



# 2023 ForgeRock Identity Breach Report

**IT ONLY TAKES  
ONE EXPOSED  
PASSWORD.**

To protect sensitive data, secure every  
identity across your business ecosystem.

# A Single Compromised Identity Can Put an Entire Organizational Ecosystem at Risk

Digital identities are often protected by usernames and passwords to help us access online accounts and services. But those credentials are prized by attackers who have various ways to acquire them, from phishing to keylogging to credential spraying to brute-force attacks and more. Or they simply buy them from the dark web. Once breached, an identity can be used as a stepping stone to infiltrate an organization.

Even if every employee is trained in security best practices, just one accidental click on a malicious link in a legitimate-looking email can open the door to an intruder. Accounts can be taken over, data stolen, and systems brought down. The results can be devastating and far-reaching for the organization, its customers, and other companies it shares data with. Still, from the intruder's standpoint, it only takes one compromised identity.

The fact that it only takes one breach to impact masses of people explains the statistics: one in three consumers globally has been the victim of a data breach.<sup>1</sup> No wonder consumers have become increasingly concerned about security — 78% of Americans are wary about doing business with a retailer that has experienced a breach.<sup>2</sup>

A cursory look at this year's data suggests possible improvements over previous years. The number of breached records reported in 2022 was the lowest in five years. By one measure, that number dropped by more than half: 1.5 billion in 2022 as opposed to an average of 3.9 billion over the past four years.

But looks can be deceiving. A closer analysis reveals that while the number of breached records is lower, the records stolen contain more highly sensitive identity data that can result in longer-term damage.

From 2018 to 2022, breached records containing a username and password or other credentials rose by more than 350%.<sup>3</sup> This increase highlights the central role that credentials belonging to an employee or other authorized user play in identity-related breaches.

During this period, the number of records containing protected health information (PHI) also rose by 160%. In 2022, attacks targeting organizations through third-party service providers accounted for 52% of all breaches, illustrating the interconnectedness of identities. Healthcare and education emerged as the most vulnerable industry sectors. From the picture the data paints, it's clear that we must manage workforce, customer, and third-party identities holistically — as compromising one identity often leads to serious breaches of another.

Using the most up-to-date breach information available, we've gathered the key insights regarding breaches that impacted consumers in 2022 and how the trends have played out over the past five years. We also share findings from other regions, including Australia, Germany, the United Kingdom (UK), and Singapore. You'll learn exactly why organizations need a no-compromise path to simple and safe online experiences and why adopting an identity and access management (IAM) solution helps to prevent data breaches, protect your brands, and preserve customer relationships.

## Eve Maler

ForgeRock Chief Technology Officer



Eve Maler is ForgeRock's CTO. She is a globally recognized strategist, innovator, and communicator on digital identity, security, privacy, and consent, and she is passionate about fostering thriving ecosystems and individual empowerment. She has 20+ years of experience innovating and leading standards, such as SAML and User-Managed Access (UMA), and has served as a Forrester Research security and risk analyst. She leads the ForgeRock Labs team investigating and prototyping innovative approaches to solving customers' identity challenges and driving ForgeRock's industry-standards leadership.



# Table of Contents

<b>A Single Compromised Identity Can Put an Entire Organizational Ecosystem at Risk</b> .....	2
<b>Introduction</b> .....	4
<b>Top Three Trends</b> .....	5
<b>Key Findings</b> .....	6
<b>Cost of Breaches</b> .....	8
<b>Top Attack Vectors</b> .....	9
<b>The Stolen Identity of a Single Authorized User Can Trigger a Massive Breach</b> .....	12
<b>Third-Party Breaches are a Growing Threat</b> .....	13
<b>Some Industries are More Resilient than Others</b> .....	15
<b>Regional Insights</b> .....	19
<b>Recommendations</b> .....	25
<b>How ForgeRock Helps</b> .....	27
<b>Conclusion</b> .....	27

# Introduction

This report has been compiled based on data from a variety of sources, including previous years' ForgeRock Consumer Identity Breach Reports and data from the 2022 Identity Theft Resource Center,<sup>4</sup> the IBM Ponemon report,<sup>5</sup> TechCrunch,<sup>6</sup> Databreaches.net,<sup>7</sup> HIPAA Journal,<sup>8</sup> and Top Class Actions.<sup>9</sup> The research behind this report includes the most up-to-date information on the cost of breaches, the number of breaches and records involved, types of data compromised, and the industries most targeted, covering 3,344 breaches reported in the U.S. in 2022. Note that some percentage calculations in charts may not add up exactly due to rounding.

This report focuses on confirmed breaches in which confidential data has been exposed and/or stolen, ranging from very small breaches to large caches of data that provide financial incentives to hackers to hold for ransom, sell on the dark web, or both. Many breaches that occurred as a result of third parties (vendors, suppliers, contractors, or other organizations) were researched to determine the root causes.

## Variations in reporting transparency and undercounting of data

Because reporting requirements differ among regions and industries, breached organizations self-report varying degrees of information about a breach's nature, scope, and timing. For example, GDPR requires a breach to be reported within 72 hours after discovery, but the HIPAA requirement demands reporting "without unreasonable delay" and no more than 50 days following discovery. There are no less than 140 state student privacy laws in the U.S. education sector.

Many organizations delay breach notifications. Our research for this report found that over 50 companies took over a year to notify customers, and one waited almost three years. In addition, almost 50% of breached organizations in 2022 could not determine the exact number of breached records, so they defaulted to reporting zero records.

A 2023 survey of 400 international cybersecurity professionals found that many have been told to keep a breach confidential when it should be reported.<sup>10</sup>



# Top Three Trends

## The stolen identity of a single authorized user can trigger a massive breach

A breach of at least one set of credentials belonging to an employee or other authorized user can grant attackers access to internal systems and sensitive data that can expose customer data. Breached records have included a steady increase in personally identifiable information (PII) over the past five years, with login credentials and protected health information (PHI) on the rise. Attackers can exploit stolen credentials repeatedly because many people use the same credentials for multiple accounts. PHI is valuable for financial fraud and can even be used to access prescription drugs.

## Third-party breaches are a growing threat

Attacks on third-party service providers have increased since first being reported by the Identity Theft Resource Center (ITRC) in 2021. Exploiting a vendor's weak security controls to gain access to all the organizations that the vendor serves can compromise far more records — with the potential for much more significant financial gain — than an attack on an individual organization ever could.

## Some industries are more resilient than others

While some industries have become more resilient, others remain vulnerable to attack. Financial services, government, and retail show fewer breaches due to the adoption of stronger authentication practices. Targeted attacks on third-party service providers in healthcare and education demonstrate the need to deepen cybersecurity practices across their ecosystems.



# Key Findings

The stolen identity of a single authorized user can trigger a massive breach

## 233%

Increase in U.S. breaches exposing user credentials compared to 2021. Credentials — username and password combinations — are attractive targets as they enable unauthorized access to sensitive systems, networks, and data.

## 72%

U.S. breaches that contained date of birth and Social Security Number (SSN), a 20% increase over 2021. SSNs are attractive targets because they are widely used to verify a person's identity, are difficult to change, and can be used to commit fraud.

## \$675

Cost per healthcare record in the U.S., compared to \$614 in 2021. Healthcare records containing date of birth and SSN are valuable, as they can be used to commit fraudulent claims for equipment, services, and prescriptions.

## 62.9M

User accounts in Germany that were compromised, and their identity data made public, in 2022.<sup>11</sup>

## 83%

Attacks on UK businesses due to phishing.<sup>12</sup>

## \$50M

Maximum penalty for Australian businesses experiencing serious or repeated privacy breaches.<sup>13</sup>



## Third-party breaches are a growing threat

**136%**

Increase in third-party breaches over 2021.

