The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase

Professor Stuart E. Madnick, Ph.D.

December 2023

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

Executive summary

Around the world, individuals' most private, most personal data has become a target for cybercriminals. Attacks and data breaches across the globe continue to increase. Even as organizations work to fight back, cybercriminals are constantly finding new ways to access and exploit readable personal data, in particular when stored in the cloud.[1]

Last year's study, "The Rising Threat to Consumer Data in the Cloud," found that these threats had reached historically high levels. And now, with complete data from 2022 and most of 2023 underway, many indicators show that the threat is getting even worse.

You can read last year's study, "The Rising Threat to Consumer Data in the Cloud," for an overview of the evolving threat to consumer and personal data stored in the cloud, and some of the most common avenues exploited by cybercriminals to expose this data, including **(1)** supply chain attacks, **(2)** corporate ransomware attacks, and **(3)** insider threats.

For US organizations, data breaches are now at an all-time high. In just the first nine months of 2023, data breaches in the US have already increased by nearly 20% compared to all of 2022[2,3,4] — and organizations around the world have faced similar trends.

These attacks are increasingly impactful because people are now living more of their lives online, meaning that corporations, governments, and other types of organizations collect more and more personal data — sometimes with little choice from individuals. And because people's most personal data can be exploited and sold for a significant profit, it's become a growing target for cybercriminals.[5]

Most recently, two key factors have contributed to the increased threat to personal data:

- First, **ransomware attacks are more numerous and dangerous than ever**.
  - In 2023, ransomware attacks increased to levels never seen before, while also becoming more sophisticated and aggressive.[6,7,8,9] Hackers are becoming more organized, often through ransomware gangs.[6] Their attacks are also more threatening and more likely to target organizations with sensitive data, like governments, mass-market genetic testing companies, or healthcare facilities.[10] In the past, ransomware attacks often locked up a company's data until a ransom was paid. Now, hackers are more likely to leak corporate and consumer data, often hurting consumers.
- Second, **attacks that exploit vendors are increasing**, and they frequently spread to many other organizations that depend on those vendors. This means that the consequences of even one attack can be devastating.[11]
  - In today's interconnected world, virtually every organization relies on a wide range of vendors and software. As a result, hackers only need to exploit vulnerabilities in third-party software or a vendor's system to gain access to the data stored by every organization that relies on that vendor.[11,12] Tellingly, 98% of organizations have a relationship with a vendor that experienced a data breach within the last two years.[13]

While organizations acknowledge these threats and pour resources into defending against them, inventive hackers have shown that they will continue to find ways to bypass security measures.[8] And as long as organizations keep collecting troves of unencrypted personal data, hackers are motivated to keep finding new ways to get it.

This is why it's imperative that organizations consider limiting the amount of personal data they store in readable format while making a greater effort to protect the sensitive consumer data that they do store. And it's why the technology industry is increasingly adopting innovative solutions that implement end-to-end encryption such as iCloud's Advanced Data Protection to reduce the amount of vulnerable data stored by organizations and the risk to individuals.[14]

"We assess that ransomware attacks targeting US networks will increase in the near- and long-terms. Cybercriminals have developed effective business models to increase their financial gain, likelihood of success, and anonymity."

Alejandro Mayorkas (US Secretary of Homeland Security)[15]

"In recent years, we have seen an unprecedented increase in both the number of cyber threats and their sophistication, with attacks becoming more tailored as criminals aim for maximum impact, and maximum profit."

Bernardo Pillot (INTERPOL's Assistant Director of Cybercrime Operations)[16]

"In cyberspace, the threats only seem to evolve, and the stakes have never been higher… And over the past few years, we've increasingly seen cybercriminals using ransomware against US critical infrastructure sectors."

Christopher Wray (Director of the FBI)[17]

"The UK is a top target for cybercriminals. Their attempts to shut down hospitals, schools and businesses have played havoc with people's lives and cost the taxpayer millions … Sadly, we've seen an increase in attacks."

Tom Tugendhat (UK Minister of State for Security)[18]

By the numbers

Overview of 2022 and 2023 key statistics

2.6 billion

Over 2.6 billion personal records were breached in 2021 and 2022 (**1.1 billion** in 2021 and **1.5 billion** in 2022).[A,19,20]

3x

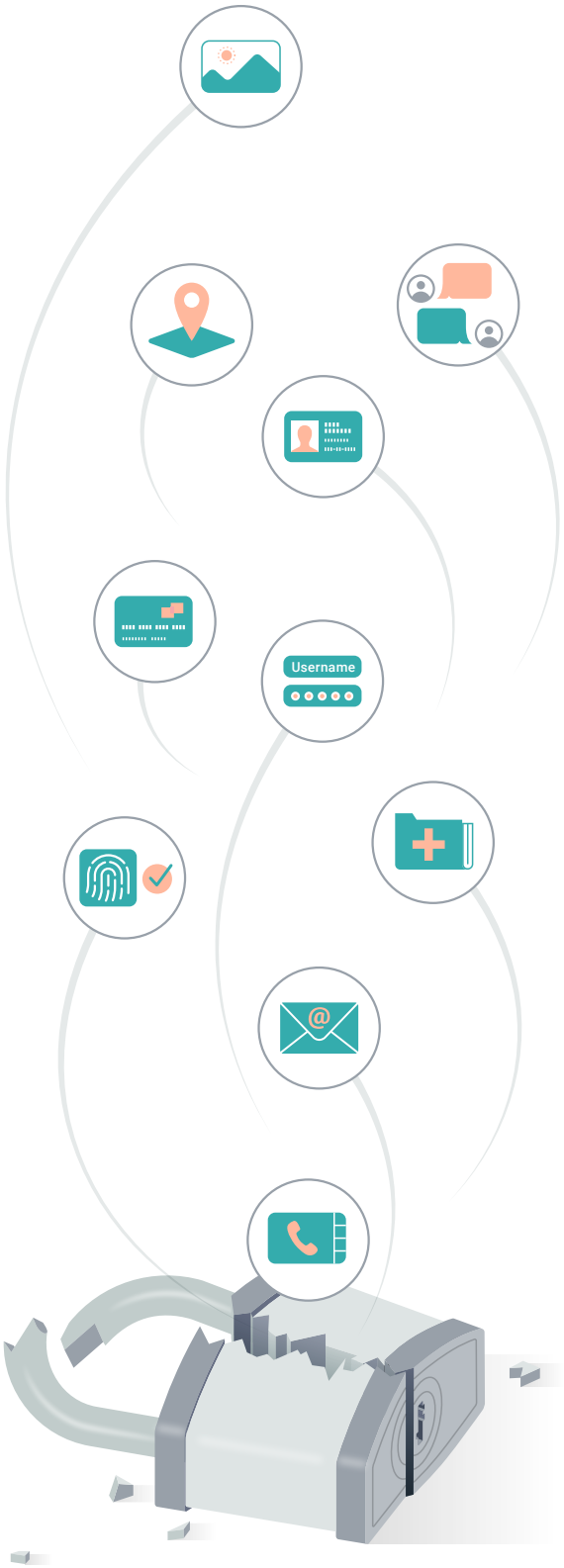
The number of data breaches **more than tripled** between 2013 and 2022.[21,22]

+20%

In the first nine months of 2023, the number of data breaches in the US have already **increased by nearly 20%** compared to all of 2022.[2,3,4]

95%

In the 2023 IBM Cost of a Data Breach Report, **95% of breached organizations surveyed experienced more than one data breach**.[23] According to a 2022 study by Forrester, nearly **75% of surveyed organizations were victims of a data breach in the prior 12 months**.[10]



80%

According to a 2023 report, **over 80% of data breaches** involved data stored in the **cloud**.[24]

+70%

In the first three quarters of 2023, **the number of ransomware attacks increased by almost 70%** compared to the first three quarters of 2022.[9]

98%

98% of organizations have a relationship with a vendor that experienced a data breach within the last two years.[13]

360 million

In the first eight months of 2023 alone, **over 360 million people were victims of corporate and institutional data breaches**.[25]

1 of 4

In the first three quarters of 2023, one in four people in the US had their health data exposed in a data breach.[26,27]

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

Cloud: common term used to refer to servers, software, data, or services that are accessed or delivered through the internet.

Cloud misconfiguration: errors, glitches, or vulnerabilities in the user-controlled settings in a cloud environment that risk exposing sensitive corporate data.

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) which makes the data "readable."

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

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: 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.

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.

Vendor exploitation attacks: bad actors targeting vendors or suppliers that have access to an organization's corporate network, code, data, software, or hardware — for example, a bad actor exploiting an outside vendor with a weaker security protocol to bypass a large organization's strong security and access its network.

Recent trends: The rise in ransomware attacks and attacks on vendors' systems

Overview of 2023

Recent examples of global data breaches

23andMe, the genetic testing company, disclosed a data breach in October 2023, potentially exposing 300 terabytes of user data (see page 9).

Discord.io, a third-party service for social platform Discord, was hacked in August 2023. Account information for over 760,000 individuals was breached.[40]

Forever 21, the global clothing company, was hacked between January and March 2023. The attack exposed personal and health insurance information of nearly 540,000 current and former employees.[41]

MGM Resorts, a global hospitality and entertainment company operating in the US, China, and Japan, was the victim of a ransomware attack in September 2023, leading to operational outages across its properties and the breach of customers' personal information. Another hospitality company, Caesars, was similarly targeted by cybercriminals weeks earlier.[42,43,44,45]

Microsoft, one of the largest software vendors in the world, suffered multiple cyberattacks in 2023 that affected consumers, employees, and government entities across several countries (see page 15).

