Similarly, the circumstances that make the vast majority of ransomware attacks possible can be traced to common errors in the configuration of corporate software and devices.[41]

Individual consumer security decisions, such as the use of two-factor authentication for a given service app or account, generally cannot prevent data from being stolen in the case of a bulk data breach of the company providing the service. Nonetheless, having consumers employ solid security practices within their control is a crucial first step in making it harder for bad actors to steal personal information. This is why technology companies continue to develop innovations to protect users from direct threats such as **social engineering** attacks and **ransomware** targeting individuals. The purpose of these innovations is to make it easier for consumers to safeguard their data, as well as to make it harder for bad actors to steal it.

- **Biometric authentication.** Biometric authenticators such as face, voice, and fingerprint identification make it easy for users to unlock their devices without the need to constantly enter their passcode, and they have been adopted by many users as a form of device authentication.[42]
- **Passwordless sign-in.** Based on the Web Authentication standard, passwordless sign-ins have broad industry support to replace passwords for websites and apps.[43] Passwordless sign-ins allow consumers to use the same technology used to unlock smartphones (PINs, fingerprints, Face ID) to access their accounts on webs and apps. They are faster for sign-in, easier to use, and much more secure than traditional passwords, eliminating entire categories of security problems such as weak and reused passwords, credential leaks, and **phishing schemes** to elicit such credentials.[44]
- **Dedicated security chips.** Technology companies have also introduced on-device hardware that allows for storing, encrypting, and processing private and sensitive data such as biometric templates on users' devices without it reaching an organization's systems, where it could be at risk of getting hacked. These chips make the sign-in process more efficient and security more effective.[45,46,47]

The Prevalence of Data Breaches

4 of 5

Over **four out of five** surveyed organizations impacted by a data breach experienced multiple breaches.[13]

290 million

In the US alone, there were over **290 million** victims of data breaches in 2021.[8]

12 billion

As of October 2022, almost **12 billion** online customer accounts and their data have been compromised in data breaches.[12]

>3x

The number of yearly reported data breaches **more than tripled** between 2013 and 2021.[3,4]

While the threat to businesses is nearly universal, the motivations and objectives of those responsible for these attacks vary widely. In some cases, hackers act on behalf of a specific country and target governments, organizations, or individuals to advance that country's interests. These "state-sponsored" attacks, as they are commonly known, often disrupt key services, compromise critical infrastructure, or provide the governments behind the attacks with access to intelligence. Some hackers also perpetrate attacks with the goal of advancing specific political interests or gaining visibility for a socially motivated cause. Most frequently though, cyber-criminals respond to economic incentives. They target lucrative data that can be easily monetized, and they continually evolve their tactics to maximize their potential for financial gain.[4]

For example, until recently, payment information (such as credit card numbers) and Social Security numbers were some of the most frequently targeted data in cyber attacks. An individual Social Security number would typically sell for $60-80 on the black market, making it a valuable commodity for hackers looking to make a quick profit.[48] But in recent years, the increase in large data breaches has made such information widely available, and the market value of a Social Security number has plummeted to just $2-4.[49] In response, economically motivated hackers have shifted their focus to other types of sensitive data, including authentication credentials.[4] As companies accumulate vast amounts of consumer data, corporate login credentials have also become highly coveted targets. In fact, the corporate login credentials of administrators can sell for as much as $120,000 on the dark web.[2]

Regardless of what motivates the attackers, the consequences of corporate data breaches are far-reaching. In 2021 and 2022, companies spent, on average, over $4 million to remedy a breach.[13] The actual cost varies from case to case, and, in some instances, has exceeded $1 billion.[50] Meanwhile, it is customers who often experience the most significant consequences. This is because the overwhelming majority of breaches involve sensitive personal information.[8] One study found that 99% of data breaches exposed users' names and addresses, over half exposed Social Security numbers and dates of birth, and over one-third contained health information.[7] These trends are likely to persist, if not worsen, as bad actors set their sights on companies that retain particularly sensitive data. In 2021, the most frequent targets of data breaches were health organizations, followed by financial organizations.[7,51]

It is crucial to recognize that the exposure of consumers' sensitive private data does not just violate their privacy, but can also cause them real financial and emotional harm. It exposes innocent people to identity theft and fraud, which often hurts their credit scores, interferes with their ability to secure a mortgage or business loan, and can take years to resolve. It also makes the victims more vulnerable to further attacks, as cyber-criminals may use their personal information to target them in future schemes. For example, hackers have targeted prospective home buyers, using data stolen from law offices or title companies regarding upcoming house purchases to impersonate employees from title agencies and convince them to wire thousands or hundreds of thousands of dollars directly into the hacker's bank account.[52] Ultimately, data breaches cause many consumers to lose trust in the institutions tasked with protecting their private information, fueling the loss of public trust across society.

Corporate Data Breaches, and How They Threaten Consumer Data

KEY TAKEAWAYS

- **Corporate data breaches in one organization often propagate to other organizations.**
- **Hackers can execute targeted attacks on users by combining and exploiting leaked data from previous breaches.**
- **Consumers are only as safe as the least secure company that has access to their data. Hackers often target vulnerable organizations, and use data stolen from those companies to target employees and systems at companies with strong security protocols.**
- **Once a company's security measures are exposed, it is likely to become the target of future attacks. According to a survey, over four out of five organizations impacted by a data breach experienced multiple breaches.[13]**

Hackers can target organizations with weaker security systems, and then use that data to orchestrate sophisticated attacks at companies with strong protocols.

Corporations have spent years fortifying their security, and they're constantly developing new ways to prevent data breaches. The problem is that hackers are evolving their tactics right alongside them. The result is an ever-escalating arms race in which each side works constantly to defeat the other's latest technique. This is why, even if consumers take all the appropriate steps to protect their data, their data is still at risk.

For example, when businesses created multifactor authentication, it offered powerful protection against compromised passwords. But now, hackers are increasingly finding ways around it for more targeted, high-value attacks. For example, they are using advanced social engineering to briefly take over a target's cellular account, steal their authentication codes, and then compromise their accounts.

As discussed, hackers often use the consumer data they steal for crimes like identity theft and financial fraud. But, in yet another evolving tactic, they also use it to launch additional attacks. Hackers can target organizations with weaker security systems, and then use the stolen credentials or data to orchestrate sophisticated attacks on companies with strong protocols.[4,9]

In these attacks, hackers take data stolen in a breach, then use it to launch detailed and highly targeted social engineering attacks against employees of another company. Even the most careful people can fall victim to these targeted social engineering attacks, because the malicious actors know so much about the victims and appear legitimate.

Ultimately, this means that even companies that have implemented best security practices are potentially vulnerable to data breaches.

And unfortunately, once a company's security measures are circumvented, they are likely to be circumvented again. According to a survey, over four out of five surveyed organizations impacted by a data breach experienced multiple breaches.[13]

Bad actors use different attack methods to try to gain unauthorized access to corporate networks, such as social engineering attacks, insider threats, and supply chain attacks, with the goal of stealing data, disrupting business, or both. We illustrate these methods next, together with a common consequence of these data breaches: ransomware.

Secondary Breaches of Other Twilio Customers

In addition to Signal and DoorDash, other customers of Twilio that were publicly reported to be secondary victims of this breach include **Authy**, a two-factor authentication app, and **Okta**, an authentication firm.[57] In total, over 200 Twilio customer organizations were impacted.[53]

Twilio

Who was targeted?