**52%**

Reported breaches that came through partners and suppliers.

**50%**

Partner breaches that resulted from unauthorized access.

**47%**

Breaches that involved ransomware.

## Some industries are more resilient than others

**67%**

Decrease in attacks on the U.S. retail sector.<sup>14</sup>

**29%**

Decrease in attacks on the U.S. financial services sector.

**50%**

Increase in breaches of the U.S. healthcare sector.

**36%**

U.S. breaches in 2022 impacting healthcare, which continues to be the most vulnerable of the 13 sectors reporting breaches in 2022.

**54%**

Increase in ransomware incidents in Singapore, impacting small and medium enterprises in manufacturing and information technology industries.<sup>15</sup>



# Cost of Breaches

---

The average cost of a breach in the United States has steadily increased over the past five years, making it the highest worldwide. In 2022, the cost of a U.S. breach reached \$9.4 million, compared to the global average of \$4.35 million. These costs include business loss, detection and escalation, notification, and post-breach response.

In addition to their substantial costs, U.S. breaches increased by 170% between 2021 and 2022. Moreover, the nature of breaches has changed, with a greater number of attacks attributed to third-party organizations that supply business-to-business (B2B) services.<sup>16</sup> Each third-party breach can impact dozens or even hundreds of organizations, including sectors such as education that were less frequently targeted in the past.

While the number of mega-breaches involving more than one million records changed little from 2021, there was a staggering 70% rise in smaller breaches. This trend serves as a clear warning to smaller companies that have assumed they were immune to attack: the era of feeling protected from such incidents is now over.

## Billions of dollars in class action lawsuit fines

A key reason for the high cost of breaches in 2022 was the surge in class action lawsuits, particularly those targeting organizations that experienced breaches involving fewer than a thousand records. These lawsuits can become exorbitant, with fines ranging from hundreds of millions to billions of dollars on a global scale.<sup>17</sup> Moreover, the European Union's General Data Protection Regulation (GDPR) fines alone amounted to €2.92 billion in 2022, more than double last year's figure of €1.1 billion.<sup>18</sup>

These rising legal implications highlight the burden faced by companies dealing with breaches, even when the number of compromised records is relatively small. It serves as a crucial reminder for smaller companies to recognize the potential financial repercussions and the importance of implementing strong cybersecurity measures. By prioritizing robust security protocols and proactive strategies, smaller companies can mitigate the risk of breaches and minimize the associated legal and financial consequences.

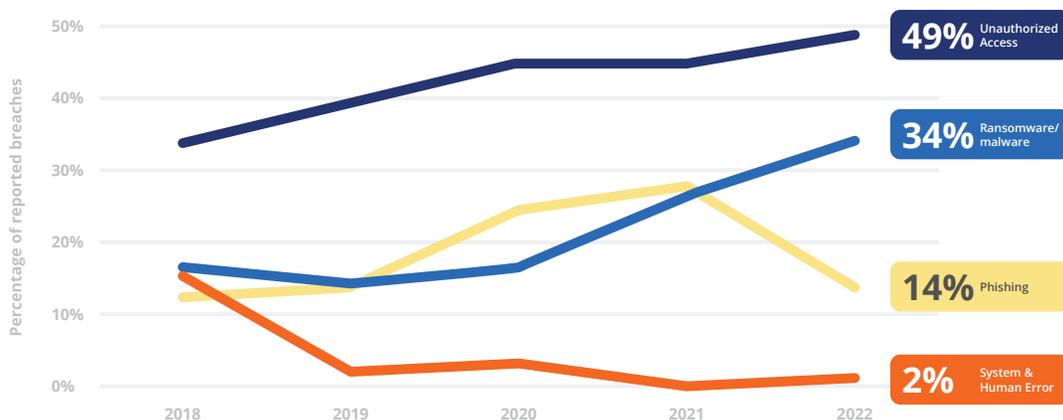


# Top Attack Vectors

## Unauthorized access and ransomware are on the rise

The number of annual breaches in the U.S. has fluctuated over the past five years, as have trends regarding the attack vector. In 2022, the number of breaches skyrocketed to more than 3,300, although compromised records dropped from 4.5 billion to 1.5 billion.

Unauthorized access has continued to be the most prevalent vector. Ransomware has steadily risen over the past five years, while phishing peaked in 2021 and fell in 2022. System and human error, which includes failure to configure cloud security, misconfigured firewalls, and unauthorized access has dropped as a root cause of breaches in recent years.



Most common attack vectors in reported breaches, 2018–2022

## Nearly 1.4 billion people were impacted by unauthorized access

The percentage of breaches attributed to unauthorized access remained unchanged in 2022 but comprised 91% of the number of records breached in 2022, impacting nearly 1.4 billion people. Two of the largest unauthorized access breaches in 2022 involving social media sites affected 900 million people.

In early 2023, telecommunications provider T-Mobile reported a data breach affecting 37 million customers that exposed their account data, including name, billing address, email, phone number, and date of birth. The breach was attributed to unauthorized access to a single application programming interface (API).<sup>19</sup>

For years, organizations have encouraged their users to employ stronger passwords, and many have been implementing multi-factor authentication (MFA) as an added layer of protection before access. However, requiring MFA for every authentication can increase friction for users. A better approach may be to add passwordless authentication and apply step-up authentication when critical resources are being accessed, and thresholds are crossed.

## PUTTING AN END TO IDENTITY-BASED ATTACKS:

# The road to passwordless authentication

With passwordless authentication, a user can log into a system without having to enter a password, respond to security questions, or provide other knowledge-based factors, known as “static shared secrets.” The purpose of passwordless authentication is to eliminate the leading cause of breaches. But there are different types and implementations of passwordless, so it’s worth a deeper dive into the journey.

### 1. Passwordless factor

A passwordless authentication method, such as a push notification or a facial recognition check, can be used as a factor in MFA. However, a passwordless factor is frequently combined with usernames and passwords, so even though it improves the security of password-based authentication, it shares many of the same vulnerabilities.

### 2. Passwordless experience

A passwordless experience eliminates user interaction with passwords. Although a password still exists, that secret is handled exclusively by back-end systems, and a passwordless method substitutes for a password in the user’s experience. New standards from the Fast Identity Online (FIDO) Alliance called FIDO2/WebAuthn and Multi-Device Credentials (the latter is known as “passkeys”) are enabling more convenient forms of passwordless authentication that are PKI-based and phishing resistant. A passwordless experience is essential to improving both security and user experience.

### 3. Complete passwordless

Complete passwordless authentication eliminates the need for static shared secrets — users don’t have to remember them, and services don’t have to store them. Today, complete passwordless is primarily achievable through facial recognition or fingerprint unlock in web and mobile contexts. Still, it is not yet fully attainable in complex enterprise IT environments.

## Phishing, “smishing,” and business email compromise

Phishing attacks — including email phishing, SMS “smishing,” and business email compromise (BEC) — use social engineering to create a sense of urgency to trick people into revealing sensitive information, clicking links that download a malicious “payload,” or transferring money to fraudulent accounts.

Phishing involves sending fraudulent emails, and smishing uses fraudulent text messages. BEC is a more sophisticated attack that involves impersonating high-level executives within an organization to convince employees that the email is legitimate and to follow its instructions, which may include exposing financial data or intellectual property. The burgeoning use of generative AI will make it easier for attackers to impersonate others, generate fraudulent emails and messages more effectively, and use AI-generated voice phishing (“vishing”) fraud, all of which will be harder to detect.

Preventing these types of social engineering attacks requires individuals and organizations to verify the authenticity of any request — from accessing an account to viewing sensitive information to transferring funds. In addition, security measures, such as two-factor authentication (2FA) or MFA, email security technologies, and employee training are what many organizations commonly recommend for thwarting these attacks.