KEY TAKEAWAYS

- **Data breaches impacting US organizations are already at "an all-time high," as there were more breaches in the first three quarters of 2023 than in any prior year.[2,3,4]**
- **Organizations across the globe have been targeted by cybercriminals this year, with those based in the UK, the US, Australia, and Canada targeted most frequently.**
- **The threat is increasing not only in the English-speaking world. For example, in the first quarter of 2023, ransomware activity in the Middle East increased by 77% compared to the same period in 2022.[28]**

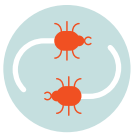
Consumer data stored by organizations, particularly in the cloud, is a major, growing target for cybercriminals. In the first eight months of 2023 alone, over 360 million people were victims of corporate and institutional data breaches, and one in four people in the US had their health data exposed in a data breach.[25,26,27] In fact, more data breaches have happened in the US through the first three quarters of 2023 than in all of 2022.[2,3,4] This is also the case in the healthcare sector, where reporting requirements are stricter.[B,29,30]

Organizations across the globe and their data have been targeted by cybercriminals this year (see sidebar on **Recent examples of global data breaches**), driving a considerable increase in attacks in many regions and countries, including in the US, the UK, Australia, and Canada. According to the Identity Theft Resource Center, a nonprofit organization with a focus on identifying theft and data privacy issues, data breaches impacting US organizations are already at "an all-time high."[4] In the UK, Australia, and Canada combined, more than double the number of accounts were breached in the first half of 2023 compared to the first half of 2022.[C,31,32,33,34] In the UK, this increase is even more dramatic, as the number of cyberattacks reported to the National Cyber Security Centre in 2023 hit an "all-time high," increasing by 64% compared to 2022.[35] In Australia, two data breaches that occurred in the last 12 months — one that targeted Latitude Financial, a financial institution, the other targeting Medibank, one of the largest health insurance companies in the country — impacted over 23 million people.[36] Moreover, according to the Australian Cyber Security Centre, reports of cybercrime in Australia increased by 23% in the 2023 fiscal year to June (July 1, 2022, through June 30, 2023) over the previous fiscal year.[37] Other regions have been affected too, such as the Middle East, where ransomware gang activity increased by 77% in the first quarter of 2023 compared to same period in 2022.[28]

This rising threat to consumer data is a consequence of the growing amount of unencrypted personal data that corporations and other organizations collect

and store, particularly in the cloud.[38,39] Organizations can reduce the likelihood of hackers using or selling their consumer data by encrypting data stored in their networks, making it only readable by those who have the key to decrypt it.

Protecting data stored in corporate networks is critical, since once hackers realize that an organization is vulnerable to an attack, they will repeatedly attempt to breach the organization's network. For example, according to a 2023 report, 95% of breached organizations surveyed experienced more than one data breach.[23] (See sidebar for a discussion of **Repeated attacks**.) Moreover, as of early 2023, more than 80% of data breaches involved data stored in the cloud, following a near doubling of attacks targeting cloud infrastructure between 2021 and 2022.[24,39] The cloud offers institutions various benefits, including channels to smoothly scale up and down storage usage and the flexibility of accessing data globally, which has led to a mass migration of data to the cloud.[46] Because cloud services are based on new technology, many organizations' technical staffs may not be familiar with all the settings and procedures needed to secure the data. Therefore, as more and more data moves to the cloud, cloud misconfigurations, caused by errors that expose a cloud environment, have become one of the most common security issues with cloud applications. Cloud misconfiguration can be caused by factors like excessively permissive cloud access, unrestricted ports, and unsecured back-ups.[47] According to the NSA, "cloud misconfigurations are the most prevalent cloud vulnerability" and can be exploited by hackers to access cloud data and services.[48] (See pullout box for examples of **Cloud misconfigurations**.)



Repeated attacks

In the last 12 months, cybercriminals continued to target organizations that were breached previously.

GoDaddy, a US-based web hosting services provider, suffered data breaches in 2020, 2021, and 2022. In one attack, hackers accessed Managed WordPress, GoDaddy's hosting platform for building and managing WordPress sites, and exposed personal information — including names, email addresses, usernames, and passwords — for over 1.2 million customers.[49,50]

T-Mobile, a global telecommunications company, suffered a data breach that exposed the personal data of 37 million customers in January 2023. Two months later, attackers again stole the data of a large number of T-Mobile's customers.[51]

Flagstar, a commercial US bank, has experienced three data breaches since March 2021. The most recent breach, in May 2023, resulted in the exposure of more than 800,000 Flagstar customers' personal information.[52,53]

The Japanese company **Sony** suffered two data breaches in 2023. The first incident resulted in bad actors exposing the personal data of thousands of employees and their family members. Months later, the company's sensitive data was stolen and put up for sale online.[54,55]

Cloud misconfigurations

Toyota Motor Corporation, a Japanese automaker, reported in May 2023 that it identified a decade-long data leak attributable to a security lapse in a misconfigured database in the cloud of its big data and mobility affiliate, Toyota Connected Corporation. The leak exposed the data of 2.15 million Japanese car owners, including vehicle identification numbers, vehicle locations, and video footage recorded by the vehicle.[56]

Slick, an India-based social media app, reported in February 2023 that a misconfiguration led to the password-free access of its database, which held the personal information of over 150,000 users — including names, mobile numbers, and profile pictures — for at least two months.[57,58]

The Egyptian government and Academic Assessment, a UK education company, exposed sensitive personal information of over 70,000 children online for months in early 2023 due to a cloud misconfiguration. The exposed data included the children's names, dates of birth, home addresses, and education information.[59]

In September 2023, it was reported that **Microsoft** exposed over 38 terabytes of employee data due to a cloud misconfiguration (see page 15).

Cybercriminals have also increasingly targeted organizations, including private companies and government entities, that collect particularly sensitive personal information, such as schools, mass-market genetic testing companies, healthcare institutions, and military and police institutions. Because such data is so sensitive, it is especially attractive to cybercriminals. (See pullout boxes for examples of **Cybercriminals targeting organizations with sensitive data and governmental entities**.)

Two trends have contributed to the heightened risk to consumer data seen in 2023, which we explore in more detail below: (1) the growth in the number and the evolution of ransomware attacks, and (2) the growth in hackers targeting widely used vendors and software to access the systems of companies that use those vendors.

Cybercriminals targeting organizations that hold particularly sensitive personal information

- **23andMe,** a mass-market genetic testing company, disclosed in October 2023 that customer data was breached, exposing sensitive customer information including names, photos, and genetic information.[60,61] The hackers claim they stole 300 terabytes of 23andMe user data.[62]
- **The Minneapolis Public Schools** announced in March 2023 that students' data was breached, exposing over 300,000 sensitive files containing details describing student sexual assaults, psychiatric hospitalizations, abusive parents, and suicide attempts. One student who reported a sexual assault had her confidential complaint released online, leading her mother to state that she felt "violated again."[63]
- **The Better Outcomes Registry & Network**, a perinatal and child registry in Ontario, Canada, reported a data breach in May 2023 due to its use of MOVEit, a file transfer service, which exposed sensitive records of over 3.4 million patients in Ontario, including names, home addresses, and health card numbers, as well as lab test results, procedures, and outcomes relating to pregnancy and newborn care.[64,65]
- **One in Four**, an Irish charity that supports survivors of childhood sexual abuse, reported a data breach in May 2023 that stemmed from an attack on its data manager, Evide. The data breach resulted in the potential exposure of around 1,000 clients' sensitive personal information, including records of people's engagement with One in Four's services and other personally identifiable information.[66]

Cybercriminals targeting governmental entities and contractors

- **The City of Oakland, California,** was the target of multiple ransomware attacks in 2023, which resulted in the exposure of over 600 gigabytes of personal information regarding city workers and residents, including Social Security numbers and home addresses. In addition, this attack forced the city to take its systems offline and declare a state of emergency.[67,68,69]
- **Egypt's Ministry of Health and Population** suffered a data breach in July 2023, which resulted in the exfiltration of sensitive health information, including personally identifiable information along with patient records such as prior procedures, diagnoses, and treatments.[70,71]
- **The UK's Ministry of Defence** suffered a ransomware attack in August 2023, which resulted in the disclosure of thousands of pages of security secrets, including data concerning a nuclear submarine base and a chemical weapon lab.[72]
- **Microsoft**, a contractor to the US State and Commerce departments, was hacked in May 2023. Microsoft Outlook email accounts from the US State and Commerce departments were breached, resulting in the theft of 60,000 emails from the US State Department and the hacking of the US commerce secretary's email account.[73,74]
- **Maximus Federal Services**, a US contractor to the Medicare program, was one of the organizations hacked as a result of the MOVEit hack (see page 17), which resulted in an estimated 612,000 Medicare beneficiaries having their health or personal identifiable information breached.[75]

Examples of regional data breaches in the last 12 months[D]

AMERICAS

CORPORATE RANSOMWARE

Andrade Gutierrez
BRAZIL
3 terabytes of employee and corporate data[76]

Alberta Dental Services Corporation
CANADA
1.5 million customers' personal and financial information[77]

Keralty Group
COLOMBIA
3 terabytes of personal data and medical records[78]

HCA Healthcare
UNITED STATES
11 million patients' personal and healthcare data[79]

PharMerica
UNITED STATES
Over 5.8 million patients' personal and healthcare data[80]

INSIDER THREAT

Former National Security Advisor
EL SALVADOR
5.1 million records of personal data belonging to citizens[81]

VENDOR EXPLOITATION

BORN Ontario
CANADA
3.4 million patients' fertility and other healthcare data[82]

T-Mobile
UNITED STATES
37 million customers' personal data[83]

Welltok
UNITED STATES
8.5 million patients' personal data[84]

Microsoft Outlook
UNITED STATES
Confidential emails of US State and Commerce departments' staff[73,74]

Maximus Federal Services
UNITED STATES
Personal or health information of over 600,000 Medicare beneficiaries[75]

TARGETED SOCIAL ENGINEERING

Citizens of Mexico
MEXICO
40 million citizens' personal records[85]

EUROPE

CLOUD MISCONFIGURATION

Scotland's People
GREAT BRITAIN, SCOTLAND
Birth, death, and adoption records going back up to 100 years[86]

CORPORATE RANSOMWARE

City of Antwerp
BELGIUM
557 gigabytes of residents' personal data[87]

Motel One Group
DENMARK, GERMANY, NETHERLANDS, SPAIN
24.5 million files containing customers' personal data[88]

Flying Blue
FRANCE, NETHERLANDS
Up to 17 million customers' personal data[89]

Hospital Clínic de Barcelona
SPAIN
4.4 terabytes of healthcare data exfiltrated, leading to operational outages[90]

R and Euskaltel
SPAIN
Over 3 terabytes of customer, employee, and corporate data[91]

Neue Zürcher Zeitung and CH Media
SWITZERLAND
800 gigabytes of personal and employee data[92]