Twilio provides companies such as Signal and DoorDash with phone number verification services. Bad actors gained access to Twilio's customer support systems by stealing login credentials of Twilio employees through an advanced phishing attack. Twilio employees received text messages claiming to be from Twilio's IT department, linking them to a website that resembled Twilio's sign-in page but was controlled by the bad actors. By breaking into Twilio's systems, bad actors managed to breach other organizations that were customers of Twilio. In other words, **the initial breach at Twilio facilitated secondary attacks on user data at additional organizations.**

How were other organizations impacted?

While these bad actors were in Twilio's customer support systems, they had the ability to view and re-register phone numbers on **Signal**, which is a Twilio customer.[9,53] Signal is a popular instant messaging service, and it is favored by many cybersecurity experts, journalists, and government officials.[54] Signal's security measures include end-to-end encryption of messages, which allows only the sender and receivers to decrypt and read messages, and the public posting of its source code so experts can verify and test Signal's security.[54] Despite being unable to defeat Signal's encryption, bad actors could use their access to Twilio to bypass Signal's phone number verification. Bad actors managed to breach other Twilio customers such as **DoorDash**, a food delivery service, by stealing the credentials of Twilio employees who had third-party access to DoorDash.[55]

How were consumers impacted?

Bad actors could not gain access to message history or contacts of Signal's users because they were end-to-end encrypted, but they had the ability to take over the Signal account registration for 1,900 users, which would have allowed them to send and receive Signal messages from the phone numbers belonging to those users.[9] They specifically targeted three users, including a reporter who covers cybersecurity, and they were able to re-register his number.[9,56] Additionally, bad actors accessed the names, delivery addresses, phone numbers, and some partial payment card information of DoorDash customers.[55]

Examples of Corporate Data Breaches

Equifax (US, Britain, Canada)

One of the largest known data breaches took place in 2017, when credit reporting company **Equifax** was breached and the personal data of over 150 million Americans, Britons, and Canadians was compromised.[58,59,60] Researchers identified 19 systemic failures as the causes of the breach, including lack of encryption of much of the compromised data.[61] Had this data been encrypted, it would have been much harder for hackers to access.[62]

Capital One (US, Canada)

In 2019, a former engineer for **Capital One**'s cloud provider hacked Capital One and downloaded data for over 100 million customers, including 140,000 Social Security numbers and 80,000 bank account numbers.[63,64] Analysis of the breach revealed that failures of the company's internal controls coupled with a lack of effective enforcement by security regulators made it easier for bad actors to gain access to this data.[37]

Ashley Madison (Global)

In 2015, **Ashley Madison**, an affair dating site, was hacked and 32 million records were leaked. Victims of the leak were targeted through personalized extortion scams for years after the leak.[65]

SingHealth (Singapore)

In 2018, **SingHealth**, Singapore's biggest network of healthcare facilities, was breached, compromising the personal data of 1.5 million patients, including the prime minister. Bad actors accessed outpatient medical information including prescription records for more than 160,000 patients.[66,67]

US Office of Personnel Management (OPM) (US)

Between 2013 and 2015, **OPM** was breached twice by bad actors. In the first breach, a hacker accessed OPM's network and stole manuals that provided a roadmap of OPM's IT environment. This was followed by a second, similar breach that went unnoticed for a year. Background investigation records of current, former, and prospective federal employees and contractors, including personal data and findings from interviews, were stolen in the attacks.[68,69]

Corporate Social Engineering Attacks

KEY TAKEAWAYS

- **Social engineering attacks are some of the most common threats facing organizations.**
- **In these attacks, hackers often trick employees into giving away their corporate credentials so the attackers can masquerade as legitimate employees.**
- **These attacks often target specific employees who have access to sensitive data. And once bad actors masquerade as employees, they can often access sensitive consumer data that is stored in readable form on corporate networks and systems.**
- **Social engineering attacks are growing in sophistication, and even the most careful employees can fall victim to them.**

In many data breaches, bad actors attack by manipulating corporations' employees. They've become very skilled at tricking these people into neglecting best security practices or giving away sensitive information. Once that's happened, hackers use what they've learned to gain access to the organization's systems, networks, or physical locations.

These attacks, commonly referred to as social engineering attacks, are some of the most common and pernicious threats that companies and users face every day.[4]

They can also take different forms depending on their intended target. In some cases, hackers are mainly interested in stealing sensitive data like payment information. They may also attempt to trick users into sending them money directly. In these instances, they target a large, random set of consumers — often with disconcerting effectiveness.

Examples of Broad-Based, Consumer-Focused Social Engineering Attacks

"Hi Mum" scam (Australia). In 2022, scammers sent messages posing as a family member or friend. The messages claimed that the family member or friend had lost or damaged their phone and needed certain personal information or money urgently. Over a thousand Australians fell victim to the scam in the first seven months, with total reported losses of $2.6 million.[70]

Zelle scam (US). Scammers impersonated bank employees to trick users of Zelle, a money transfer app, into sending them money. Using personal information likely obtained from a data breach, scammers tricked users into thinking their calls and texts originated from legitimate bank employees.[71,72]

In other cases, malicious actors directly target specific corporations and their employees. They employ sophisticated tactics like using leaked information from previous data breaches to convince employees to give up their corporate credentials, then masquerade as legitimate employees to gain access to the organization's network, systems, and sensitive consumer data stored on corporate networks.

This is precisely what happened twice to the email marketing service MailChimp in 2022.[73,74] Hackers used phishing attacks to obtain employee credentials, then used what they stole to target multiple organizations that used MailChimp's services.[73] For instance, they stole names, emails, and IP addresses from customers at Trezor, a cryptocurrency hardware wallet company. The hackers then used this information to trick Trezor customers into downloading a cloned version of Trezor, thereby giving hackers full access to their funds.[73,75]

Other Corporate Social Engineering Attacks

Anthem (US): In 2014, bad actors gained access to the corporate system of Anthem, one of the largest health insurance companies in the US at the time, through spear phishing emails sent to employees of an Anthem subsidiary. As a result of the scheme, bad actors exfiltrated 78.8 million unique user records — including names, medical IDs, and employment and income data.[79,80]

Twitter

Who was targeted?

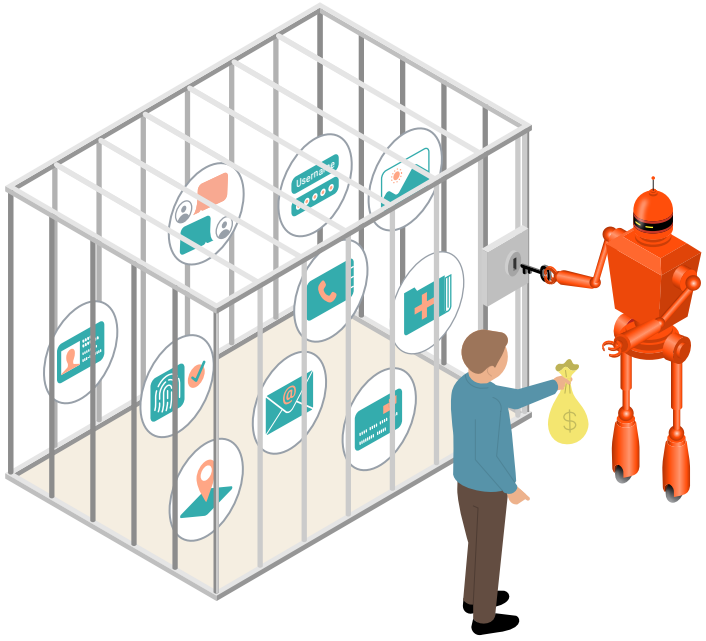
In 2020, hackers gained access to Twitter's internal account management tools. This allowed them to access several Twitter accounts, including those of an elected official, other high-profile Twitter users, and multiple cryptocurrency companies. The hackers were also able to view and download data stored on Twitter's platform, such as direct messages (DMs), photos, and videos.[76,77]

How did the breach occur?