**Phishing, smishing, and BEC attacks comprised 14% of all U.S. attacks in 2022.**

## MFA prompt-bombing creates new avenues for infiltration

Combining information from multiple data breaches can spell profit for cybercriminals, especially when credentials are involved. With millions of valid username and password combinations available for sale on the dark web, an attacker who has successfully logged into an account using stolen credentials is likely to come up against accounts that use MFA. The thought was that MFA push notifications would help keep out the bad guys, but attackers are getting wiser.

“MFA prompt bombing” or “MFA spam” is an insidious ploy in which an attacker repeatedly sends authentication prompts to a user’s device(s), such as a phone or email address, until the user carelessly accepts the MFA prompt to make it stop, thus granting account access to the attacker. Successful prompt-bombing attacks can result in attempts to drain bank accounts, open new credit cards, take out loans, or harm an individual’s credit rating and reputation. These attacks can be subtle, taking advantage of user distraction or inattention by sending one or two prompts per day. These less frequent prompts are not as likely to be reported, and there remains a good chance that a target will accept the MFA request.

Prompt bombing is especially painful when it’s the vector for a workforce identity attack. Many organizations, including Cisco,<sup>20</sup> were the targets of prompt-bombing attacks in 2022.

In an illustration of the line that runs through workforce and customer identity, a prompt bombing attack on another organization<sup>21</sup> in September 2022 gave cybercriminals access to the organization’s VPN and internal networks, where they obtained access to privileged accounts. This infiltration, in turn, gave the attackers free rein over multiple internal systems, exposing the PII of more than 57 million people.

## One in three attacks are ransomware

Ransomware attacks are malicious software (malware) that encrypts a victim’s files, rendering them inaccessible, and demands payment (often in cryptocurrency) in exchange for the decryption key to restore access to the files.

Before they can encrypt all the files on a system — or multiple systems on a network — attackers must gain access, primarily through compromised credentials, phishing, smishing, or business email compromise. However, access can also result from a misconfiguration leading to website compromise or a vulnerable application. Due to attackers’ relentless efforts to bypass strong passwords and MFA, ransomware and malware comprised 34% of attacks in 2022.



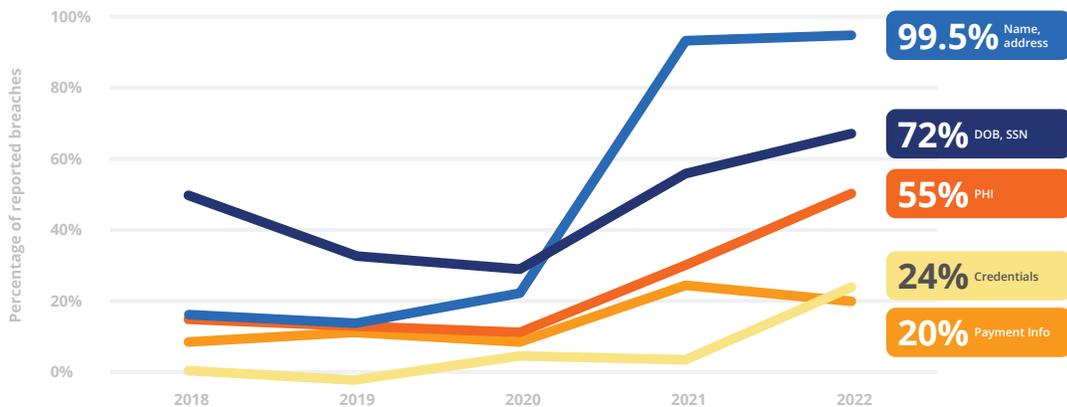
**Ransomware and malware comprised 34% of U.S. attacks in 2022.**

Organizations can significantly reduce the risks of unauthorized access, phishing, prompt bombing, and ransomware attacks by designing user experiences that decrease or eliminate the username/password combination and weak MFA methods like SMS one-time passcodes — for consumers and workers alike.

# The Stolen Identity of a Single Authorized User Can Trigger a Massive Breach

Personally identifiable information (PII) gleaned from data breaches can be used for a variety of fraudulent activities, such as filing falsified tax returns, opening bank accounts, or submitting claims on government-run services like Medicare. Fraudsters can also file false claims using stolen patient PHI to receive reimbursement or to obtain and sell prescription drugs.

Over the past five years, the amount of PII in breached records has increased. Even relatively innocuous data, such as name and address, which appeared in 20% of breaches in 2018, is now found in virtually all records. Meanwhile, the incidence of valuable data, including login credentials, PHI, date of birth, and Social Security Numbers, continues to rise. Only payment/credit card information has dropped, and only in the most recent year.



Personally identifiable information (PII) types reported in breaches, 2018–2022

## Some PII is everywhere

In almost all breaches, PII remains prevalent, with sharp increases in date of birth and Social Security Numbers and in PHI between 2021 and 2022. It's almost certain that name and physical address will be present in breached records; for two years running, they were in at least 99% of records.

However, the incidence of payment information in breaches has dropped in the past year. The decrease may be due to enhanced security in the financial services industry and the adoption of digital wallets, which help prevent data breaches through MFA, tokenization technology in place of credit card numbers, and encryption.

# Third-Party Breaches are a Growing Threat

Data breaches on third-party service providers are becoming attractive targets because they offer attackers the potential to gain access to sensitive data from multiple organizations simultaneously. Loose integrations between third-party suppliers and the organizations that rely on them — weak access controls, poor API integrations, or lack of MFA for employee accounts — can be used to exploit third-party providers. Without strong identity governance and a least-privileged access model, an attacker can breach one workforce user’s account through unauthorized access and move laterally across a vendor’s systems to find and exploit valuable data.

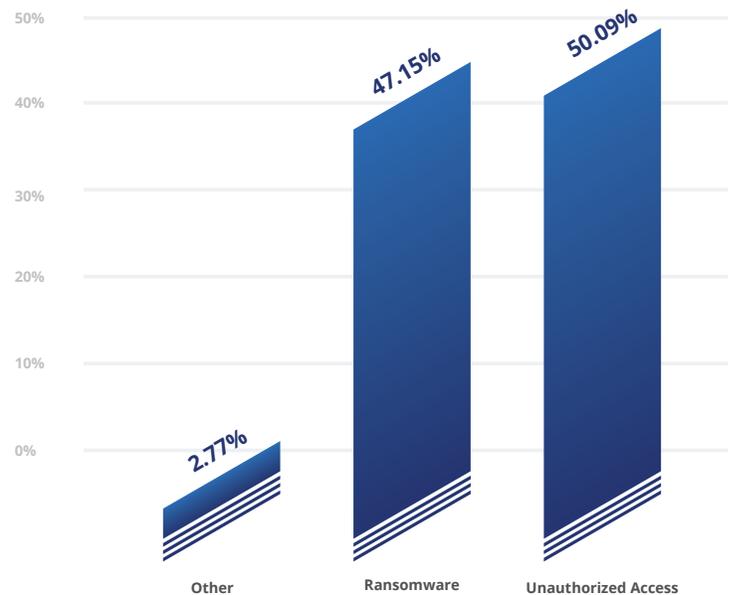
We first reported breaches of third-party service providers in 2021, and the percentage has quickly risen to comprise more than half of all reported attacks. Breaches of third-party service providers, as defined by the Identity Theft Resource Center, are “cyberattacks against a single entity in hopes of gaining access to information maintained by the organization on behalf of other businesses or institutions.”