VENDOR EXPLOITATION

Pôle Emploi
FRANCE
10 million citizens' employment data[93]

Blauw
NETHERLANDS
1.5 million customers' personal data[94]

Microsoft Exchange
UNITED KINGDOM
Over 40 million voters' personal data from the UK Electoral Commission[95]

National Health Service
UNITED KINGDOM
2.5 million patients' healthcare data[96]

Over 40 Different Charities
UNITED KINGDOM
Over 600,000 donors' personal data and contribution data[97]

MIDDLE EAST AND AFRICA

CLOUD MISCONFIGURATION

Egypt's Ministry of Education
EGYPT
72,000 children's education records and personal data[59]

CORPORATE RANSOMWARE

Egypt's Ministry of Health
EGYPT
2 million citizens' health records[70,71]

Fanap Behnama
IRAN
20 gigabytes of sensitive corporate data[98]

Foreign Ministry of Iran
IRAN
11,000 federal employees' personal data[99]

Technion Israel Institute of Technology
ISRAEL
Up to 15,000 students' data[100]

Armed Forces of the Republic of Ivory Coast
IVORY COAST
Over 37,000 files, including facial records[101]

Adidas Morocco
MOROCCO
Over 62,000 customers' and employees' personal data[102]

South African Dept. of Defense
SOUTH AFRICA
1.6 terabytes of classified information[103]

e-Devlet
TÜRKIYE
85 million citizens' personal data[104]

Elca Cosmetics
TÜRKIYE
83,000 customers' personal data[105]

INSIDER THREAT

Kenya Airports Authority
KENYA
514 gigabytes of corporate data, including blueprints[106]

VENDOR EXPLOITATION

Hotic Shoes
TÜRKIYE
2 million employees' and customers' data[107]

ASIA PACIFIC

CLOUD MISCONFIGURATION

Office of the Registrar General
BANGLADESH
Over 50 million citizens' personal data[108]

Slick
INDIA
153,000 teens' personal data[57,58]

Toyota
JAPAN
Over 2.15 million customers' location data over 10 years[109]

CORPORATE RANSOMWARE

Medibank
AUSTRALIA
9.7 million customers' personal and healthcare data[110]

SuperVPN
CHINA
360 million records of personal data[111]

OT&P Healthcare
HONG KONG
100,000 patients' personal data and medical histories[112]

Sphero
HONG KONG
Over 1 million students' and educators' personal data[113]

Directorate General of Immigration
INDONESIA
34 million individuals' passport information[114]

Auckland University of Technology
NEW ZEALAND
60 gigabytes of corporate data[115]

PhilHealth
PHILIPPINES
Over 13 million customers' personal data[116]

VENDOR EXPLOITATION

Latitude Financial
AUSTRALIA, NEW ZEALAND
14 million customers' personal data[117]

Te Whatu Ora
NEW ZEALAND
Over 18,000 coronial files and about 14,000 health records[118]

The growth and evolution of ransomware attacks

KEY TAKEAWAYS

- **Nearly 50% more organizations suffered a ransomware attack in the first half of 2023 compared to the first half of 2022.**[119]
- **Cybercriminals are becoming more organized, frequently operating as part of specialized "ransomware gangs."**[6]
- **Ransomware attacks have expanded from "locking up" an organization's data until it pays the ransom to publicly disclosing personal data breached to increase the pressure to pay the ransom.**

Countries frequently targeted by ransomware attacks

United States: Ransomware attacks increased by more than 50% between October 2022 and September 2023, compared to the previous 12 months.[128]

United Kingdom: Ransomware attacks climbed by over 80% in the first half of 2023 compared to the first half of 2022.[129]

Canada: The Canadian Centre for Cyber Security called ransomware "the most disruptive form of cybercrime facing Canada"[130] and concluded that organized cybercrime will very likely pose a threat to Canada's national security and economic prosperity in 2023 and 2024.[131]

Australia: In the first half of 2023, ransomware attacks were the most common cybersecurity incidents.[132] In 2023, Australia suffered one of the largest data breaches in recent history, when a ransomware attack on Latitude Financial affected around 14 million people.[36,117,133]

In the last year, ransomware attacks on corporations and institutions — in which hackers take control of a corporate or institutional asset, such as consumer data, and demand a ransom in exchange for the asset's return or to prevent its public exposure — have become more common, more aggressive, and more harmful to consumers.

More organizations have suffered a ransomware attack this year, as reflected by multiple measures. For example:

- More ransomware attacks were reported through September 2023 than in all of 2022. In the first three quarters of 2023, the number of ransomware attacks increased by nearly 70% compared to the first three quarters of 2022.[9]
- The number of ransomware attacks was two and a half times higher in September 2023 compared to September 2022.[120]
- A 2023 survey of 233 IT/cybersecurity professionals across 14 countries working in the healthcare sector found that 60% of organizations have faced a ransomware attack, which is almost double the 34% reported by the sector in 2021.[121]

More ransomware attacks also mean more victims. In May 2023, the number of ransomware victims listed on leak sites was almost three times higher than in May 2022.[122]

The US and UK were the countries most frequently targeted by ransomware attacks in 2023, followed by Canada and Australia. Nearly 70% of ransomware attacks occurred in these four countries.[123,124,125] (See sidebar on **Countries frequently targeted by ransomware attacks**.) For example, Digital ID, a supplier of ID cards for various UK governmental organizations, including the Greater Manchester Police and the London Metropolitan Police Service, fell victim to a ransomware attack in August 2023. As a result, police records, including police officers' names and photos, were exposed.[126,127]

Not only have these attacks become more common; hackers have also shifted their strategies over the years to cause the most harm possible. Originally, many ransomware attacks focused on taking control of the operational structure of corporations or institutions, causing operational outages and locking corporate data, and then extorted a ransom from these institutions in exchange for releasing control of their systems.[134] Over the last few years, bad actors have increasingly focused on taking control of personal data collected and stored by the corporations and institutions. Moreover, as organizations have been able to retrieve their customer data through backups and other countermeasures, hackers are becoming more aggressive, often leaking the stolen data on the dark web.[135] For example, the hackers responsible for the attack on Western Digital threatened to publish the data they stole if Western Digital did not respond to their communications.[136] (See pullout box on **Western Digital**.)

This shift in focus has caused ransomware attacks to be even more harmful to consumers, as their data has been exposed more often. A study looking at ransomware attacks in the healthcare sector from 2016 through 2021 found that cybercriminals became more likely to expose sensitive personal health information.[137]

Western Digital

Who was targeted?

Western Digital is a California-based computer drive manufacturer and data storage company with around 300 million customers.[138] Hackers gained access to its systems and stole the personal information of the Western Digital online store's customers, reportedly over 10 terabytes of customer and company data in total. The hackers later requested a ransom of a "minimum 8 figures" in exchange for not publishing the stolen data.[136]

How did the breach occur?

In March 2023, a group of hackers exploited vulnerabilities within Western Digital's infrastructure to gain access to the company's systems, steal the information in its online store's database, and obtain its code signing certificates, giving hackers the ability to impersonate Western Digital staff. Hackers later leaked private information related to Western Digital's incident response to the dark web, demonstrating that they had continued access to its servers even weeks after the company identified the breach.[136,139,140,141]

How were consumers impacted?

Hackers were able to access a Western Digital database containing sensitive information of online store customers, including names, phone numbers, shipping and billing addresses, and email addresses. Hackers also stole customers' partial credit card numbers and password data.[141]

In addition, Western Digital shut down its cloud storage services, My Cloud, for two weeks, and its online store for over one month after the attack. During this time, customers lost their access to all cloud-hosted files and were unable to make any online purchases.[140,141,142]

The role of cybersecurity insurance and its cost to society

Cybersecurity insurance is a common tool that organizations rely on to protect themselves from monetary and legal risk from ransomware and other cybersecurity attacks. In a 2022 survey of business leaders in the US and Canada, nearly half reported that their organizations had purchased cybersecurity insurance.[149] The cost of cybersecurity measures, including insurance, is another expense for firms, which can affect consumers through higher prices.

Cybersecurity insurance has also created perverse incentives, as some hackers target insured organizations specifically because they are often more likely to pay a ransom. However, paying a ransom does not ensure that cybercriminals will not leak the victims' data.[150]

The International Counter Ransomware Initiative, a US-led initiative that includes over 30 countries,[151] is considering a ban on ransomware payments to reduce the incentives of cybercriminals.[152]

Even if organizations pay the required ransom, that is often not enough to protect consumers, as there is no guarantee that bad actors won't still use that data for nefarious purposes. In fact, in recent years, hackers have been more likely to leak data even after receiving a ransom, a phenomenon described as "double extortion."[135,136,137] This trend has led regulatory authorities, including the FBI, to warn organizations not to pay ransoms.[143] (See sidebar for a discussion of **The role of cybersecurity insurance and its cost to society**.)