Hackers masquerading as employees who worked at Twitter's IT department contacted legitimate Twitter employees over the phone. Once in contact, the hackers tricked them into granting access to Twitter accounts.[76,77] Some of those employees had authorized access to the platform's internal user-support tools, making the breach even more serious. These kinds of attacks are commonly referred to as phone spear phishing (or vishing) attacks.

How were consumers impacted?

After gaining access, the hackers tweeted from high-profile accounts, and asked those followers to send Bitcoin to a specific cryptocurrency wallet. The scammers promised that their money would be doubled and returned to them. Bitcoin worth more than $118,000 was collected from over 300 transactions within three hours of the tweets being posted.[78] In an attempt to contain the attack, Twitter disabled verified accounts as well as accounts that had recently initiated a password reset. This action had its own negative impacts. For instance, it prevented the National Weather Service from issuing warnings on Twitter about a tornado in Illinois because its verified account was disabled.[78]



Corporate Ransomware

KEY TAKEAWAYS

- **Corporate ransomware has become more common, and bad actors with little to no technical expertise can lease and deploy ransomware against an organization (Ransomware-as-a-Service).**
- **As healthcare organizations have some of the most sensitive consumer data, the number of ransomware attacks against these organizations almost doubled between 2020 and 2021.[81]**
- **Despite improvements in cybersecurity technology and increased insurance coverage against corporate ransomware attacks, end-users, through no fault of their own, often suffer the consequences of ransomware attacks, with their data being stolen, lost, and leaked.**

In corporate ransomware attacks, bad actors take control of corporate assets and demand ransoms in exchange for the assets' return, or to prevent their public exposure. While bad actors can also use ransomware attacks to target regular people directly by encrypting the files on their computer or locking them out of their phones and demanding payments, the focus in this report is on ransomware affecting corporate data.[82]

While corporate ransomware attacks once largely centered on crippling a company's system, hackers are starting to shift their focus toward corporate data.[83] In fact, in 2021, over 60% of corporate ransomware attacks involved stolen data.[84]

Because of this shift, these attacks can now be especially devastating for both consumers and companies. It also means that companies with particularly sensitive consumer data are increasingly the target. Between 2020 and 2021, for instance, ransomware attacks against healthcare organizations nearly doubled.[81]

And hacking groups like Lapsus$ are now targeting telecommunications companies, government entities, and education and healthcare organizations, stealing their data and threatening to release or destroy it if a ransom is not paid.[85,86]

Ransomware attacks are particularly dangerous for two reasons. First, there is no guarantee that the perpetrator will decrypt (or return) the data, or even destroy the stolen copy of the data once the ransom is paid. In fact, even when companies pay the ransom, one-third of the data stolen (on average) is never recovered.[87] Second, as the FBI warns, paying the ransom can encourage the perpetrator to target more victims and incentivizes further attacks.[88]

While organizations often have insurance against the rising threat of ransomware, consumers, through no fault of their own, see more of their data stolen and leaked.

And ransomware attacks haven't just become more common;[89] their complexity has also increased. In 2020 and 2021, ENISA (the European Union Agency for Cybersecurity) described ransomware as the prime cybersecurity threat.[90] One key driver of the growth in ransomware attacks is the rise of **Ransomware-as-a-Service** (RaaS), the sale or lease of malware by technical hackers to hackers with little to no technical expertise.[90,91] With RaaS, the developers of the ransomware software lease it to other criminals in exchange for a fee, often providing customer support to make it easy to use. RaaS has lowered the entry-level barrier to conducting ransomware attacks, and with growing competition among ransomware developers, RaaS is being sold to buyers at a discount. Almost anyone can now be an attacker, to the point that RaaS accounts for two-thirds of all ransomware attacks.[90] Additionally, a conservative estimate of the profitability of ransomware attacks indicate that the ROI of this activity could be upwards of 500%.[92]

As ransomware attacks have become more commonplace, organizations are increasingly obtaining cyber insurance coverage to protect themselves from the financial risk arising from these attacks. Indeed, a recent survey estimated that 83% of organizations have some form of cyber insurance.[93] However, cyber insurance coverage does not prevent attacks from taking place, nor does it stop consumer data from being leaked into the public. Despite investments in cybersecurity technology and cyber-insurance coverage, there has been an almost threefold increase in the share of organizations paying ransoms of $1 million or more (up from 4% in 2020 to 11% in 2021).[6] Thus, while organizations often have insurance against the rising threat of ransomware, consumers, through no fault of their own, see more of their data stolen and leaked.

Examples of the Harm of Corporate Ransomware

Corporate Ransomware Attacks Usually Target Sensitive Consumer Information

Vastaamo (Finland), the largest network of private mental-health providers in Finland at the time, received a ransomware demand in October 2020 after records of tens of thousands of patients were stolen. Hackers demanded a ransom from patients to avoid the exposure of their highly sensitive data.[94,95]

Optus (Australia), Australia's second-largest telecommunications company, suffered a ransomware attack in September 2022. Bad actors gained access to the records of up to 10 million customers (40% of Australians), including home addresses, driver's licenses, and passport numbers, and threatened to release 10,000 records a day until the ransom was paid.[96,97] Following the attack, Australian regulators vowed to amend privacy legislation, forcing companies to notify banks about customers affected in any data breach to minimize fraud.[98]

Professional Finance Company (US), a small debt collection firm that serves hundreds of hospitals and medical facilities across the US, was hit by a ransomware attack in February 2022. As a result, more than 650 healthcare providers were affected by the data breach, one of the biggest healthcare breaches in 2022. The bad actors stole patient names, information relating to patient accounts, and, in some cases, health insurance and medical treatment information.[99]

Corporate Ransomware Attacks Are Often Centered Around High-Profile Targets

In 2020, the entertainment law firm **Grubman Shire Meiselas & Sacks (US)** was attacked. Hackers demanded a payment of $42 million while threatening to leak confidential documents about the firm's celebrity clients.[100]

In 2021, **Graff (UK)**, a luxury British jeweler, suffered a ransomware attack. Hackers threatened to release the records of its high-profile customers unless a $15 million ransom was paid.[101]

Corporate Ransomware Attacks Can Result in Institutional Breakdowns

In 2022, a ransomware gang attacked the **Government of Costa Rica** and threatened to leak government data unless a ransom was paid. The government refused, which led hackers to cripple its systems, forcing a state of emergency.[102]

The ransomware attack on the Government of Costa Rica is not the first to target critical government infrastructures. In the **US**, cities such as **Atlanta** and **Baltimore** have also been targets of ransomware attacks. In 2018, a ransomware attack targeting the City of Atlanta impacted more than one-third of the software used by the city, and affected critical services, including the police and court systems.[103] The City of Baltimore suffered a cyber attack in 2018 that affected the emergency dispatch system, and in 2019 bad actors gained control of 10,000 government computers, taking down essential websites used by citizens to pay water bills, property taxes, and parking tickets for over two weeks.[104,105]