Attacks on third-party service providers often compromise outdated systems or those not appropriately designed or managed. These breaches are more expensive and have a longer life cycle because they impact many organizations simultaneously. Fully half of the breaches in 2022 resulted from an attack on a third-party service provider, an increase of 136% over 2021. Whether the breach of a third-party vendor was due to unauthorized access, ransomware, or phishing, these attacks affected thousands of organizations and caused untold damage. In 2022, ransomware and unauthorized access were the leading attack vectors in third-party service provider breaches.

## A third-party breach affected 657 healthcare organizations

Professional Finance Company, Inc. (PFC), an accounts receivable management company supporting hundreds of healthcare organizations, suffered a ransomware attack in February 2022. As a result of this breach, attackers accessed systems and documents containing patient-related data. Although the vendor discovered and neutralized the threat on the same day it hit, the breach adversely affected more than 657 healthcare organizations and impacted almost two million people.<sup>22</sup> These numbers show an organization’s vulnerability when the third-party service providers’ cybersecurity practices fall short.

**Fully half of the breaches in 2022 resulted from an attack on a third-party service provider.**



Attack vectors used in third-party breaches, 2022

## ARTIFICIAL INTELLIGENCE:

# The Power to Protect; the Power to Attack

ChatGPT has taught the world that different kinds of artificial intelligence (AI) exist. AI-based chat uses its language model to access a massive body of text to figure out how to fill in the next blank. AI is increasingly used to personalize online shopping experiences by creating recommendations based on a user's browsing history, preferences, and interests. AI also bolsters secure access through improved facial recognition and prevents fraud by detecting suspicious patterns or behaviors in real-time.

However, AI-driven fraud is increasing. Generative AI, which produces various types of content, including text, imagery, audio, and synthetic data, makes it easier for fraudsters to impersonate others. The first case of AI-based identity fraud reported by the Identity Theft Resource Center occurred in 2019, in which an attacker generated a "deep fake" AI voice cloning impersonation of a CEO, compelling a transfer of \$243,000.<sup>23</sup> Researchers at Check Point Research have found underground hacking communities using ChatGPT to generate malware, create encryption suitable for ransomware, and devise other fraudulent schemes.<sup>24</sup> The new AI wave contributes to soaring voice and video deepfakes. Voice deepfakes, in particular, are targeting over a third of companies and half of the banking industry.<sup>25</sup>

When it comes to the marriage of fraud prevention and customer experience, AI plays a key role. AI specializing in risk decisioning can take in a wide variety of signals about who is trying to do what, information about their permissions, and then fill in the blanks for what they can do next. Decisioning AI can also prevent attempts to gain unauthorized access by incorporating multiple contextual signals into the decision process, such as login location, IP network reputation, and the distance between login attempts and registered MFA devices.

Organizations with fully deployed security AI and automation can detect unexpected activity, stopping intruders in real-time at the point of user authentication. Not only can AI and automation quickly identify and contain a breach, but their use can also result in a 65.2% decrease in breach costs.<sup>26</sup>

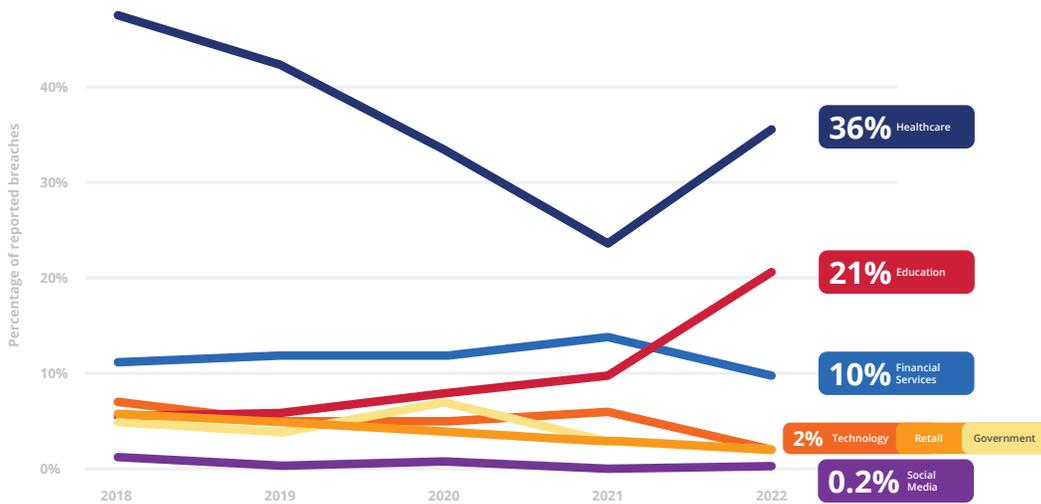
In organizations, decisioning AI can automate cumbersome workforce identity governance tasks to evaluate users quickly and the resources they can access. It also helps to eliminate over-provisioned access that can enable attackers to use one compromised account to move laterally and unhindered throughout the organization, culminating in a breach that results in the theft of sensitive and regulated data.

Decisioning AI is an essential component for elevating protection against AI-based threats. It simultaneously enables continuous analysis of multiple risk signals, making detecting and thwarting attacks easier. Since attackers are determined to invent new ways to perpetrate fraud – including using AI and machine learning – decisioning AI is rapidly becoming a must-have component for battling attacks quickly and creatively.

# Some Industries are More Resilient than Others

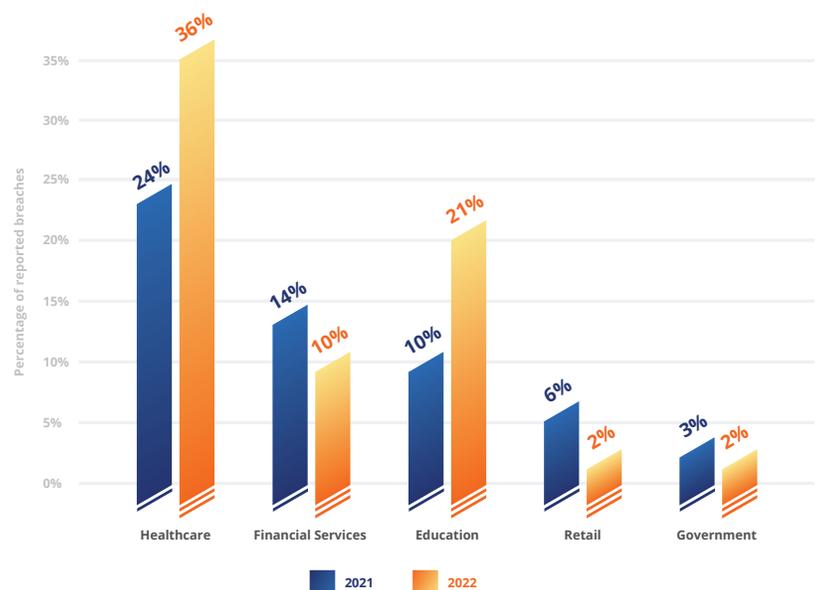
Over the past five years, some vertical industry segments have become more resilient to cyberattacks. Others remain vulnerable, experiencing increased attacks on valuable data that cybercriminals successfully target.

Healthcare was the most attractive target for cyberattacks for the fifth consecutive year, accounting for 36% of breaches in 2022. Education rose to second place for the first time, garnering 21% of breaches. Financial services, retail, and government were far more at risk five years ago but have steadily decreased as targets of attack.