In addition, cybercriminals have developed more sophisticated techniques that have helped them to become faster and more aggressive. Over the last few years, hackers have also become more organized, relying on more efficient organizational structures, higher budgets, and more sophisticated tools, including generative AI.[144] This has led to an increase in cybercriminal groups specializing in ransomware attacks, known as ransomware gangs. (See pullout box for **Examples of ransomware gangs**.) Ransomware gangs behave like major enterprises, crafting a public web presence, offering customer service, and offering franchising opportunities by renting out ransomware software.[145] Ransomware gangs also frequently target the same victim multiple times in a short period with different ransomware variants to further exploit their weakened defenses, a type of attack known as "dual ransomware attacks." The FBI has recently warned organizations about the rise of these attacks, reflecting the gravity of the threat.[146]

As a way of gaining access to target organizations, ransomware gangs have more frequently and aggressively targeted individuals inside an organization. For example, some ransomware gangs rely on communications with technical personnel within the organization to deceive them into giving up credentials or granting access to protected systems. In fact, ransomware gangs now increasingly resort to aggressive tactics during these communications, including violent threats toward these personnel or their families.[147,148]

Examples of ransomware gangs

LockBit, one of the most prolific ransomware gangs, was behind 28% of all known ransomware attacks between July 2022 and June 2023.[153] For instance, LockBit attacked Boeing in October 2023 and leaked at least 50 gigabytes of Boeing's sensitive company data on its leak site, including financial data.[154] Since 2020, LockBit has used its own data leak site on the dark web to double extort its victims.[155]

The **ALPHV/BlackCat** ransomware group claimed responsibility for several high-profile ransomware attacks in 2023.[156,157] For example, it was responsible for the attack on Barts Health NHS Trust, from which it claims to have stolen 70 terabytes of sensitive data, including employee identification documents such as passports and driver licenses, and internal emails labeled "confidential."[158]

Clop, one of the most active ransomware gangs, accounted for over a third of all ransomware attacks in July 2023[159] and 10% of victim organizations in the first half of 2023.[160] Clop was responsible for the MOVEit data breach campaign, which has impacted over 65 million individuals.[161,162]

Vendor exploitation: Attacking the security flaws of vendors

KEY TAKEAWAYS

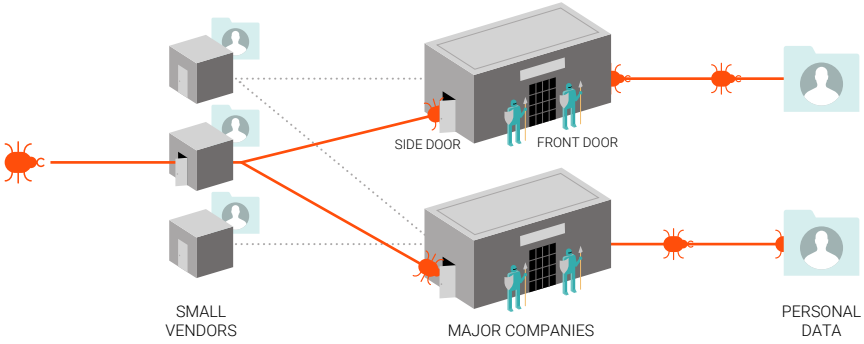
- **Vendor exploitation attacks allow hackers to target organizations that rely on vendors with security vulnerabilities.**
- **98% of organizations have a relationship with a vendor that experienced a data breach in the last two years.**[13]
- **Vendor exploitation attacks can have particularly broad consequences, as a single vulnerability in the software of one vendor may allow hackers to breach the personal data of any organizations that rely on this software or vendor, which could number in the thousands or more.**[11]

Corporations and institutions increasingly rely on third-party software and vendors for their daily operations, including accounting software, technical software, and file transfer or security services. Once these software packages are installed in an organization's systems, they often provide vendors with unfettered access (through a "side door") to the organization's network so that they can provide services such as software updates.

In many cases, these vendors are small- or medium-sized companies that are not able to devote the resources to security that larger organizations often can. However, any security vulnerability in software or a vendor's system has the potential to become a vulnerability for the organizations that rely on it. Bad actors are increasingly targeting vendors to bypass the larger organizations' own security (the "front doors"), allowing them to quickly and effectively access data either stored by the organizations that rely on the vulnerable software or stored by the vendors themselves. (See sidebar for **Examples of attacks on vendors with security flaws**.)

Vendor exploitation attacks can impact virtually all organizations; even those with the strongest security measures can be exposed. In fact, 98% of organizations have a relationship with a vendor that experienced a data breach in the last two years.[13]

Attacker exploits vulnerability in a vendor and gains access to personal data on many company systems that rely on that vendor.



Examples of attacks on vendors with security flaws

Capita, a UK company that administers over 450 pension plans, was breached by a ransomware group in March 2023.[163,164] Hackers stole clients' pension data from Capita servers, including bank accounts, passport, and retirement information.[163] In May 2023, Capita suffered a second data breach as a result of a cloud misconfiguration that exposed benefit data to the public.[165,166] Over 90 organizations have reported breaches of personal and pension data as a result, affecting customer data for renowned UK brands like Marks & Spencer, Unilever, and Rothesay.[165,167]

GoAnywhere, a file transfer software, was breached by the Clop ransomware group in January 2023. Hackers exploited GoAnywhere's vulnerability to breach the networks of more than 130 organizations all over the world that use it as a third-party file-sharing vendor, including the City of Toronto, Crown Resorts in Australia, Saks Fifth Avenue in the US, and Virgin Red in the UK.[168,169]

3CX, a Cyprus-based communications software maker, had its systems hacked through an insider threat. As a result, its app was also compromised, potentially exposing the corporate and personal data of the 12 million daily users and over 600,000 organizations worldwide that rely on it, including Coca-Cola, BMW, and Air France.[170,171,172,173]

Latitude Financial Services, an Australian personal loan and financial services provider, suffered a data breach through a vendor exploitation attack in March 2023 that exposed around 14 million customers' data, including driver's license, passport, and financial information. Cybercriminals stole Latitude login credentials during an attack on one of Latitude's vendors.[36,133,174]

Vendor exploitation attacks often have broad ripple effects. As the initial attack allows hackers to gain access to the vendor's system and data, it may also allow hackers to access the systems and data of that vendor's clients. This is precisely what happened with the campaign targeting flaws in MOVEit, a widely used file transfer service,[175] and in GoAnywhere, a popular managed file transfer service.[176] In both cases, an unpatched vulnerability allowed hackers to compromise the data of organizations that relied on those two vendors and steal sensitive information from their customers.

These vendor exploitation attacks can have particularly broad consequences, as a single vulnerability in one vendor's software may allow hackers to gain access to the personal data of the many organizations it serves across the globe. For example, schools in 140 countries over the world rely on ClassPad, an education platform developed by the Japanese electronics manufacturer Casio. Earlier this year, when hackers breached Casio and the servers of ClassPad, they were able to access the names, email addresses, and purchase information for the students at over 1,100 educational institutions.[177]

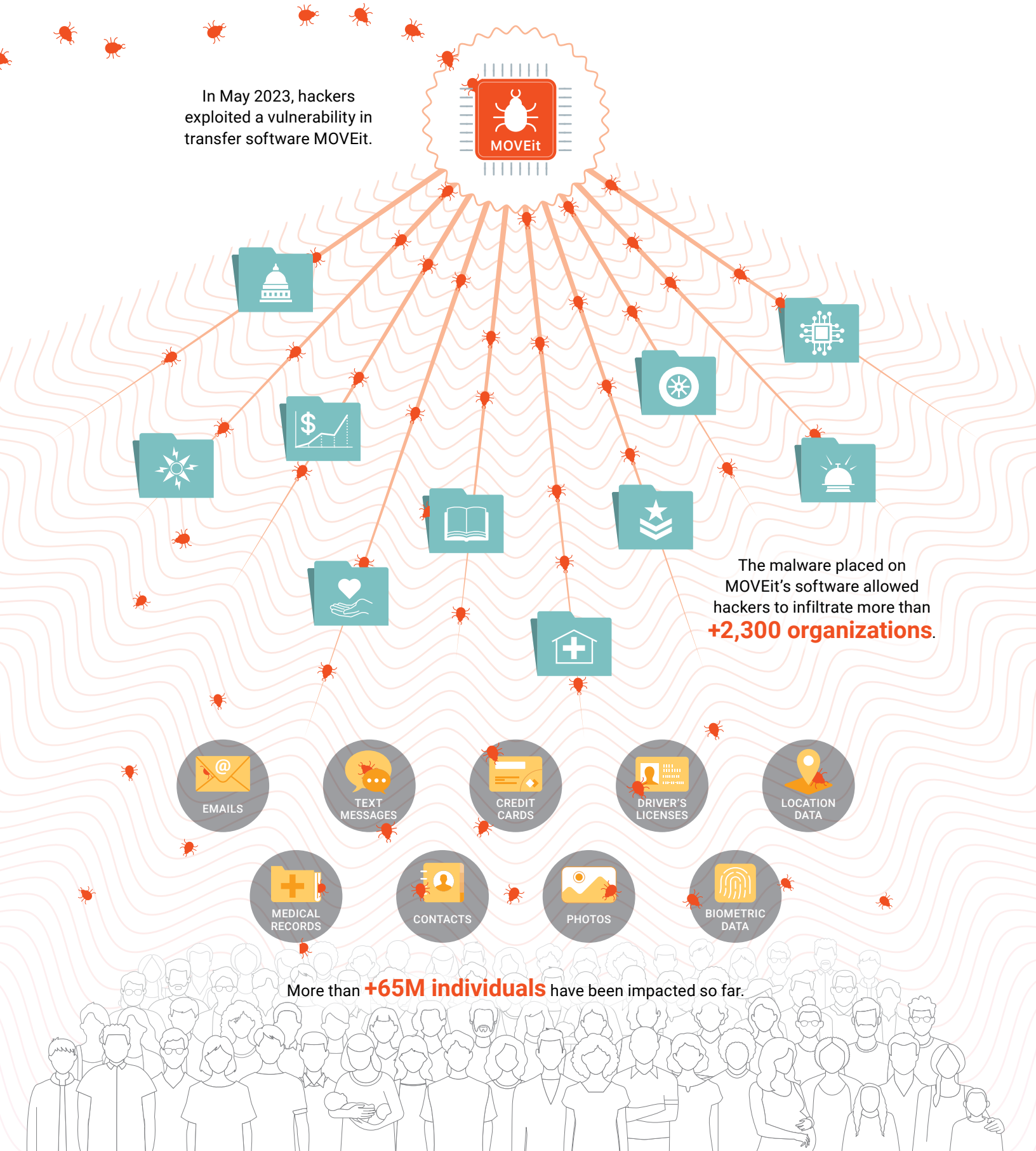
Microsoft

Even software vendors with sophisticated security are often unable to avoid data breaches. In 2023, multiple cyberattacks affecting Microsoft consumers, employees, and government entities were reported. In response, Microsoft has launched a new initiative to advance cybersecurity protection, Secure Future Initiative.[178] Recent attacks on Microsoft included:

- **Microsoft Outlook:** In May 2023, the account of a Microsoft engineer was hacked by sophisticated cybercriminals who acquired a key to access Outlook accounts of approximately 25 high-profile organizations, including the US State and Commerce departments.[73,179] Over 60,000 emails were stolen from 10 US State Department email accounts, and the hackers were able to access the email account of US Commerce Secretary Gina Raimondo.[73,74]
- **Microsoft Exchange:** In August 2023, the UK Electoral Commission reported that hackers exposed over 40 million voters' personal information due to a zero-day vulnerability in Microsoft Exchange.[180,181] Hackers first accessed the UK Electoral Commissions' systems in August 2021, and the Commission first identified suspicious activity in October 2022.[182] The attack led hackers to access the Electoral Commission's email, control systems, and obtain copies of the electoral registers, and it may have affected anyone who registered to vote in the UK between 2014 and 2022, as well as those registered as overseas voters.[183]
- **Microsoft AI:** TechCrunch reported in September 2023 that Microsoft AI's research division exposed over 38 terabytes of sensitive information due to a cloud misconfiguration, including passwords to Microsoft services, secret keys, and more than 30,000 internal Microsoft Teams messages from hundreds of Microsoft employees.[184]

MOVEit

In May 2023, hackers exploited a vulnerability in transfer software MOVEit.