Corporate Ransomware Attacks Can Impact the Most Vulnerable People

In 2022, the **Chicago Public Schools** system suffered a massive data breach that exposed the private data of nearly 500,000 students and 60,000 employees after one of the school system's vendors suffered a ransomware attack the previous year. In addition to students' names, dates of birth and other personal identifying information, hackers also stole school records, information on courses taken, and test scores going back many years.[106]

In 2022, the **Los Angeles Unified School District (LAUSD)** was attacked by a hacker group that disrupted the LAUSD's access to email and other IT services through a ransomware attack. The hacker group, Vice Society, is known for targeting schools and the education sector. Vice Society set a deadline for the ransom demand, and, after the LAUSD refused to pay, posted the data containing personal identifying information, including passport details, contracts, and other legal documents, to the dark web.[107]

Insider Threats

KEY TAKEAWAYS

- **Insider threats are those that arise from within an organization. Sometimes they occur when employees accidentally misplace confidential information with no malicious intent. In other instances, employees deliberately misuse their access to confidential data for personal reward.**
- **While insider threats are less common than attacks by external actors, the frequency of insider attacks doubled between 2016 and 2022.[108] On average, the number of records leaked by insiders is also higher than the number of records leaked by external actors.[4]**
- **A recent survey found that the two out of three cybersecurity professionals consider their organization vulnerable to an insider threat.[109]**
- **Whether corporate insider threats are caused by malicious intent or not, consumers and their sensitive data still suffer from these attacks.**

External threats are not the only threats to consumer data stored by organizations — sometimes the threat comes from inside the organization. Insider threats sometimes involve employees without malicious intent who accidentally misplace confidential files. In other cases, insiders use their corporate access to consumer data for their own personal gain.

Insider threats can also pose a direct risk to consumers. For instance, external bad actors can pay phone companies' employees to assist with SIM card swaps, thereby switching the victim's mobile number to the hacker's device. This gives the hacker control over a user's phone number, which they can use to bypass two-factor authentication and access their accounts.[110,111]

Insider threats also risk exposing or accessing corporate consumer data. In these attacks, employees assist malicious actors in gaining access to a corporate network. Bad actors are now targeting entry-level employees, offering monetary rewards in exchange for access to corporate networks and data.

The hacking group Lapsus$, for example, recruits insiders by posting on public forums like Telegram and Reddit. They offer rewards for credentials and multifactor

authentication approval, then use them to steal data they either leak publicly or use to extort victims.[85,86] In other cases, employees themselves misuse their privileged access to improperly obtain or mishandle consumer data.[112] In both cases, insider threats can affect consumers directly through subsequent attacks, identify theft, or fraud.

Even though insider threats account for only around 20% of data breaches, they have become more common, and their consequences are often worse.[4,108] The frequency of insider attacks doubled between 2016 and 2022,[108] and, on average, the size of a data breach (as measured by the number of leaked records) is larger in the event of an insider threat.[4] In 70% of these cases, personal information is compromised.[4]

The main motivation for insiders is often financial reward. But even in cases in which insiders do not leak a vast amount of personal information, they can use their privileged access to obtain information on specific third parties, either for political (e.g., an enemy of the state) or personal (e.g., an ex-partner) reasons.[4]

Security professionals are particularly concerned with insider threats. A 2021 survey found that two out of three cybersecurity professionals consider their organizations moderately to extremely vulnerable to insider attacks, and over half of organizations do not have programs in place to prevent insider threats.[109]

Examples of Insider Threats

Desjardins (Canada): Between 2017 and 2019, an employee at Desjardins, one of the largest financial institutions in Canada, exfiltrated the personal information of more than 9 million customers, including their social insurance numbers.[29]

Twitter (US): In August 2022, a former Twitter employee was found guilty of abusing internal system privileges in 2015 to spy on behalf of the Saudi Arabian government on allegedly more than 6,000 accounts of dissidents and political detractors.[113,114] Furthermore, according to company whistleblowers, the Indian government also reportedly forced Twitter to put an agent on payroll, providing the agent with access to sensitive user data.[113,114,115]

Uber

Who was targeted?

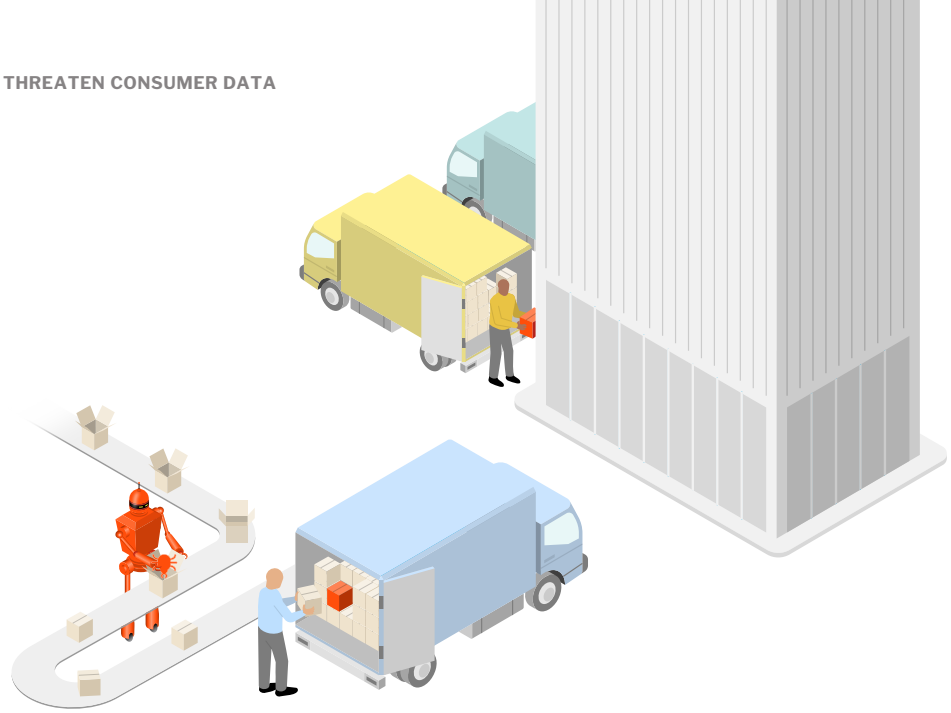
Some employees of Uber, a digital ride-hailing platform, repeatedly misused their privileges to spy on journalists, celebrities, and ex-partners. Uber employees were able to regularly access a tool called "God View," which allowed them to see the real-time movements of Uber users.[116]

How were consumers impacted?