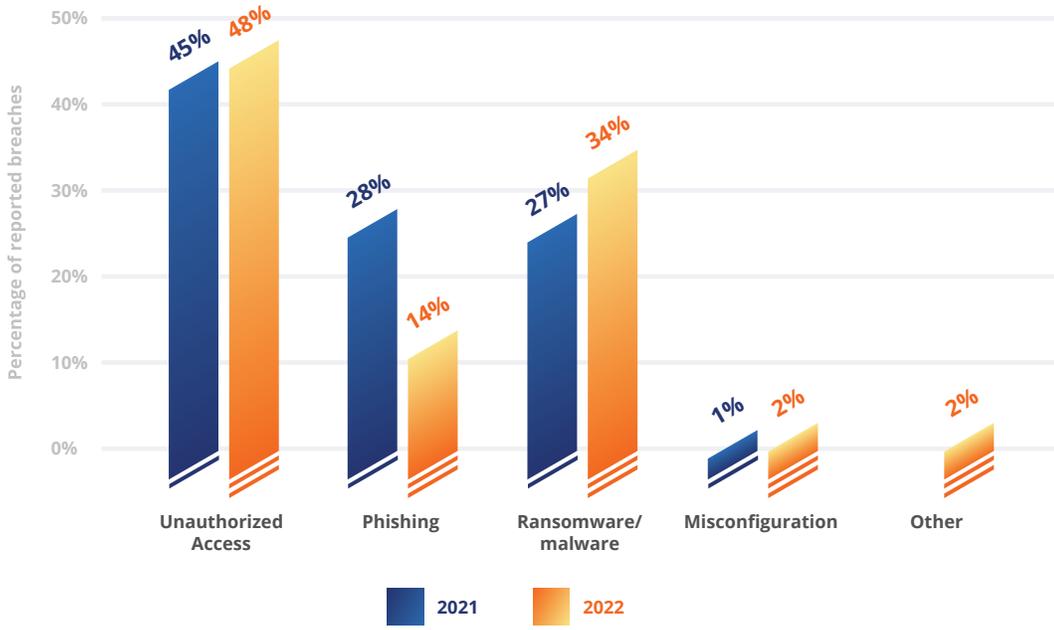


Breaches by industry, 2018–2022

The past year saw considerable increases in breaches that hit education and healthcare. Other sectors, notably financial services, retail, and manufacturing, dropped substantially. Ransomware and unauthorized access were responsible for the bulk of both healthcare and education attacks; conversely, decreases in breaches in other industries were primarily due to them implementing strong authentication and phishing-resistant MFA.<sup>27</sup>



Targeted industries, 2021–2022



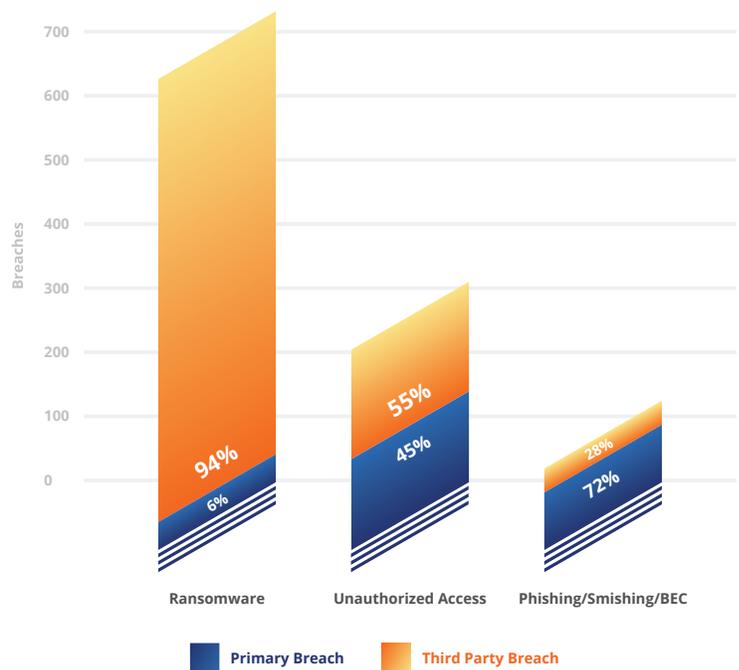
Attack vectors, 2021–2022

## Ransomware attack costs hospital over \$150 million

Cybercriminals continue to target healthcare. Due to increasing reliance on electronic health records and PHI stored in the cloud, attackers know that they can access not only personal and financial information but also medical history, prescriptions, treatments, and more. This data can be used to impersonate patients to gain access to Medicare and Medicaid benefits, healthcare devices, and prescription medications. Attackers can even use stolen records to produce fake licenses to practice medicine.

Healthcare organizations were hit hard by ransomware with devastating effects. One hospital reported that a ransomware attack had so far cost it more than \$150 million, and they had not calculated the final tally at the time of this report. The attack cost was much higher than the average in healthcare — \$10 million<sup>28</sup> — due to a month-long outage and extended disruption to system operations. Large health systems can incur losses of between \$1 million and \$2 million per day due to business disruption.<sup>29</sup>

In the U.S. healthcare sector, breaches originating from third-party service providers comprised 94% of ransomware breaches, 55% of unauthorized access, and 39% of phishing/smishing/BEC breaches. Overall, healthcare breaches impacted 1,212 healthcare organizations in 2022, revealing Social Security Numbers, accounts receivable balances, dates of birth, and more.



Healthcare breaches, primary vs. third party, 2022

# The largest ransomware attack of 2022 affected 2.5 million healthcare users

Ransomware was responsible for 32% of the breaches in 2022. It is difficult to determine how many records were breached in ransomware attacks because breached organizations often state the impact only in terms of gigabytes of information stolen/encrypted. The largest attack in 2022<sup>30</sup> impacted more than 30 healthcare firms and 2.5 million patients when a single mailing and printing services vendor discovered active ransomware in its network.

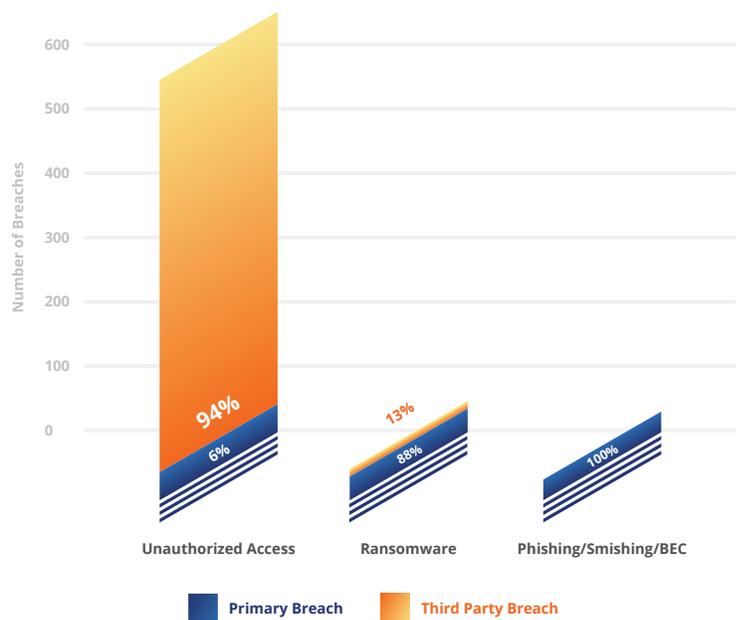
Ransomware attacks continue to target industries classified as “critical infrastructure” in the Cyber Incident Reporting for Critical Infrastructure (CIRCI),<sup>31</sup> including education, healthcare, and financial services. Such attacks encrypt data and threaten to delete it forever unless the victims pay a ransom; many also threaten to publicize or sell the data in a practice known as double-extortion ransomware.

# A single breach hits 602 schools, affecting 14 million students

Education has become an important target in recent years, partly due to the value of children’s data, including SSNs, Green Card serial numbers, naturalization document control numbers, and other PII that can be used to apply for credit cards or benefits. A single breach can send ripples across the sector, as we saw with a breach of a third-party provider of an online record and grade tracking system.<sup>32</sup> That breach hit more than 600 K-12 institutions in the U.S. and affected 14 million students. Third-party breaches represented 94% of the unauthorized access breaches in education in 2022.