The malware placed on MOVEit's software allowed hackers to infiltrate more than **+2,300 organizations**.

More than **+65M individuals** have been impacted so far.

MOVEit

Who was targeted?

MOVEit is a popular file transfer software that helps organizations transfer large amounts of often sensitive files and data over the internet. Thousands of organizations in the public and private sectors around the world rely on MOVEit to transfer files and data.[185] Hackers discovered a vulnerability in MOVEit that allowed them to infiltrate MOVEit's web application. As of October 2023, the MOVEit hack has affected at least 2,300 known organizations and more than 65 million individuals, for a global cost of more than $10 billion.[185,186] Given that only a fraction of the impacted organizations publicly reported the breach, the actual number of victims is estimated to be far larger. The attack is currently being investigated by the SEC.[162,187]

How did the breach occur?

In May 2023, a ransomware and extortion group called Clop (sometimes written as CL0P) gained access to data in corporate and institutional networks around the world by exploiting a zero-day vulnerability in the MOVEit software (i.e., a vulnerability that had not been previously discussed, thus not yet patched) that allowed hackers to raid the customer data in the MOVEit Transfer servers.[162] Through that vulnerability, Clop hackers emplaced web shells on MOVEit Transfer web applications to target MOVEit's downstream clients.[161,188] By exploiting this vulnerability, hackers were able to extract sensitive files from thousands of organizations that rely on this software.

How were other organizations impacted?

That flaw in the MOVEit software set off a massive worldwide data breach, with more than 2,300 public and private entities across 30 countries impacted.[186] Many victims of the MOVEit hack were compromised via third parties, subcontractors, or vendors that relied on this software.[189] Some notable organizations impacted include:[187,190]

Government entities and contractors: The Department of Justice (US), the Department of Energy (US), the Louisiana Office of Motor Vehicles (US), Maximus (US), BORN Ontario (Canada), the Government of Nova Scotia (Canada), Transport for London (UK), the Health Service Executive (Ireland), the Austrian Financial Market Authority (Austria)

Financial institutions: 1st Source Bank (US), First National Bankers Bank (US), Deutsche Bank (Germany), Comdirect Bank (Germany), Brookfield Asset Management (Canada), Kotak Life Insurance (India)

Public institutions: Nearly 900 universities and colleges, including the University of California, Los Angeles (US); the University of Missouri (US); the University of Georgia (US); and University College London (UK)[191,192]

Private companies: Shell (UK), Siemens Energy (Germany), IBM (US), Radisson Hotels (US), British Airways (UK), Aer Lingus (Ireland), PWC (UK), Sony (Japan), Landal GreenParks (Netherlands), Marti Group (Switzerland), Welltok (US)

How were consumers impacted?

More than 65 million consumers are known to have been impacted as a result of this campaign. Some notable examples of the data exposed include:

Medical records: Through IBM, more than 4 million Colorado residents' health information, including names, dates of birth, health insurance, and clinical and medical data, was exposed.[193] Similarly, hackers stole pregnancy, birth, and newborn care data for 3.4 million people, including 2 million infants, from Ontario's government birth registry, BORN Ontario.[65,194]

Financial information: Financial customer data breached included International Banking Account Numbers (IBANs) from customers at Deutsche Bank and its retail banking division, Postbank.[195]

Employee information: Hackers downloaded personal information (e.g., name, address, and employee ID number) belonging to employees of Gen Digital, a multinational software company that owns the popular antivirus software Norton, Sony, and Shell's Australian unit BG Group, exposing employees to identity theft and phishing attacks.[55,196,197]

Conclusion: Innovative solutions to protect consumer data

Data breach victims suffer real-life consequences

A data breach of the UK's Metropolitan Police Service exposed personal identifiable information of over a thousand victims and witnesses of sexual offenses and domestic assaults. Victims of sexual offenses thereby lost their lifelong guarantee of anonymity under law.[202]

A three-year-old boy hospitalized in Iowa was given five times his prescribed dose of opioids due to a manual error after the hospital's computer systems were shut down after a ransomware attack.[203]

Many customers of CloudNordic and AzeroCloud, two Danish cloud hosting firms, permanently lost their data, including websites, email inboxes, and documents, due to a ransomware attack in August 2023.[204]

A data breach of 168 million Indian citizens in March 2023 had serious national security implications, exposing the sensitive information of many defense personnel, including their ranks and postings.[205]

Five hospitals in Ontario had to reschedule and postpone surgeries after their shared IT provider was attacked in October 2023.[206]

An attack on the UK's Royal Mail left customers at more than ten thousand UK post offices without international mail services for over a month.[207]

KEY TAKEAWAYS

- **Given the prevalence of data breaches and their real-life consequences for individuals, keeping personal data safe should be at the forefront of organizations' priorities.**
- **Cyberattacks have proven that organizations are only as secure as their "least secure link." In this landscape, no organization, and, by extension, no individual, is safe from a data breach.**
- **This is why, in the last year, technology platforms and other industry players have expanded their use of end-to-end encryption, a method of securing data or communications by scrambling them into unreadable data so that third parties cannot read it.**

As long as organizations worldwide continue to store troves of valuable personal data in unencrypted form in the cloud, individuals remain at risk of having their personal data stolen, exploited, and exposed. Beyond a loss in privacy, breaches can have significant real-life consequences for victims, often through financial loss, identity theft, or follow-on attacks that leverage the stolen data. (See sidebar for a discussion of **Data breach victims suffer real-life consequences**.) Individuals can also be affected by data breaches indirectly — for instance, when an attack forces an organization on which they rely to shut down its operations. For example, Prospect Medical Holdings, a healthcare provider with hospitals and clinics in several states, including California and Texas, had to shut down some of its services, including its emergency departments, after a cyberattack disrupted its computer systems.[198,199] In another example, a ransomware attack targeting multiple government ministries in Colombia forced the country's Supreme Court to suspend all hearings for a week.[200]

On many occasions, individuals need to rely on organizations to safeguard their best interests, particularly when they have little choice but to share sensitive data. When an individual wants to obtain a driver's license from the DMV, register to vote at their local government office, or buy a plane ticket to a different country from an airline, they must share sensitive and personal information with these entities, such as their name, race, address, and passport number. As governments have frequently been the target of cyberattacks, consumers are losing confidence in how governments protect their data.[201] Given the prevalence of data breaches and their real-life consequences on individuals, keeping personal data safe should be at the forefront of these organizations' priorities.

And yet, even as the urgency to protect individuals has increased, most organizations around the world are still falling short. Recent trends continue to show that inventive hackers are becoming more sophisticated and aggressive. Ransomware attacks are at an all-time high, and ransomware gangs are increasingly targeting organizations that hold the most sensitive personal data. Additionally, as shown by the campaigns targeting MOVEit and GoAnywhere, a single vulnerability in a vendor's system can put hundreds or even thousands of organizations and their

users at risk. These incidents have, time and again, proven that organizations are only as secure as their "least secure link." In this landscape, no organization, and, by extension, no individual, is safe from a data breach.

This is why organizations must rethink the amount of data they collect and, especially, limit the amount of unencrypted consumer data they retain. It's also why, in the last year, technology platforms and other industry players have expanded their use of end-to-end encryption, a method of securing data or communications that ensures only the sender and receiver can access and modify that data. (See pullout box on **End-to-end encryption as a tool to protect consumer data**.) For example, Apple introduced Advanced Data Protection worldwide in January 2023, which included end-to-end encryption as well as other security measures for the majority of users' iCloud data, including iCloud Backup and Photos.[14] This and other innovative solutions are necessary to protect consumers and keep their personal data safe.

End-to-end encryption as a tool to protect consumer data

Limiting the amount of readable consumer data retained by organizations is one of the most effective ways to protect consumers. **End-to-end encryption,** a type of encryption that ensures only the sender and receiver of the data can access and modify data, is one method used by companies to protect their data. In 2023, most technology companies have implemented and expanded end-to-end encryption, or planned to do so, as one solution to protect consumers and their data.

- **Apple**: In 2011, iMessage was the first widely available messaging service to provide end-to-end encryption by default.[208] Apple broadened its use of end-to-end encryption by rolling out **Advanced Data Protection for iCloud** in December 2022 in the US, and worldwide starting in January 2023. This user security feature uses end-to-end encryption to provide the highest levels of security to consumers to protect their data in the cloud. Consumers can turn on this feature to encrypt their sensitive data and communications so that no one but the consumer – not even Apple – can access their iCloud data.[14,209]
- **Google**: In February 2023, Google expanded client-side encryption (CSE) to include additional Google Workspace products such as Gmail and Calendar.[210]
- **Meta**: Meta plans to launch end-to-end encryption as a default for Messenger by the end of 2023[211] and for Instagram chats shortly afterward.[212] WhatsApp messages are already end-to-end encrypted by default.[213]
- **Proton Mail**: Proton Mail uses client-side encryption and automatically end-to-end encrypts the emails between all of the 100 million Proton accounts.[214,215]
- **Signal**: Since its release for iPhone in 2014, messaging app Signal has offered end-to-end encryption for voice calls, later expanding to text-based messages.[216,217,218]
- **Skiff**: Launched in 2022 with the aim of building a privacy-first workspace, Skiff provides a suite of workspace tools including email, calendar, notes, and cloud storage, all end-to-end encrypted.[219]

Notes

A. The 2023 Verizon Data Breach Investigations Report (DBIR) doesn't report the number of personal records breached as a result of data breaches in 2022. In this absence, this statistic was calculated by applying the growth rate of the personal records breached between 2021 and 2022 using the Vocabulary for Event Recording and Incident Sharing (VERIS) Community Database to the number of personal records breached in 2021 as reported in the 2022 Verizon DBIR. The VERIS database was filtered consistent with its use in the Verizon DBIR series. In particular, the dataset was filtered to include observations where (i) the incident occurred between November 1, 2020, and October 31, 2021 ("2021 breaches"), or between November 1, 2021, and October 31, 2022 ("2022 data breaches"), (ii) the incident resulted in the confirmed disclosure of data to an unauthorized party, (iii) an incident was a confirmed security incident, defined as a loss of confidentiality, integrity, or availability, and (iv) the incident is categorized under at least one VERIS threat action. Once these filters were imposed, the growth rate of the total personal records breached from 2022 to 2021 was calculated by dividing the difference between the total number of personal records breached in 2022 data breaches and the total number of personal records breached in 2021 data breaches by the total number of records breached in 2021 data breaches. This growth rate was applied to the number of personal records breached in 2021 as reported in the 2022 Verizon DBIR.