Some Uber employees misused the tool to spy on the movements of ex-partners, while others allegedly used the tool to spy on celebrities, including Beyoncé.[116] During the launch party of Uber Chicago, the real-time movements of well-known users including venture capitalist Peter Sims were broadcast on a large screen for all party attendees to see.[117] Additionally, a New York executive used the tool to track the movements of a BuzzFeed News journalist who covers the ride share industry. When the journalist arrived at Uber's headquarters for an interview, the executive told her, "I was tracking you."[118] The executive had previously emailed the same journalist records of Uber rides, which he obtained without her permission.[118]

Consequences of the data breach

Uber has since settled a federal probe with the Federal Trade Commission (FTC) requiring it to improve its privacy protections and submit to 20 years of outside monitoring.[119] The FTC probe was in response to a previous data breach at Uber in 2014 in which bad actors used access IDs posted by an Uber engineer on GitHub to access Uber's network. Another Uber breach occurred in 2022, likely after a bad actor stole an employee's credentials through social engineering.[120]



Software and Supply Chain Vulnerabilities

KEY TAKEAWAYS

- **Supply chain attacks occur when hackers target vendors or suppliers that have access to an organization's corporate network, code, software, or hardware. These attacks more than tripled between 2020 and 2021.**[7]
- **Supply chain attacks allow bad actors to bypass the target organization's security by targeting vendors, suppliers, and widely used software that often have weaker security protocols.**
- **Due to the nature of supply chain attacks, even organizations with strong security are at risk of being breached, allowing bad actors to gain access to consumer data.**

In some cases, bad actors do not target an organization directly, but instead work to access its systems through vulnerabilities. In these attacks, often referred to as **supply chain attacks** or side-door attacks, hackers do not try to get in through the protected "front door" of these secure companies but rather via the special relationships that suppliers, especially small ones with weaker security, have with these larger companies. For instance, hackers may:

1. Exploit the supplier's need and ability to access the large company's network. For instance, bad actors could exploit an outside supplier's credentials and access the large company's network.
2. Exploit the auto-update feature of software that is installed in the larger company's network. By compromising the software supplier, malware can be transferred along with the software update.
3. Exploit malware or vulnerabilities that exist in software coming from third-party suppliers, including open-source software. By leveraging accidental vulnerabilities in third-party software, bad actors could gain access to corporate networks and, for instance, deploy malware.

Supply chain attacks have become increasingly common: nowadays, almost every organization relies on software created or managed by third parties, and any software is susceptible to vulnerabilities, or flaws in the code that can be exploited by hackers. For example, if a company offers cloud software — such as some service on the web, app, or the increasingly common everyday products connected to the internet — this company's software is at risk of hackers finding a vulnerability in its code, or in the software the company relies on. Between 2020 and 2021, the number of data breaches caused by supply chain attacks more than tripled.[7]

Supply chain attacks provide a pathway for hackers to bypass the target organization's security, no matter how strong it might be.

These attacks are particularly problematic because vendors or suppliers often have access to an organization's corporate network, code, software, or hardware. And when they have weaker security protocols than the main organization, they provide a pathway for hackers to bypass the target organization's security, no matter how strong it might be.

For instance, a famous example of supply chain attacks involves SolarWinds, a software firm that provides IT monitoring to thousands of companies. When hackers breached SolarWinds in 2019, they implanted malicious code into its software, and when customer organizations of SolarWinds downloaded this software, the hackers gained access to systems at as many as 18,000 organizations, including Microsoft, Intel, and government departments.[121,122] Hackers gained access to emails at the Departments of Homeland Security, State, Commerce, and the Treasury, and some of those emails went missing for good.[122]

This is just one example. In 2021, almost one-quarter of all data breaches were related to security issues with third-party suppliers.[7] These attacks are difficult to prevent, because even when organizations specify security requirements in their vendor contracts, they are often hard to monitor and enforce.[123] These attacks also aren't slowing down. According to a recent survey, in the second half of 2021, supply chain attacks increased by over 50% compared to the prior six months.[123]

Supply chain attacks show that even organizations that take all the right steps to protect themselves, and any consumer data they collect, are still at risk. As the SolarWinds attack demonstrated, even a cybersecurity company like FireEye, with strong security practices, can be infected with malware in a supply chain attack.[122] Today, virtually all major organizations rely on a series of third-party vendors, software, and suppliers. It is simply not possible for them to constantly vet and monitor the security requirements of each and every vendor or third-party software they rely on — and that ultimately means that, as long as companies store large amounts of readable consumer data, this data will be at risk, no matter how secure any organization may purport to be.

Examples of Supply Chain Attacks

SolarWinds (US), a software firm that provides IT monitoring to other companies, was hacked in September 2019. This is another type of supply chain attack where hackers target software used internally by many other companies. Bad actors gained access to SolarWinds networks, and, through those, were able to access many of the organizations that relied on SolarWinds software, including the Departments of Homeland Security, State, Commerce, and the Treasury; Microsoft; Intel; Cisco; and Deloitte.[122]

Dragonfly is an organization of bad actors known for employing supply chain attacks. Dragonfly first targets third-party companies with lower network security in order to gain access to government entities in the energy, aviation, nuclear, and critical manufacturing sectors.[132]

log4j

Who was targeted?

log4j is code used by hundreds of millions of computers online that run online services.[124,125] Companies such as Google, Apple, Amazon, Microsoft, and IBM rely on log4j, as do consumer devices that connect to the internet such as smart TVs, medical devices, and security cameras. In late 2021, a vulnerability was discovered in log4j that allowed bad actors to take control of any server running log4j and steal data or plant malicious software. Millions of attacks followed this discovery, and a large number of devices and applications were affected.[124,126,127]

How were consumers impacted?

This vulnerability puts consumer data at risk. For instance, ONUS, one of the largest Vietnamese crypto trading platforms, suffered an attack in which bad actors exploited the log4j vulnerability to steal the data of 2 million customers, and later threatened to release it if a $5 million ransom was not paid. After ONUS refused to pay, the bad actors sold the data on the dark web, which included customers' personal information, hashed passwords, ID cards, passports, and videos.[128] Hacking groups have also leveraged the log4j vulnerability to release ransomware such as "Night Sky," which is used to demand payment in return for decrypting hijacked systems and withholding the release of stolen data.[129] The log4j vulnerability also poses a risk to end-consumers directly. For instance, players running an impacted version of Minecraft could have had their computers compromised.[130]

Does the risk to consumers remain?

Likely yes. Fixing the log4j vulnerability requires each organization to update this specific piece of software quickly. Considering how widely it is adopted, quick fixes are likely not feasible for many companies, and the vulnerability likely remains an issue with some software today.[124] The Cyber Safety Review Board, which was tasked by the US government with reviewing the log4j vulnerability and providing recommendations, concluded that, as of July 2022, despite organizations spending significant resources to address the issue, "the Log4j event is not over. Log4j remains deeply embedded in systems, and [...] community stakeholders have identified new compromises, new threat actors, and new learnings."[131]

Keeping Consumers Safe: Rethinking the Corporate Approach to Consumer Data

KEY TAKEAWAYS

- **Even if consumers take the best available precautions to protect themselves, they remain at risk of having their personal information leaked through corporate data breaches.**
- **While existing security practices can help organizations limit data breaches, it is not feasible for all organizations to adopt them broadly, quickly, and effectively enough to protect all consumer data.**
- **Companies should rethink the amount of data they collect, limiting the readable consumer data they retain to only what is necessary. This way, there is less data to exploit, and less risk to consumers.**

Benefits of End-to-End Encryption

- **Hackers cannot access end-to-end encrypted consumer data in the cloud,** even in the case of a data breach.
- **End-to-end encrypted communications can only be read by the sender and recipients**, even if hackers can compromise the networks and systems through which the communications are transiting.

As this report shows, the increasing digitalization of our personal and professional lives has fueled a dramatic rise in data breaches around the world. Each year, thousands of data breaches expose the personal information of hundreds of millions of consumers. Malicious actors continue to grow more determined and sophisticated, shifting their tactics to exploit vulnerabilities and steal valuable data. And the consequences of these attacks can be devastating — for the organizations that are hacked, and especially for the consumers whose sensitive data is compromised.

There is no easy solution to this problem. What is clear is that limiting the harm that is caused by data breaches will require a concerted effort from all parties.

Consumers should adopt modern security practices, such as multifactor authentication and proper password hygiene (such as not using the same password on multiple accounts), that make it more difficult for bad actors to target their individual accounts. In addition, **key industry players must continue to develop innovative security solutions** that make it easier for consumers to keep their data safe. Tools like biometric authentication combined with passwordless sign-in, for example, help consumers protect their private accounts without having to remember hundreds of different passwords. However, even if consumers deploy all of the best available tools to protect themselves, the rising number of corporate data breaches puts their data at constant risk.