As schools and universities transitioned rapidly to distance learning, they embraced cloud-based solutions for tuition, curriculum, and evaluation without scrutinizing their vendors’ compliance and security postures. A recent report showed that out of 164 online educational tools evaluated, 89% “engaged in data practices that put children’s rights at risk.”<sup>33</sup>

It is difficult to protect student information in light of the various regulations that cover the education sector. In some cases, these regulations require only an annual accounting of breaches; in others, there is no requirement to notify students or parents. Voluntary pledges, like the Student Privacy Pledge, do little if anything to protect PII: one of the largest education breaches of 2022 came from signatories to the pledge.<sup>34</sup>



Education breaches, primary vs. third-party, 2022

## Making the grade: financial services, government, and retail

Financial services, government, and retail sectors continue to outperform others, with financial services reporting 19% fewer breaches in 2022 than the average of the past four years, with government at 55% fewer and retail at 65% fewer.

We attribute some of the success in financial services and retail to the enthusiastic adoption of what the Open Banking movement refers to as Strong Customer Authentication (SCA), spearheaded by regulatory regimes in the UK and the EU. Their mandates have encouraged the speedy adoption of best practices in an unforgiving environment of poor user experiences. In addition, a strong economic imperative to mitigate fraud risks has helped banks apply better-than-average cybersecurity protections.

Embedded payment mechanisms in e-commerce have also enabled the retail sector to benefit. Nevertheless, financial services and retail sectors fell victim to attacks other than unauthorized access. Misconfigured firewalls and code vulnerabilities in financial services exposed nine million<sup>35</sup> credit card transactions. The biggest retail breach in 2022 resulted from a credential-stuffing attack.<sup>36</sup>

Regarding the government, there are stark differences between the number of attacks on local governments vs. state and federal levels. Federal agencies are required to implement strong identity and access controls, including phishing-resistant MFA, leading to greater resiliency against cyberattacks.<sup>37</sup> Not subject to the same stringent requirements, local governments were the target of 78% of the data breaches reported in 2022, as hackers exploited their staffing and budgetary shortfalls. State governments saw their share of incidents: a security flaw in a state tax website led to the disclosure of eight million taxpayers' SSNs and bank account numbers.<sup>38</sup> The State and Local Government Cybersecurity Act,<sup>39</sup> signed into law in June 2022, will bring information- and resource-sharing to state and local governments to improve their identity and access controls and help them prevent or recover from cyberattacks.

## Falling short: insurance

Despite being a highly regulated part of the financial services sector, the insurance industry is increasingly being targeted by cybercriminals. They exploit the vast amounts of PII stored in outdated systems, the lack of user training, and the slow adoption of strong authentication.<sup>40</sup> In 2022, while attacks on the financial services sector decreased by 28.6% compared to the previous year, nearly half (47%) of all breaches affected the insurance industry.

**The insurance sector finds itself increasingly in the crosshairs of cybercriminals due to the vast amounts of PII stored in legacy systems, lack of user training, and slow adoption of strong user authentication.**



# Regional Insights

# United Kingdom

Globally, 2022 was another whirlwind year in cybersecurity, and the UK was not immune. Over the past 12 months, 39%<sup>41</sup> of businesses in the UK suffered a cyberattack, 20% of which resulted in the loss of money or data.

In 2022, the UK saw 18 ransomware incidents that required a nationally coordinated response, one of which was an attack on a water utility, and there were 2.7 million cyber-related fraud incidents reported across the UK.<sup>42</sup> Fortunately, there has been progress in the fight against attackers. The National Cyber Security Centre (NCSC)<sup>43</sup> launched a free early warning system that informs organizations of potential threats and malware and alerts them to vulnerabilities or open ports in their networks. By the end of August 2022, the system had sent 34 million notifications to its growing membership.

## The threat landscape: Who?

In 2022, the UK experienced a range of data breaches by three specific actors: nation-states; cybercriminals, lone actors and gangs such as Lapsus\$ or Conti; and insiders. According to an Annual Review<sup>44</sup> conducted by the NCSC, the most prominent nation-state actors were Russia, China, Iran, and North Korea, targeting critical UK infrastructure and institutions for espionage, theft, destruction, or leaks aimed at changing the government decision-making process.

Gangs and lone actors represent an equally significant threat. In 2022, a 17-year-old from Oxford breached<sup>45</sup> global technology company Uber and video-game leader Rockstar Games, while the notorious Lapsus\$ gang managed to access data<sup>46</sup> from Okta, Nvidia, Samsung, and Ubisoft in one fell swoop.

Human error has also posed a significant risk to UK data security, in some cases due to hackable passwords, failure to update software, or falling for social engineering.

## What?

Ransomware continued to plague the UK, with attacks morphing into more expensive and destructive double- and triple-extortion forms in which more than one party is held at ransom. While the UK experienced 18 ransomware attacks requiring a national response, the NCSC<sup>47</sup> expects that this number is significantly higher due to under-reporting.

Phishing also dominated the UK threat landscape in 2022. Of the nearly 40% of UK businesses that reported an attack<sup>48</sup> in 2022, phishing attempts were the most common.

Other notable forms of breaches in 2022 included impersonating an organization/corporate identity fraud, spyware or malware, attempted hacking of online bank accounts, and account takeover (ATO).

## Nearly 40% of UK businesses reported an attack in 2022.

## Where?

Academic institutions<sup>49</sup> in the UK are known as the most popular feeding ground for cybercriminals, experiencing a weekly average of 2,653 attacks, up 237% compared to 2021. Healthcare once again proved to be the costliest sector. In addition, the financial industry maintained its position as the sector with the second-most expensive breaches.

Other industries have also been affected. The NCSC warned<sup>50</sup> of malicious campaigns by Russia- and Iran-based groups targeting defense, government, NGOs, and think tanks. In addition, charities were hit hard: 30% of UK charities<sup>51</sup> identified a cyberattack in the last 12 months.

## UK pushing back

The UK has taken significant steps to implement policy and regulatory changes to help fight data breaches throughout the past year, with tangible results beginning to be seen. Examples include the NCSC's sanctioning of leading threat actors<sup>52</sup>, and its support of organizations, including the Royal Mail<sup>53</sup>, which refused to pay what it considered exorbitant ransomware demands. The UK recently led Western Europe's largest cyber warfare exercise<sup>54</sup>, a clear indication of its position as a global security leader.

Data breaches pose an enormous risk to the safety of UK citizens. To help vulnerable organizations mitigate threats, security providers must provide cutting-edge solutions, including phishing-resistant multi-factor authentication (MFA), passwordless access, and artificial intelligence/machine learning (AI/ML)-powered solutions. When used correctly, these tools can empower organizations to fight against attackers. Security data in the face of evolving threats is only getting more complicated. As a nation, the breach resilience of the UK lies in the hands of every business working together with the government to tackle data breaches.

# Germany

The cybersecurity situation in Germany, already under considerable pressure due to a 358% increase in blackmail and system failure losses from 2019-2021,<sup>55</sup> became even tenser in 2022, greatly influenced by the war in Ukraine and its effects on threats such as hacktivism. Non-political cybercrime has also remained high, with the most recent report of the German Federal Office for Information Security (BSI)<sup>56</sup> rating Germany's overall cybersecurity threat level as higher than ever before..

## Ransomware and “big game hunting”

Ransomware remained one of the main cybersecurity threats for private and public organizations, with the British Standards Institution (BSI) recording 116.6 million new variants during the reporting period. A survey by Bitkom,<sup>57</sup> Germany's association for the information and telecommunications industry, states that 63% of all surveyed companies had “sensitive digital data or information” stolen, including “communication data such as e-mail correspondence” (68% of cases), “customer data” (45%), and “non-critical business information” (38%).