B. US institutions in the healthcare sector are required to report data breaches that expose data of over 500 individuals. As a result, breaches in the US healthcare sector are a reliable benchmark for broader trends.

C. Surfshark does not report the total number of breached accounts in the UK, Australia, and Canada combined in the first half of 2023 and the first half of 2022 in one report. For the first half of 2023, the number of breached accounts combined across the UK, Australia, and Canada was calculated as the sum of breached accounts in the UK, Australia, and Canada in Q1 and Q2 of 2023, according to Surfshark's 2023 report comparing Q1 2023 to Q4 2022 and its 2023 midpoint report describing Q2 2023. Similarly, for the first half of 2022, the number of breached accounts combined across the UK, Australia, and Canada was calculated as the sum of the number of breached accounts in each country in Q1 and Q2 of 2022, according to Surfshark's Q1 2022 report and its Q3 2022.

D. The description of the attack (e.g., Corporate Ransomware, Vendor Exploitation) describes the method hackers used to infiltrate the organization's network in that particular attack. In some cases, the description illustrates the new vectors created from this attack (e.g., Vendor Exploitation); in other cases, the description signifies the technology hackers used in the attack (e.g., Corporate Ransomware).

Sources

1. Sabin, Sam, "Hackers head to the cloud," *Axios*, March 7, 2023.
2. "2022 Data Breach Report," *Identity Theft Resource Center*.
3. "H1 2023 Data Breach Analysis: 2023 Data Compromises Are on a Blistering Pace to Set a New Record," *Identity Theft Resource Center*, June 30, 2023.
4. "Q3 2023 Data Breach Analysis: Record Smashed! How Many Data Breaches Will Be Reported In 2023?," *Identity Theft Resource Center*, October 11, 2023.
5. Knutsson, Kurt, "You won't believe how much money hackers get from stealing your data," *Fox News*, March 5, 2023.
6. Pitrelli, Monica, "Leaked documents show notorious ransomware group has an HR department, performance reviews and an 'employee of the month'," *CNBC*, April 13, 2022.
7. Vicens, AJ, "Ransomware gangs increasingly deploy zero-days to maximize attacks," *CyberScoop*, April 11, 2023.
8. Robertson, Jordan, "Hackers Are Finding Ways to Evade Latest Cybersecurity Tools," *Bloomberg*, April 27, 2023.
9. Corvus Threat Intel, "Q3 Ransomware Report: Global Ransomware Attacks Up More Than 95% Over 2022," *Corvus*, October 24, 2023.
10. Wrozek, Brian, Allie Mellen, et al., "Top Cybersecurity Threats In 2023," *Forrester*, April 16, 2023.
11. Satter, Raphael, and Zeba Siddiqui, "Analysis: MOVEit hack spawned over 600 breaches but is not done yet -cyber analysts," *Reuters*, April 8, 2023.
12. "More Lessons Learned from Analyzing 100 Data Breaches," *Imperva*, 2022.
13. Delano, Derek, "SecurityScorecard Research Shows 98% of Organizations Globally Have Relationships With At Least One Breached Third-Party," *SecurityScorecard*, February 1, 2022.
14. "Apple advances user security with powerful new data protections," *Apple*, December 7, 2022.
15. Mayorkas, Alejandro N., "Threats to the Homeland," *US Department of Homeland Security*, October 31, 2023.
16. "Notorious phishing platform shut down, arrests in international police operation," *Interpol*, August 8, 2023.
17. Wray, Christopher, "Director Wray's Remarks at the 2023 Homeland Security Symposium and Expo," *Federal Bureau of Investigation*, February 16, 2023.
18. Martin, Alexander, "Don't focus on ransomware variants, say UK's national cyber and crime agencies," *The Record*, September 11, 2023.
19. Verizon Cyber Security Consulting Research (DBIR), https://github.com/vz-risk/VCDB.
20. "VERIS: The Vocabulary for Event Recording and Incident Sharing," *The VERIS Framework*.
21. "Data Breach Investigations Report," *Verizon*, 2023.
22. "Data Breach Investigations Report," *Verizon*, 2014-2022.
23. "IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs," *IBM*, July 24, 2023.
24. IBM Security, "Cost of a Data Breach Report 2023," *IBM*.
25. Dubuis-Welch, Camille, Rachel Sadler, et al., "Live company data breaches and stats for 2023," *Independent Advisor*, September 6, 2023.
26. Ngila, Faustine, "One in four Americans have had their health data compromised this year," *Quartz*, October 20, 2023.
27. S., William, "Patient data breaches doubled, reaching 87M in 2023," *Atlas VPN*, October 18, 2023.
28. "2023 Ransomware Attacks: Trends and Countermeasures," *Specialized Technical Services*.
29. Shryock, Todd, "Patient data breaches doubled in 2023," *Medical Economics*, October 23, 2023.
30. "Data Breaches: In the Healthcare Sector," *Center for Internet Security*.
31. "Data breach statistics 2023'Q1 vs. 2022'Q4," *Surfshark*, May 10, 2023.
32. "Data breaches rise globally in Q3 of 2022," *Surfshark*, October 19, 2022.
33. "Data breaches ramped up globally as 2023 reaches midpoint," *Surfshark*, August 1, 2023.
34. "Data breach statistics by country: first quarter of 2022," *Surfshark*, April 13, 2022.
35. Martin, Alexander, "Cyber incident reports hit 'all-time high,' warns UK NCSC," *The Record*, November 13, 2023.
36. Kost, Edward, "13 Biggest Data Breaches in Australia [Updated 2023]," *UpGuard*, August 4, 2023.
37. Australian Cyber Security Centre, "ASD Cyber Threat Report 2022-2023," *Australian Signals Directorate*.
38. "The Future of the Data Storage Market," *Open-E*, 2022.
39. "2023 Global Threat Report," *Crowdstrike*.
40. Powell, Olivia, "Discord.io exposes personal data of more than 760,000 users," *Cyber Security Hub*, August 18, 2023.
41. Whittaker, Zack, "Forever 21 data breach affects half a million people," *TechCrunch*, August 31, 2023.
42. Page, Carly, "MGM Resorts blames 'cybersecurity issue' for ongoing outage," *TechCrunch*, September 11, 2023.
43. Page, Carly, "MGM Resorts confirms hackers stole customers' personal data during cyberattack," *TechCrunch*, October 6, 2023.
44. Turton, William, Christopher Palmeri, et al., "MGM and Caesars Hacked by Same Group in Span of a Few Weeks," *Bloomberg*, September 13, 2023.
45. "MGM Resorts Destinations," *MGM*.
46. "Why Are Businesses Moving the the Cloud?," *Westlake*, May 9, 2022.
47. Elgan, Mike, "Why are cloud misconfigurations still a major issue?," *Security Intelligence*, November 1, 2022.
48. "Mitigating Cloud Vulnerabilities," *National Security Agency (Cybersecurity Information)*, January 22, 2020.
49. Gatlan, Segiu, "GoDaddy: Hackers stole source code, installed malware in multi-year breach," *Bleeping Computer*, February 17, 2023.
50. Vijayan, Jai, "GoDaddy Breach Exposes SSL Keys of Managed WordPress Hosting Customers," *Dark Reading*, November 22, 2023.
51. Gatlan, Sergiu, "T-Mobile discloses second data breach since the start of 2023," *Bleeping Computer*, May 1, 2023.
52. Toulas, Bill, "Third Flagstar Bank data breach since 2021 affects 800,000 customers," *Bleeping Computer*, October 8, 2023.
53. "About Flagstar," *Flagstar Bank*.
54. Kovacs, Eduard, "Sony Confirms Data Stolen in Two Recent Hacker Attacks," *Security Week*, October 5, 2023.

55. Toulas, Bill, "Sony confirms data breach impacting thousands in the U.S.," *Bleeping Computer*, October 4, 2023.

56. Hope, Alicia, "Toyota Connected Service Decade-Long Data Leak Exposed 2.15 Million Customers," *CPO Magazine*, May 19, 2023.

57. Bîzgă, Alina, "Leaky database at India-based social media app Slick exposes personal info of kids online," *Bitdefender*, February 13, 2023.

58. Singh, Jagmeet, "Indian social media app Slick exposed childrens' user data," *TechCrunch*, February 10, 2023.

59. "Egypt: Data of Tens of Thousands of Students Compromised," *Human Rights Watch*, April 19, 2023.

60. Hunter, Tatum, "Worried about the 23andMe hack? Here's what you can do.," *The Washington Post*, October 13, 2023.

61. Murphy, Margi, "Hacker Puts 23andMe User Data Up for Sale on the Internet," *Bloomberg*, October 6, 2023.

62. Franceschi-Bicchierai, Lorenzo, "Hacker leaks millions more 23andMe user records on cybercrime forum," *TechCrunch*, October 18, 2023.

63. Bajak, Frank, Heather Hollingsworth, et al., "Ransomware criminals are dumping kids' private files online after school hacks," *Associated Press*, July 5, 2023.

64. Sharma, Ax, "SickKids impacted by BORN Ontario data breach that hit 3.4 million," *Bleeping Computer*, September 26, 2023.

65. Dangerfield, Katie, "BORN Ontario data breach left health data of millions exposed. What went wrong?," *Global News*, September 26, 2023.