This is why **corporations must adopt strong baseline security practices to defend against attacks**. But while many breaches could be prevented with good security practices, this alone will not be enough for two important reasons. First, it is unrealistic to expect quick and system-wide adoption of constantly evolving best security practices by all organizations that handle consumer data. Second, hackers are constantly **adapting and shifting their tactics to obtain consumer data they deem valuable**. Indeed, as the breach of Twilio that compromised Signal user data demonstrates, **even organizations (and individuals) with strong security practices can fall victim to sophisticated attacks, putting sensitive user data at risk**.

Government Efforts to Protect Consumer Data

The Cybersecurity and Infrastructure Agency (CISA, US) was established in 2018 to work across both the private and public sectors and reduce the risk to America's cyber and physical infrastructure.[135] In June 2022, new federal cybersecurity legislation passed, but, so far, only a few states have comprehensive data privacy laws.[136,137,138]

The General Data Protection Regulation (GDPR, EU) was established in 2018 and imposes requirements on organizations collecting data related to people in the EU.[139] The EU also passed the Cybersecurity Act strengthening ENISA, the European Union Agency for Cybersecurity, by providing it with more resources and broadening its role.[140]

The Personal Information Protection Act (PIPA, KR), which imposes obligations for most organizations that collect and process information of South Korean users — including government and foreign entities — was amended to include the protection of personal information processed by information and communication service providers.[141]

Governments around the world have started to recognize the extent of the problem and the need to take action. By 2023, an estimated 65% of the world's population will have their data covered under modern privacy regulation.[133] This is encouraging, yet there is a growing call by security experts for improved coordination between governments and organizations to better tailor legislation to address the risks.[134] Cybersecurity experts also underscore the need for stronger reporting mandates that require organizations, upon the discovery of a data breach, to disclose the types of records compromised and information about the incident.[19]

Ultimately, it is extremely unlikely that any steps taken by consumers, companies, or governments will deter cybercriminals and hackers who are determined to strike. While an increase in the number of digital interactions between companies and consumers provides some benefits to consumers, the increase in the volume of readable consumer data being collected that accompanies it is fueling the value of data to malicious actors. And as long as organizations continue to store troves of readable consumer data, inventive hackers will aim to find ways to exploit it.

This is why, today, organizations need to do more than fight to limit the frequency of data breaches. They must also act decisively to minimize the potential impact of breaches that can compromise even those with the strongest security measures. This means that for digital interactions between consumers and organizations to continue to grow safely, **companies that collect consumer data should rethink the types and amount of readable data they store**.

End-to-End Encryption Protecting Consumer Data

- **LastPass**, a password manager that has positioned data security as a top priority, suffered a breach through an account of a developer that was compromised following the Twilio data breach.[142,143,144,145]
- Despite the breach, bad actors failed to steal data stored in customers' vaults, including passwords, because the data was encrypted using an end-to-end encryption security model.
- LastPass' use of end-to-end encryption meant that no one — not even LastPass — had access to data stored in a customer's vault except for the user.[142,143,145] By limiting the amount of consumer readable data it retained, LastPass was able to protect sensitive personal data, and avoid a major password leak, despite being breached.

Considering how cheap it is to store data, it is easy to assume that there is little downside to gathering endless amounts of data, even if the benefits are minimal or uncertain. **But there is an important cost that is being ignored: the cost to the company and the impact on consumers if that data is stolen.** To protect consumers, companies must continue to innovate and find better solutions to secure consumer data, and take steps to prevent data breaches, including:

- **Consider only collecting data that is essential.** Companies should reconsider whether retaining particularly sensitive consumer data is necessary for their business purposes. And they should recognize that the most effective way to be responsible stewards of consumer data is to collect and retain less of it in the first place — minimizing the amount of readable data that hackers can exploit and reducing the risk to consumers around the world. For example, many stores scan and store customer drivers' licenses to confirm age when purchasing liquor or to confirm identity when returning products. Does this information really need to be saved once the age and identity of the person have been confirmed? Data that is not stored cannot be stolen.
- **Use strong encryption to create barriers around consumer data stored in the cloud.** In cases in which collecting and retaining consumer data is necessary, encryption can help protect that data against breaches. For data that needs to be accessed in the cloud, corporations should:
    - Strictly limit access to encryption keys, to minimize the likelihood that hackers can decrypt the data. While many organizations encrypt data at rest for compliance reasons, that encryption is often transparent, which means the data is automatically decrypted when accessed through the corporate system. Unfortunately, the convenience of this automatic decryption also means that a hacker who has breached the corporate system has unrestricted access to the decrypted data.
    - Corporations should also consider the strongest version of this protection by encrypting the data end-to-end. This means that even as the data is stored on, or transits through corporate systems, it can only be decrypted by the consumer to whom it belongs.