The country has seen a continued trend of attacks targeting financially strong, high-value targets, which are particularly sensitive to downtime and, therefore, more likely to pay a large ransom (a practice known as “big game hunting”). In its survey, Bitkom reported damages of €10.7 billion due to ransom payments from stolen data.

However, according to an IBM report,<sup>58</sup> the total costs of a data breach in Germany decreased slightly to \$4.85 million (USD) on average in 2022, compared to \$4.89 million in the previous year.

**62.9 million user accounts in Germany were compromised in 2022.**

The common practice of leaking breached and stolen data on dark web platforms if ransom demands are not met — and sometimes even if they are — creates an additional threat: other cybercriminals can use the data to facilitate further attacks, either on the organization itself or others connected to it. According to research by the Hasso Plattner Institute,<sup>59</sup> which has been recording data leaks of

compromised accounts in Germany since 2006, approximately 62.9 million user accounts were compromised in 2022.

Significant ransomware attacks targeted companies in the medical technology sector and a major electronics wholesaler with two retail chains. In July 2021, a municipality declared a state of emergency for the first time in German history due to a ransomware attack. It lasted seven months, as the municipal government declined to pay the ransom. The attack impaired all municipal IT systems to a degree in which essential services, such as payment of unemployment benefits or parental allowances, were significantly impeded. When the municipality lifted the state of emergency, they had not mitigated all of the damage but were able to restore the functional capabilities of the affected systems and processes.

## War in Ukraine

In addition to ransomware-based threats, the BSI reported several direct attacks, such as hacktivism connected to the Russian war of aggression in Ukraine, often via distributed denial-of-service attacks (DDoS). Some of these attacks led to disruptions of IT supply chains and critical infrastructure, including a hacktivist attack on a German oil trader with a Russian parent company and the remote maintenance failure of wind turbines after an attack on a connected satellite communications company. However, there was no evidence of a targeted Russian cyberwarfare campaign against German targets due to German support of the Ukrainian war effort.

## Poor IT and software quality

The BSI also found that IT and software products' poor quality and security have been an increasingly serious concern. Its Common Vulnerability Scoring System (CVSS)<sup>60</sup> showed 20,174 vulnerabilities in IT and software products, representing a total increase of 10% over 2021. Of these, more than half scored as “high” and 13% as “critical” vulnerabilities.

## State of GDPR

Since the introduction of the General Data Protection Regulation and the law's 2018 implementation in Germany (Bundesdatenschutzgesetz, BDSG),<sup>61</sup> the regulation has been used in multiple high-profile cases to impose multimillion-euro fines on companies for data breaches. In 2022, there were 29,795 data breaches reported to authorities in Germany,<sup>62</sup> compared to 30,123 in 2021.



## Breached businesses in Germany suffered €23.6 billion in image and reputation damages.



In 2022, several significant fines were imposed by German data protection authorities for GDPR violations, as reported by Virtuelles Datenschutzbüro,<sup>63</sup> an information platform of the public data authorities in Germany. These fines ranged in size from €50,000 imposed on a property development company for failing to provide information about the origin of data to a €1.9 million fine imposed on a housing association for unlawfully processing sensitive data about potential tenants.

In its survey, Bitkom reports total costs of €18.3 billion due to data privacy measures, such as customer data and information recovery, and an estimated €23.6 billion in image and reputation damages due to negative media attention for affected businesses. The latter increased significantly compared to the estimated €12.3 billion in damages in 2021, indicating increased public scrutiny of organizations' insufficient cybersecurity and data protection measures.

# Australia

Australia saw a total of 890 breaches in 2022, according to the government's Office of the Australian Information Commissioner (OAIC) Notifiable Breaches Report for 2022.<sup>64</sup> The industries most affected by data breaches were healthcare (16% of all breaches), followed by finance (13%), and legal, accounting, and management services (7%).

Similar to 2021 and 2020, personal contact information (home addresses, phone numbers, or email addresses) remained the most frequently sought-after information in data breaches from January to June 2022, at 37%, followed by identity information<sup>65</sup> at 24%, financial details at 17%, health information at 15%, and tax file numbers at 9%.

Between January to June 2022, 71% of entities notified the OAIC within 30 days of becoming aware of an incident, down from 75% from July to December 2021. Reporting breaches due to human error and system faults was shorter, while organizations took longer to report breaches resulting from malicious attacks. However, between December of 2022, 80% of organizations notified the OAIC within 30 days of becoming aware of an incident.

**Every seven minutes, a cybercrime is reported in Australia.**

## Deepening threat landscape

The need for better protection of the personal data of Australians is in the spotlight. The Australian Cyber Security Centre's Annual Cyber Threat Report,<sup>66</sup> covering the 2021–22 financial year, received more than 76,000 cybercrime reports. This is an increase of nearly 13% from the previous financial year, with cybercrimes now reported in Australia every seven minutes. Following high-profile incidents, including the Optus data breach<sup>67</sup> in September and the Medibank data breach<sup>68</sup> in October, which led to the spread of sensitive customer information on the dark web, there is rising concern about the local threat landscape.

## Investments rise, but more is needed

In 2022, there was a stronger investment in cybersecurity from the Australian federal government. Announced as part of the 2022–23 federal budget in March 2022, the government's \$9.9 billion AUD program, REDSPICE<sup>69</sup> ("Resilience, Effects, Defence, Space, Intelligence, Cyber & Enablers"), marks a significant investment in the Australian Signals Directorate that will help bolster Australia's cyber capabilities through artificial intelligence (AI), machine learning (ML), and cloud technology, among others. The federal government also swiftly increased the penalties for businesses experiencing serious or repeated privacy breaches<sup>70</sup> to a maximum of \$50 million.

**Businesses experiencing serious or repeated privacy breaches now face fines of up to \$50 million AUD.**

Despite rising economic uncertainty and tighter budgets, technology investments remain a priority for local businesses: Gartner projects that IT spending in Australia will increase by 5.8% in 2023.<sup>71</sup> Australian organizations are embracing more cloud-based services and progressing AI and automation strategies as part of these technology investments. At the same time, KPMG's Global Tech Report<sup>72</sup> revealed that 59% of Australian organizations reported that less than 10% of their overall budget was dedicated to technology, compared to 46% of global organizations.

With cybersecurity incidents still rising, more education is needed to help these investments deliver meaningful business results. There is also a shortage of people with the skills to help drive digital transformation initiatives. Zero Trust architectures, AI, automation, passwordless login methods, and more cloud-based systems will continue to create innovative ways for organizations to combat cyber threats in 2023 and beyond. To take full advantage of these advances, Australian industry and government must collaborate to create training paths and fuel the growth of jobs focused on guiding technology decisions.

# Singapore

Singapore<sup>73</sup> saw a 7% increase in cybercrime in 2021, at 48% of overall crime, according to the Singapore Cyber Landscape (SCL) 2021.<sup>74</sup>

The biggest contributor to successful attacks in Singapore was phishing scams, accounting for more than 18,000 incidents in 2021 (a 50% increase over the previous year). The second leading attack method was unauthorized access, which was used in more than 3,700 cases, similar to 2020. Cyber extortion dramatically increased to 420 cases in 2021, compared to 245 in 2020. Ransomware also rose, with a 54% increase in cases reported to SingCERT<sup>75</sup> in 2021, continuing a steady trend from 2019. Website defacements, on the other hand, were down slightly in 2021.

## Phishing scams were the leading attack method, increasing by 50% over the previous year.

Approximately 55,000 phishing URLs with a Singapore-linked website were detected in 2021, an increase from 47,000 in 2020. In 2021, commonly spoofed sectors included social networking sites, the financial sector, and the online/cloud service sector.