66. McGreevy, Ronan, and Vivienne Clarke, "Sex abuse survivors' charity One in Four victim of data breach," *The Irish Times*, April 17, 2023.

67. "City of Oakland Targeted by Ransomware Attack, Work Continues to Secure and Restore Services Safely," *City of Oakland*, April 4, 2023.

68. BondGraham, Darwin, "Oakland ransomware hackers dumped gigabytes of sensitive city files on the web," *The Oaklandside*, March 6, 2023.

69. BondGraham, Darwin, "Hackers leaked a second, larger set of stolen city files on the dark web," *The Oaklandside*, April 5, 2023.

70. "Authorities dealt with leak of data for 2 million Egyptian patients: Health minister," *Ahram Online*, August 2, 2023.

71. Poireault, Kevin, "Hacker Claims to Have Stolen Sensitive Medical Records from Egypt's Ministry of Health," *Infosecurity Magazine*, July 25, 2023.

72. O'Sullivan, Kevin, and Simon Murphy, "Russia linked hackers hit UK Ministry of Defence as security secrets leaked," *The Mirror*, September 2, 2023.

73. Barr, Luke, "Commerce Secretary Gina Raimondo's emails hacked in Microsoft cyber breach," *ABC News*, July 12, 2023.

74. Satter, Raphael, and Zeba Siddiqui, "Chinese hackers stole emails from US State Dept in Microsoft breach, Senate staffer says," *Reuters*, September 27, 2023.

75. "CMS Responding to Data Breach at Contractor," *Centers for Medicare & Medicaid Services*, July 28, 2023.

76. Muncaster, Phil, "Brazilian Conglomerate Suffers 3TB Data Breach: Report," *Infosecurity Magazine*, March 7, 2023.

77. "Nearly 1.5 million affected by data breach at Alberta Dental Service Corporation," *CBC News*, August 10, 2023.

78. "LATAM Data Breaches: Top 3 Countries Affected," *Kiuwan*, March 14, 2023.

79. Ivanova, Irina, "HCA Healthcare says hackers stole data on 11 million patients," *CBS News*, July 11, 2023.

80. Alder, Steve, "Almost 6 Million Individuals Affected by PharMerica Data Breach," *The HIPAA Journal*, May 17, 2023.

81. Dissent, "El Salvadoran database raises questions of possible political intrigue," *DataBreaches.net*, August 21, 2023.

82. Toulas, Bill, "BORN Ontario child registry data breach affects 3.4 million people," *Bleeping Computer*, September 25, 2023.

83. Page, Carly, "Google Fi says hackers accessed customers' information," *TechCrunch*, January 31, 2023.

84. Toulas, Bill, "Welltok data breach exposes data of 8.5 million US patients," *Bleeping Computer*, November 22, 2023.

85. "Manipulated Caiman – 39,901,389 breached accounts," *RedPacket Security*, August 16, 2023.

86. Cowan, David, "Second site error left national records wide open," *BBC News*, August 17, 2023.

87. Abrams, Lawrence, "Play ransomware claims attack on Belgium city of Antwerp," *Bleeping Computer*, December 12, 2022.

88. Toulas, Bill, "Motel One discloses data breach following ransomware attack," *Bleeping Computer*, October 2, 2023.

89. "Air France-KLM's frequent flyer program hit by hackers in data breach," *NL Times*, January 9, 2023."

90. Toulas, Bill, "Hospital Clínic de Barcelona severely impacted by ransomware attack," *Bleeping Computer*, March 7, 2023.

91. Carames, Jesus, "Euskaltel: 3,1 T of confidential information compromised by the most harmful Ransomware," *Bilbaohiria*, May 18, 2023.

92. Proctor, Emily, "Hackers hold Swiss media to ransom, threatening 800GB data leak," *I Am Expat*, May 5, 2023.

93. Toulas, Bill, "Data breach at French govt agency exposes info of 10 million people," *Bleeping Computer*, August 25, 2023.

94. "Blauw breach now affects 1.5M people," *iapp*, March 31, 2023.

95. Mason, Rowena, and Hibaq Farah, "Electoral Commission apologises for security breach involving UK voters' data," *The Guardian*, August 8, 2023.

96. Page, Carly, "UK battles hacking wave as ransomware gang claims 'biggest ever' NHS breach," *TechCrunch*, July 10, 2023.

97. Clayton, Molly, Kevin O'Sullivan, et al., "Top stars are among hundreds of thousands of donors targeted in huge cyber attack on charities including the RSPCA and Battersea Dogs And Cats Home," *Daily Mail*, September 27, 2023.

98. Woollacott, Emma, "Hacktivists Breach Iranian Surveillance System," *Forbes*, July 29, 2023.

99. "Hacktivists Target Iran's Foreign Ministry, Leak Trove Of Data," *Volant Media*, May 7, 2023.

100. Venkat, Apurva, "Hackers attack Israel's Technion university, demand over $1.7 million in ransom," *CSO Online (Foundry)*, February 13, 2023.

101. Pandagle, Vishwa, "About 50GB of Ivory Coast Armed Forces Data on Sale," *The Cyber Express*, January 25, 2023.

102. Cybersecurity Analyst, "Adidas Morocco Hacked, 62k Clients Exposed," *KADUU*, December 15, 2023.

103. Vermeulen, Jan, "Interview with the hackers who broke into South Africa's Department of Defence," *My Broad Band*, August 30, 2023.

104. "Last Minute: e-Government data has been stolen! Even TR ID numbers are visible..." *Cumhuriyet*, September 6, 2023. (Translated)

105. "Public Announcement (Data Breach Notification) – Elca Kozmetik Limited Şirketi," *KİŞİSEL VERİLERİ KORUMA KURUMU*. (Translated)

106. Maombo, Sharon, "KAA confirms data breach, says no sensitive data leaked," *NTV Kenya*, April 12, 2023.

107. "Public Announcment (Data Breach Notification) – Hotiç Ayakkabı San. A.S.," *KİŞİSEL VERİLERİ KORUMA KURUMU*. (Translated)

108. Raywood, Dan, "Bangladesh Government Website Leaks Personal Data," *Informa Tech*, July 11, 2023.

109. Toulas, Bill, "Toyota: Car location data of 2 million customers exposed for ten years," *Bleeping Computer*, May 12, 2023.

110. Taylor, Josh, "Medibank hackers announce 'case closed' and dump huge data file on dark web," *The Guardian*, November 30, 2022.

111. Hope, Alicia, "Free VPN Data Leak Exposed Over 360 Million User Records," *CPO Magazine*, June 5, 2023.

112. Hamer, Lars, "Personal data, medical history of 100,000 patients may have been leaked in cyberattack at Hong Kong group OT&P Healthcare," *South China Morning Post*, May 8, 2023.

113. Grundy, Tom, "Hong Kong tech firm Sphero suffers massive, alleged data theft – details of a million students, educators leaked," *Hong Kong Free Press*, October 20, 2023.

114. Hope, Alicia, "34 million Indonesian Passports Exposed in a Massive Immigration Directorate Data Breach," *CPO Magazine*, April 13, 2023.

115. Chapman, Luke, "Auckland University of Technology Hacked by Monti Ransomware Gang, Data Breach Feared," *Thaiger*, September 22, 2023.

116. Kuzhanthaivel, Abbinaya, "PhilHealth estimates 13 to 20 million members affected by data breach," *iTnews Asia*, October 23, 2023.

117. Toulas, Bill, "Latitude Financial data breach now impacts 14 million customers," *Bleeping Computer*, March 28, 2023.

118. "Investigation underway into cyber attack which hit thousands of coronial and health files," *Radio New Zealand*, December 6, 2022.

119. "Most Impactful Ransomware Attacks of 2023," *BlackFog*, August 15, 2023.

120. "Cyber Threat Intelligence Report," *NCC Group*, September 2023.

121. "The State of Ransomware in Healthcare 2023," *Sophos*, August 2023.

122. "2023 State of the Threat," *Secureworks*.

123. "State of Ransomware Report," *BlackFog*, August 2023.

124. "State of Ransomware Report," *BlackFog*, September 2023.

125. "State of Ransomware Report," *BlackFog*, October 2023.

126. "More than 20,000 details 'at risk' after police data cyber attack," *BBC News*, September 18, 2023.

127. Page, Carly, "UK police officers' data stolen in cyberattack on ID supplier," *TechCrunch*, September 18, 2023.

128. "Worldwide Ransomware Activity October 2022-September 2023: Europe, North America, and Asia Among Top Targeted Regions," *Cyber Threat Intelligence Integration Center*, October 31, 2023.

129. "UK Ransomware Trends: 2023 Mid-year Update," *JUMPSEC*.

130. Canadian Centre for Cyber Security, "National Cyber Threat Assessment," *Government of Canada (Communications Security Establishment)*, 2022.

131. Canadian Centre for Cyber Security, "Baseline cyber threat assessment: Cybercrime," *Government of Canada*, August 28, 2023.

132. "Notifiable Data Breaches Report: January to June 2023," *Australian Government (Office of the Australian Information Commissioner)*, September 5, 2023.

133. Toulas, Bill, "Latitude cyberattack leads to data theft at two service providers," *Bleeping Computer*, March 16, 2023.

134. Burgess, Tony, "Ransomware today: Encryption waning, extortion on the rise," *Barracuda*, June 20, 2023.

135. Ellis, Jessica, "Ransomware Groups Break Promises, Leak Data Anyway," *Fortra PhishLabs*, November 25, 2020.

136. Franceschi-Bicchierai, Lorenzo, "Hackers claim vast access to Western Digital systems," *TechCrunch*, April 13, 2023.

137. Neprash, Hannah T., Claire C. McGlave, et al., "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021," *JAMA Health Forum*, Vol. 3, No. 12, December 29, 2022.

138. Sparrow, Mark, "Western Digital Announces New Products For Global Storage Markets," *Forbes*, May 9, 2022.

139. "Western Digital Provides Information on Network Security Incident," *Business Wire*, April 3, 2023.

140. Abrams, Lawrence, "Hackers leak images to taunt Western Digital's cyberattack response," *Bleeping Computer*, May 1, 2023.

141. "Western Digital Provides Update on Network Security Incident," *Western Digital*, May 5, 2023.