Sources

1. "How COVID-19 has pushed companies over the technology tipping point - and transformed business forever," *McKinsey & Company*, October 5, 2020.
2. "15 billion usernames and passwords for internet services including bank and social media accounts on offer to cyber criminals, finds new research from Digital Shadows," *Cision PR Newswire*, July 8, 2020.
3. "Data Breach Investigation Report," *Verizon*, 2014-2021.
4. "2022 Data Breach Investigations Report," *Verizon*.
5. "Cyentia Institute Publishes Groundbreaking Research on the Frequency and Cost of Breaches," *Cyentia Institute*, March 18, 2020.
6. "The State of Ransomware 2022," *SOPHOS*, April 2022.
7. "2022 ForgeRock Consumer Identity Report," *ForgeRock*.
8. "2021 Annual Data Breach Report," *Identity Theft Resource Center*, January 2022.
9. "Twilio Incident: What Signal Users Need to Know," *Signal*.
10. "2022 Data Breach Investigations Report," *Verizon*, p .34.
11. Sood, Gaurav, and Ken Cor, "Pwned: The Risk of Exposure From Data Breaches," *11th ACM Conference on Web Science*, 2019.
12. "';-- have i been pwned?," *Have I Been Pwned*.
13. "Cost of a Data Breach," *IBM*, July 2022.
14. Smith, David M., "Data Loss and Hard Drive Failure: Understanding the Causes and Costs," *Deepspar*.
15. Stamm, Stephanie, "How Pizza Night Can Cost More in Data Than Dollars," *The Wall Street Journal*, April 10, 2018.
16. Overberg, Paul, and Kevin Hand, "How to Understand the Data Explosion," *The Wall Street Journal*, December 8, 2021.
17. Ward, Lisa, "Small Businesses Struggle With an Increase in Cyberattacks," *The Wall Street Journal*, June 7, 2022.
18. "Small Business, Might Attack Surface," *RiskRecon*, August 23, 2022.
19. Neto, Nelson Novaes, Stuart Madnick, et al., "Developing a Global Data Breach Database and the Challenges Encountered," *ACM Journal of Data and Information Quality*, Vol. 13, No. 1, January 2021.
20. White, Jamie, "Yahoo Announces 500 Million Users Impacted by Data Breach," *LifeLock*, February 4, 2021.
21. Perlroth, Nicole, "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack," *The New York Times*, October 3, 2017.
22. Mari, Angelica, "Experian challenged over massive data leak in Brazil," *ZDNet*, February 20, 2021.
23. Whittaker, Zach, "Dailymotion admits hack exposed millions of accounts," *ZDNet*, December 5, 2016.
24. Kumar, Mohit, "Tianya, China's biggest online forum 40 million users data leaked," *The Hacker News*, December 26, 2011.
25. "Equifax Data Breach Settlement," *Federal Trade Commission*, September 2022.
26. Cimpanu, Catalin, "Hacker steals government ID database for Argentina's entire population," *The Record*, October 18, 2021.
27. "Ticketmaster UK Limited, Penalty Notice," *Information Commissioner's Office*, November 13, 2020.
28. Lomas, Natasha, "Cathay Pacific fined £500k by UK's ICO over data breach disclosed in 2018," *TechCrunch*, March 4, 2020.
29. "Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019," *Office of the Privacy Commissioner of Canada*, December 14, 2020.
30. Krebs, Brian, "Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions," *Krebs On Security*, May 31, 2022.
31. Dickey, Megan Rose, "Ride-hailing app Careem reveals data breach affecting 14 million people," *TechCrunch*, April 23, 2018.
32. Whittaker, Zack, "A new data leak hits Aadhaar, India's national ID database," *ZDNet*, March 23, 2018.
33. Dellinger, AJ, "Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?," *Forbes*, May 26, 2019.
34. Abrams, Lawrence, "Quantum ransomware attack disrupts govt agency in Dominican Republic," *Bleeping Computer*, August 24, 2022.
35. "Turkish Based Airline's Sensitive EFB Data Leaked," *Safety Detectives*.
36. Davis, Jessica, "Massive SingHealth Data Breach Caused by Lack of Basic Security," *Health IT Security*, January 10, 2019.
37. Khan, Shaharyar, et al., "A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned," *ACM Transactions on Privacy and Security*, 2022.
38. Cluley, Graham, "Hackers demand $15 million ransom from TransUnion after cracking "password" password," *Bitdefender*, March 21, 2022.
39. Yu, Eileen, "Australia kicks off investigation into Optus data breach," *ZDNet*, October 11, 2022.
40. "Digital Defense Report," *Microsoft*, October 2021.
41. "Cyber Signals August 2022," *Microsoft*, August 22, 2022.
42. "Face ID and Touch ID Security," *Apple Support*, February 18, 2021.
43. "Apple, Google, and Microsoft commit to expanded support for FIDO standard to accelerate availability of passwordless sign-ins," *Apple*, May 5, 2022.
44. "About the security of passkeys," *Apple Support*, June 7, 2022.
45. "Secure Enclave," *Apple Support*, May 17, 2021.
46. Xin, Xiaowen, "Titan M makes Pixel 3 our most secure phone yet," *Google Blog*, October 17, 2018.
47. "This is protection. Samsung Knox," *Samsung Insights*, October 21, 2021.
48. Kan, Michael, "Here's How Much Your Identity Goes for on the Dark Web," *PCMag*, November 15, 2017.
49. Damiani, Jesse, "Your Social Security Number Costs $4 On The Dark Web, New Report Finds," *Forbes*, March 25, 2020.
50. "Form 10-K," *Equifax*, 2020.
51. "Healthcare Breach Report," *Critical Insight*, July-Dec 2021.
52. Wong, Natalie, "Hackers Target Homebuyers in Infuriating Scam That Keeps Working," *Bloomberg*, October 7, 2022.
53. "Incident Report: Employee and Customer Account Compromise," *Twilio*, October 27, 2022.
54. McCall, Vivian, and Barbara Smith, "What is Signal? How the popular encrypted messaging app keeps your texts private," *Business Insider*, October 19, 2021.
55. Page, Carly, "DoorDash hit by data breach linked to Twilio hackers," *TechCrunch*, August 25, 2022.

56. Franceschi-Bicchierai, Lorenzo, "How a Third-Party SMS Service Was Used to Take Over Signal Accounts," *Motherboard Vice*, August 17, 2022.

57. Newman, Lily H., "Why the Twilio Breach Cuts So Deep," *Wired*, August 26, 2022.

58. Bomey, Nathan, "How Chinese military hackers allegedly pulled off the Equifax data breach, stealing data from 145 million Americans," *USA Today*, February 10, 2020.

59. "Equifax says more than 19,000 Canadians affected by security breach," *CBC*, November 29, 2017.

60. McCrank, John, "Equifax says 15.2 million UK records exposed in cyber breach," *Reuters*, October 10, 2017.

61. Kabanov, Ilya, and Stuart Madnick, "Applying the Lessons from the Equifax Cybersecurity Incident to Build a Better Defense," *MIS Quarterly Executive*, Vol. 20, No. 2, June 2021.

62. Madnick, Stuart, "The Rest of the Cybersecurity Story," *MIT Sloan Management Review*, June 21, 2022.

63. "Information on the Capital One Cyber Incident," *Capital One*.

64. Glover, Claudia, "Former AWS engineer who hacked Capital One will face no further jail time," *Tech Monitor*, October 5, 2022.

65. Doffman, Zak, "Ashley Madison Hack Returns To 'Haunt' Its Victims: 32 Million Users Now Watch And Wait," *Forbes*, February 1, 2020.

66. Hatmaker, Taylor, "Healthcare data breach in Singapore affected 1.5M patients, targeted the prime minister," *TechCrunch*, July 20, 2018.

67. "SingHealth's IT System Target of Cyberattack," *Ministry of Communications and Information*, July 20, 2018.

68. "Cybersecurity Incidents," *U.S. Office of Personnel Management*.

69. Chaffetz, Jason, et al., "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation: Majority Staff Report," *U.S. House of Representatives Committee on Oversight and Government Reform*, September 7, 2016.

70. "ACCC warnng of suspicious messages as 'Hi Mum' scams spike," *Australian Competition & Consumer Commission*, August 23, 2022.

71. Cowley, Stacy, and Lananh Nguyen, "Fraud Is Flourishing on Zelle. The Banks Say It's Not Their Problem.," *The New York Times*, March 6, 2022.

72. Finney, Michael, "Zelle scammers use stolen personal information to trick bank customers," *ABC7 News*, July 28, 2022.

73. "Details of the Mailchimp data breach," *Trezor Blog*, April 14, 2022.

74. "Information About a Recent MailChimp Security Incident Targeting Crypto Companies," *MailChimp*, August 22, 2022.

75. "Ongoing phishing attacks on Trezor users," *Trezor Blog*, April 4, 2022.

76. "An update on our security incident," *Twitter*, July 18, 2020.

77. "Twitter Investigation Report," *The New York State Department of Financial Services*, October 14, 2020.

78. Frenkel, Sheera, et al., "A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam," *The New York Times*, July 15, 2020.

79. "Anthem Data Breach," *California Department of Insurance*.

80. Whittaker, Zack, "Justice Department charges Chinese hacker for 2015 Anthem breach," *TechCrunch*, May 9, 2019.

81. "The State of Ransomware in Healthcare 2022," *SOPHOS*, May 2022.

82. "How to protect your Android phone from ransomware - plus a guide to removing it," *Avira*, August 13, 2020.

83. "Ransomware and the CIA Triad: Considerations for Evolving Attack Methods," *CyberOne*, April 28, 2020.

84. "Ransomware Uncovered 2021-2022," *Group-IB*, May 2022.

85. "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction," *Microsoft*, March 22, 2022.

86. Krebs, Brian, "A Closer Look at the LAPSUS$ Data Extortion Group," *Krebs On Security*, March 23, 2022.

87. "Ransomware in Midsize Enterprises," *Gartner*.

88. "Ransomware," *Federal Bureau of Investigation*.

89. Skulkin, Oleg, "Group-IB: ransomware empire prospers in pandemic-hit world. Attacks grow by 150%," *Group-IB*, March 4, 2021.

90. Ardagna, Claudio, et al., "ENISA Threat Landscape 2021," *European Union Agency for Cybersecurity*, October 2021.

91. Palmer, Danny, "Ransomware as a service is the new big problem for businesses," *ZDNet*, March 4, 2021.

92. Huang, Keman, et al., "Systematically Understanding the Cyber Attack Business: A Survey," *ACM Computing Surveys*, Vol. 51, No. 4, July 2018.

93. "Information Security and Cyber Risk Management Survey Report," *Zurich and Advisen*, October 2021.

94. Ralston, William, "They Told Their Therapists Everything. Hackers Leaked It All.," *Wired*, May 4, 2021.

95. Ralston, William, "A dying man, a therapist and the ransom raid that shook the world," *Wired*, September 12, 2020.

96. Jackson, Lewis, et al., "Australia flags privacy overhaul after huge cyber attack on Optus," *Reuters*, September 26, 2022.

97. Taylor, Josh, and Ben Butler, "Alleged Optus hacker apologises for data breach and drops ransom threat," *The Guardian*, September 27, 2022.

98. Faife, Corin, "Australia to overhaul privacy laws after massive data breach," *The Verge*, September 26, 2022.

99. Whittaker, Zack, "A ransomware attack on a debt collection firm is one of 2022's biggest health data breaches," *TechCrunch*, July 13, 2022.

100. Battaglio, Stephen, "Celebrity law firm won't pay ransom to hackers claiming they have 'dirty laundry' on Trump," *Los Angeles Times*, May 18, 2020.

101. Fletcher, Olivia, "Billionaire's Jeweler Pays $7.5 Million Crypto Ransom to Hackers," *Bloomberg*, July 6, 2022.

102. Collier, Kevin, "Costa Rica declares state of emergency over ransomware attack," *NBC News*, May 11, 2022.

103. "Atlanta officials reveal worsening effects of cyber attack," *Reuters*, June 6, 2018.

104. "Baltimore's 911 emergency system hit by cyberattack," *NBC News*, March 28, 2018.

105. "Hackers have been holding the city of Baltimore's computers hostage for 2 weeks," *Vox*, May 21, 2019.

106. Abrams, Lawrence, "Ransomware attack exposes data of 500,000 Chicago students," *Bleeping Computer*, May 21, 2022.

107. Page, Carly, "Hackers leak 500GB trove of data stolen during LAUSD ransomware attack," *TechCrunch*, October 3, 2022.

108. "2022 Cost of Insider Threats Global Report," *Ponemon Institute*.

109. "2021 Insider Threat Report," *Cybersecurity Insiders*.

110. O'Brien, Rachel, "Tech Consultant Fights AT&T's Attempt To Nix Theft Suit," *Law360*, July 8, 2020.

111. "Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public," *Federal Bureau of Investigation*, February 8, 2022.

112. Marotta, Angelica, and Stuart Madnick, "Cybersecurity as a unifying factor for privacy, compliance and trust: The Haga Hospital Case," *Issues in Information Systems*, Vol. 23, No. 1, 2022, pp. 102-116.

113. Newman, Lily H., "Twitter Insiders Allegedly Spied for Saudi Arabia," *Wired*, November 6, 2019.

114. Huang, Kalley, and Kate Conger, "Former Twitter Employee Convicted of Charges Related to Spying for Saudis," *The New York Times*, August 9, 2022.

115. Vengattil, Munsif, and Fanny Potkin, "India forced Twitter to put agent on payroll, whistleblower says," *Reuters*, August 23, 2022.

116. Hern, Alex, "Uber employees 'spied on ex-partners, politicians, and Beyoncé'," *The Guardian*, December 13, 2016.

117. Hill, Kashmir, "'God View': Uber Allegedly Stalked Users for Party-Goers' Viewing Pleasure (Updated)," *Forbes*, October 3, 2014.

118. Bhuiyan, Johana, and Charlie Warzel, "'God View': Uber Investigates Its Top New York Executive For Privacy Violations," *BuzzFeed News*, November 18, 2014.

119. Kendall, Marisa, "Uber settles federal probe over alleged spying on passengers," *Mercury News*, August 15, 2017.

120. Conger, Kate, and Kevin Roose, "Uber Investigating Breach of Its Computer Systems," *The New York Times*, September 15, 2022.

121. Madnick, Stuart, "More 'Side Door' Hacks Are Coming. Here Is How Businesses Can Prepare," *The Wall Street Journal*, February 23, 2021.

122. Oladimeji, Saheed, and Sean Michael Kerner, "SolarWinds hack explained: Everything you need to know," *TechTarget*, June 29, 2022.

123. "Insight Space: Supply Chain Risk A back door for hackers? (Issue 6)," *NCC Group*.

124. Hunter, Tatum, and Gerrit De Vynck, "The 'most serious' security breach ever is unfolding right now. Here's what you need to know.," *The Washington Post*, December 20, 2021.

125. Slabodkin, Greg, "FDA warns about Log4j cybersecurity vulnerabilities in medical devices," *MedTech Dive*, December 20, 2021.

126. Gallo, Katlyn, "Log4j Vulnerability Explained: What It Is and How to Fix It," *Built In*, September 23, 2022.

127. Uberti, David, et al., "The Log4j Vulnerability: Millions of Attempts Made Per Hour to Exploit Software Flaw," *The Wall Street Journal*, December 21, 2021.

128. Sharma, Ax, "Fintech firm hit by Log4j hack refuses to pay $5 million ransom," *Bleeping Computer*, December 29, 2021.

129. "Log4j in 2022: The best expert insights, adversaries and actions," *CyberTalk*, January 13, 2022.

130. "Security Vulnerability in Minecraft: Java Edition," *Minecraft Help Center*, November 11, 2022.

131. "Review of the December 2021 Log4j Event," *Cyber Safety Review Board*, July 11, 2022.

132. "Dragonfly ICS Cyber Attack," *Catapult*.

133. "Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations," *Gartner*, September 14, 2020.

134. Jain, Samir C., and Lisa M. Ropple, "Stopping Data Breaches Will Require Help from Governments," *Harvard Business Review*, December 14, 2018.

135. "About CISA," *Cybersecurity and Infrastructure Security Agency*.

136. "Press Release: Bill Signed: S. 1097, S. 2520, and S. 3823," The White House Briefing Room, June 21, 2022.

137. Klosowski, Thorin, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)," *The New York Times*, September 6, 2021.

138. Stauss, David, "State data privacy legislation: Takeaways from 2022 and what to expect in 2023," *iapp*, August 23, 2022.

139. Wolford, Ben, "What is GDPR, the EU's new data protection law?," *GDPR.eu*.

140. "The EU Cybersecurity Act," *Digital Strategy European Commission*, June 7, 2022.

141. Feigenbaum, Evan A., et al., "The Korean Way With Data: How the World's Most Wired Country Is Forging a Third Way," *Carnegie Endowment for International Peace*, August 2021.

142. Toubba, Karim, "Notice of Recent Security Incident," *LastPass*, November 30, 2022.

143. "LastPass Security History," *LastPass*.

144. Townsend, Chance, "DoorDash data breach leaves important customer details exposed," *Mashable*, August 28, 2022.

145. "LastPass Security Reports," *LastPass*.