142. Crider, Michael, "Western Digital hacked: Your deeply personal data might be stolen," *PC World*, May 8, 2023.

143. Cybersecurity & Infrastructure Security Agency, National Security Agency, et al., "#StopRansomware Guide," *Multi-State Information Sharing & Analysis Center*, October 19, 2023.

144. "Global Threat Landscape Report (Semiannual)," *Fortinet*, August 7, 2023.

145. Steinberg, Sean, "Ransomware Goes to Business School," *Slate*, October 18, 2022.

146. "Two or More Ransomware Variants Impacting the Same Victims and Data Destruction Trends," *Federal Bureau of Investigation (Cyber Division)*, September 27, 2023.

147. Vicens, AJ, "Hackers that breached Las Vegas casinos rely on violent threats, research shows," *CyberScoop*, October 25, 2023.

148. Cox, Joseph, "SIM Swappers Are Working Directly with Ransomware Gangs Now," *404 Media*, October 26, 2023.

149. Matthews, Les, Diego Szteinhendler, et al., "Securing the digital economy," *Mastercard*, March 2023.

150. Gura, David, "Companies May Be Flagging Themselves For Hackers By Buying Cybersecurity Insurance," *NPR*, July 15, 2023.

151. Department of Home Affairs, "Counter Ransomware Initiative," *Australian Government*.

152. Kapko, Matt, "White House considers ban on ransom payments, with caveats," *Cybersecurity Dive*, May 8, 2023.

153. "LockBit Ransomware: Inside the World's Most Active Ransomware Group," *Flashpoint*, July 20, 2023.

154. Petkauskas, Vilius, "Boeing breach: LockBit leaks 50 GB of data," *Cybernews*, November 10, 2023.

155. Abrams, Lawrence, "LockBit ransomware launches data leak site to double-extort victims," *Bleeping Computer*, September 16, 2020.

156. Taylor, Josh, "Australian law firm HWL Ebsworth hit by Russian-linked ransomware attack," *The Guardian*, May 1, 2023.

157. Quinlan, Kelly, "BlackCat ransomware group claims attack on Florida court system," *State Scoop*, October 10, 2023.

158. Bernardone, Leonard, "2.5 million affected by UK hospital cyber attack," *Information Age*, July 31, 2023.

159. "Cyber Threat Intelligence Report," *NCC Group*, July 2023.

160. Matsugaya, Shingo, "Lockbit, BlackCat, and Clop Prevail as Top RAAS Groups: Ransomware in 1H 2023," *Security News*, September 21, 2023.

161. "#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability," *Cybersecurity & Infrastructure Security Agency*, June 16, 2023.

162. Page, Carly, "MOVEit, the biggest hack of the year, by the numbers," *TechCrunch*, August 25, 2023.

163. "Capita data breaches 2023: Everything you need to know," *Higgs Newton Kenyon Solicitors*.

164. "Capita data breach carried out by Russian hackers could affect the data of millions," *Higgs Newton Kenyon Solicitors*.

165. Bateson, Simone, "The Capita data breach explained," *Verdict*, May 31, 2023.

166. Alabi, Leke Oso, Ian Smith, et al., "Capita hit by new data breach incident," *Financial Times*, May 17, 2023.

167. Cumbo, Josephine, Leke Oso Alabi, et al., "M&S and Diageo pension schemes hit by Capita cyber attack," *Financial Times*, May 19, 2023.

168. Sharma, Ax, "City of Toronto confirms data theft, Clop claims responsibility," *Bleeping Computer*, March 23, 2023.

169. Toulas, Bill, "Crown Resorts confirms ransom demand after GoAnywhere breach," *Bleeping Computer*, March 28, 2023.

170. Page, Carly, "3CX's supply chain attack was caused by… another supply chain attack," *TechCrunch*, April 20, 2023.

171. Greenberg, Andy, "The Huge 3CX Breach Was Actually 2 Linked Supply Chain Attacks," *WIRED*, April 20, 2023.

172. Lyngaas, Sean, "North Korean hackers breach software firm in significant cyberattack," *CNN Politics*, April 20, 2023.

173. "Leading 3CX Customers," *3CX*.

174. "Asx Announcement: Cybercrime update," *Latitude*, March 27, 2023.

175. Newman, Lily Hay, and Matt Burgess, "The Biggest Hack of 2023 Keeps Getting Bigger," *WIRED*, October 2, 2023.

176. Arghire, Ionut, "GoAnywhere Zero-Day Attack Hits Major Orgs," *Security Week*, March 27, 2023.

177. Gatlan, Sergiu, "Casio discloses data breach impacting customers in 149 countries," *Bleeping Computer*, October 19, 2023.

178. Smith, Brad, "A new world of security: Microsoft's Secure Future Initiative," *Microsoft*, November 2, 2023.

179. Goodin, Dan, "Microsoft finally explains cause of Azure breach: An engineer's account was hacked," *Ars Technica*, September 6, 2023.

180. Goodin, Dan, "How an unpatched Microsoft Exchange 0-day likely caused one of the UK's biggest hacks ever," *Ars Technica*, August 9, 2023.

181. Robinson, Dan, "Electoral Commission had internet-facing server with unpatched vuln," *The Register*, August 11, 2023.

182. "Public notification of cyber-attack on Electoral Commission systems," *The Electoral Commission*, August 8, 2023.

183. Page, Carly, "Electoral Commission hack exposed data of 40 million UK voters," *TechCrunch*, August 8, 2023.

184. Page, Carly, "Microsoft AI researchers accidentally exposed terabytes of internal sensitive data," *TechCrunch*, September 18, 2023.

185. Simas, Zach, "Unpacking the MOVEit Breach: Statistics and Analysis," *Emisoft Blog*, July 18, 2023.

186. Kondruss, Bert, "MOVEit hack victim list," *Kon Briefing*, November 16, 2023.

187. Page, Carly, "SEC is investigating MOVEit mass-hack, says Progress Software," *TechCrunch*, October 11, 2023.

188. Sussman, Bruce, "Clop Ransomware and the MOVEit Cyberattack: What to Know," *BlackBerry*, June 19, 2023.

189. Page, Carly, "The MOVEit mass hacks hold a valuable lesson for the software industry," *TechCrunch*, August 11, 2023.

190. "What we know about the MOVEit exploit and ransomware attacks," *BlackFog*, June 22, 2023.

191. Greig, Jonathan, "MOVEit fallout continues as National Student Clearinghouse says nearly 900 schools affected," *The Record*, September 25, 2023.

192. Dalrymple, Donna, "SAUL response to cyber incident and data breach," *University College London*, June 23, 2023.

193. Page, Carly, "Millions of Americans' health data stolen after MOVEit hackers targeted IBM," *TechCrunch*, August 14, 2023.

194. Whittaker, Zack, "Decade of newborn child registry data stolen in MOVEit mass-hack," *TechCrunch*, September 25, 2023.

195. Hope, Alicia, "MOVEit Data Breach Leaks Deutsche Bank, ING, Postbank, and Comdirect's Customer Data," *CPO Magazine*, July 19, 2023.

196. Arghire, Ionut, "Norton Parent Says Employee Data Stolen in MOVEit Ransomware Attack," *Security Week*, June 20, 2023.

197. Nair, Roushni, and Navya Mittal, "Shell says its Australian BG Group business hit by MOVEit breach," *Reuters*, September 15, 2023.

198. Eaton-Robb, Pat, "A cyberattack has disrupted hospitals and health care in several states," *AP News*, August 4, 2023.

199. Bruce, Giles, "Prospect Medical's 16 hospitals back online 40 days after cyberattack," *Becker's Health It*, September 13, 2023.

200. Greig, Jonathan, "Several Colombian government ministries hampered by ransomware attack," *The Record*, September 15, 2023.

201. "Social Media, Government and Media & Entertainment Companies Least Trusted by Consumers to Keep Personal Data Secure," *Thales*, October 4, 2022.

202. Scotter, Kate, "Norfolk and Suffolk police: Victims and witnesses hit by data breach," *BBC News*, August 15, 2023.

203. Guzman, Alyssa, "Des Moines hospital claims cyber-attack was to blame for boy, 3, being given 'MEGADOSE' of opioids while recovering from having his tonsils out," *Daily Mail*, October 13, 2022.

204. Toulas, Bill, "Hosting firm says it lost all customer data after ransomware attack," *Bleeping Computer*, August 23, 2023.

205. Press Trust of India, "In Massive Data Breach, Details Of 16.8 Crore Citizens Leaked, 7 Arrested," *NDTV*, March 23, 2023.

206. "Radiation care moved out of Windsor, international law enforcement working on cyberattack," *CBC News*, October 31, 2023.

207. "Royal Mail resumes overseas mail at post offices after cyber-attack," *BBC News*, February 21, 2023.

208. Apple Security Engineering and Architecture, "Advancing iMessage security: iMessage Contact Key Verification," *Apple*, October 27, 2023.

209. Klosowski, Thorin, "How to Enable Advanced Data Protection on iOS, and Why You Should," *Electronic Frontier Foundation*, May 17, 2023.

210. "Google Workspace expands data privacy controls to Gmail and Calendar with client-side encryption," *Google*, February 28, 2023.

211. Miranda, Melissa, "Expanding Features for End-to-End Encryption on Messenger," *Meta*, August 22, 2023.

212. Kelly, Makena, "Meta refreshes promise to roll out default end-to-end encryption in Messenger this year," *The Verge*, August 22, 2023.

213. "About end-to-end encryption," *WhatsApp Help Center*.

214. Martinoli, Marco, "What is end-to-end encryption and how does it work?," *Proton*, May 24, 2022.

215. Yen, Andy, "There are now over 100 million Proton Accounts," *Proton*, April 18, 2023.

216. "Signal 2.0: Private messaging comes to the iPhone," *Signal*, March 2, 2015.

217. "Free, Worldwide, Encrypted Phone Calls for iPhone," *Signal*, July 29, 2014.

218. Mimoso, Michael, "New Signal App Brings Encrypted Calling to iPhone," *Threat Post*, July 29, 2014.

219. Shrivastava, Rashi, "Encrypted Email Company Skiff Wants You To Sign Out Of Google Workspace Forever," *Forbes*, December 16, 2023.