## Increased digitization leads to greater risk

Sophisticated threat actors were hard at work in 2021 around the globe, especially regarding ransomware. As it continues to advance its digitization efforts, Singapore saw an increase in ransomware incidents of 54% over 2020, as reported to SingCERT. These incidents primarily impacted small and medium enterprises (SMEs) in the manufacturing and IT industries.

Phishing campaigns and data breaches continued to affect Singaporean businesses, such as financial services leader OCBC<sup>76</sup> (December 2021), Starbucks<sup>77</sup> (September 2022), Shangri-La<sup>78</sup> (October 2022), and Carousell<sup>79</sup> (October 2022). The government has noted the growing number of cyberattacks and is working with the broader industry to deepen awareness.

Businesses need to be aware of the expanded attack surface presented by digitization, taking the necessary steps to protect their infrastructure by increasing cyber

awareness, adopting passwordless measures, and implementing step-up authentication tools to block unauthorized access.

Collaborating for a more resilient cyber infrastructure Singapore recognizes the importance of digital trust for businesses in the region. In June 2022, Mrs. Josephine Teo, Singapore's Minister for Communications and Information, announced the launch of the Digital Trust Centre<sup>80</sup> (DTC) to lead Singapore's research and development efforts for trust technologies and support talent development in this space.

A Memorandum of Understanding<sup>81</sup> (MOU) was signed between Singapore and the United States in August 2022 to expand cooperation on cybersecurity. The MOU will create new areas of collaboration, such as research and development in critical technologies, enhancing information sharing, encouraging cybersecurity exchanges between Singapore and the U.S., and joint exercises.

In October 2022, The Monetary Authority of Singapore (MAS) Cyber Security Advisory Panel<sup>82</sup> (CSAP), comprising cybersecurity experts worldwide, provided insights into ways the Singapore financial sector can build on its cyber hygiene. The CSAP advised Singaporean enterprises to stay alert to new threats that may arise as a result of geopolitical tensions to help prevent digital banking fraud by implementing artificial intelligence (AI) and machine learning (AI/ML)-based solutions that prevent unauthorized access, and to increase their resilience against attacks.

## The Monetary Authority of Singapore (MAS) advises using AI and ML-based solutions to prevent digital banking fraud.

The Counter Ransomware Task Force<sup>83</sup> (CRTF) was established to bring together Singapore Government agencies from various relevant fields to strengthen Singapore's counter-ransomware efforts. In November 2022, the CRTF published a report that will guide Singapore's efforts to foster a resilient and secure cyber environment, domestically and internationally, to combat the growing ransomware threat.

# Recommendations

ForgeRock experts recommend focusing on eight strategic areas for preventing data breaches:

## 1. Secure your organization's workforce identities

Organizations are often breached because at least one workforce user's account — an employee, contractor, partner, or supplier — within the organization itself becomes compromised through credential-stuffing attacks, an email phishing or SMS "smishing" attack that tricks an employee into entering credentials at a spoofed domain, or other means.

Over-provisioned workforce accounts that become compromised through unauthorized access enable attackers to move laterally through the organization and gain access to sensitive systems or data, including customer data. Implementing single sign-on (SSO) and passwordless MFA to all internal and external systems and services, along with solid identity governance practices, can help secure organizations against data breaches due to unauthorized access.

## 2. Secure and enhance customers' interactions through CIAM

Strong customer identity and access management (CIAM) allows customers to simply and securely interact with your digital business. From registration to authentication to account recovery and more, a robust CIAM solution orchestrates powerful and flexible interaction journeys that deliver customers convenience, value, and control. Users' ability to manage privacy preferences, choose sign-in devices and methods, and provide data that enables service personalization all rest on an adaptable approach to CIAM.

## 3. Implement a Zero Trust framework

A mature Zero Trust deployment can result in significant cost savings of up to \$1.51 million per breach.<sup>84</sup> This approach ensures that every user, device, and API connects to every application securely, with layered intelligence and step-up authentication. Identity and access management (IAM) and identity governance and administration (IGA) technologies are key components of a Zero Trust framework. Zero Trust is mandated in the U.S. federal government, but every industry and region worldwide can benefit from implementing its practices.

## 4. Leverage AI and intelligent decisioning for all identities across the identity life cycle

These technologies can help to prevent fraud and fine-tune offerings for all sectors. For example, AI can present high-value offers for someone based on their ability to pay. AI-driven threat protection can bring together pattern recognition, fraud prevention (including account takeover), and customer experience to provide a secure and personalized login experience for all identity types across the identity life cycle, starting with registration. AI and intelligent decisioning can reduce security blind spots by treating each login request individually and adapting decisions dynamically instead of based on static and predictable patterns. Based on risk scores, it can fast-track users with advanced options like passwordless authentication and implement additional authentication steps for known users on new devices or those logging in at unusual times and places.<sup>85</sup>

## 5. Embrace passwordless authentication

Known as “static shared secrets,” username and password-based credentials are the main ingredient in many attacks. Look for IAM that supports passwordless authentication and can orchestrate no-code passwordless authentication and other user journeys. Rather than taking an all-or-nothing approach, choose the right passwordless solution — passwordless as an additional authentication factor, a passwordless experience where the user needn’t interact with a password, or complete passwordless solutions — where each makes sense.<sup>86</sup>

## 6. Leverage NIST digital identity guidelines

The U.S. National Institutes of Standards and Technology (NIST) Digital Identity Guidelines SP-800-63 provide solid recommendations for securing your business and meeting end users’ privacy needs. It describes how to secure an Identity Assurance Level (IAL), an Authenticator Assurance Level (AAL), and, for federated systems, a Federation Assurance Level (FAL). These taxonomies are also important for communicating security requirements between departments and even between partner organizations in third-party relationships.<sup>87</sup>

## 7. Thoroughly vet your third-party service providers

You should vet your partners’ cybersecurity practices to prevent breaches affecting your customers. Before onboarding a third-party service provider, conduct a risk assessment of their data protection policies, security controls, and incident response capabilities. Inform them of your organization’s security requirements regarding data protection, access management, and incident reporting, and review these requirements with them regularly. Continuously verify that your suppliers comply with your organization’s required security practices and maintain processes to monitor vendors’ security incidents.

If your third-party service provider is to have access to data from your organization, be sure it is using a standard protocol, such as SAML (Security Assertion Markup Language) or OAuth 2.0 (Open Authorization), to establish federated access to your organization. Finally, be prepared to cut ties: have a plan and processes to secure and reclaim data managed by that vendor, and terminate a supplier relationship if the vendor has not properly addressed a security incident or breach.

## 8. Be ready for a breach

While the above recommendations can help prevent identity-related breaches, you should still have a breach incident response plan (IRP) in place to define the roles and responsibilities of each team member in the event of a data breach. Train employees on what they can do to prevent data breaches and audit your security posture regularly. Establish a communication plan for how you will notify employees, customers, partners, and vendors in the event of a breach. Have a plan to back up and recover data. Regularly test the effectiveness of your IRP, and have a breach response team of key stakeholders in your organization.

# How ForgeRock Helps

ForgeRock's unified IAM platform provides a comprehensive identity perimeter for your organization. It includes full-suite identity and access management and identity governance and administration (IGA) capabilities to secure all identities (workforce, consumers, applications, and things). The platform is delivered as a cloud service with self-managed and hybrid deployment options.

With ForgeRock, you can modernize and consolidate your IAM practices, implementing standard capabilities such as federated single sign-on (SSO),<sup>88</sup> multi-factor authentication (MFA) and provisioning, and enabling identity for backend applications and services.<sup>89</sup> ForgeRock also offers advanced AI capabilities: threat detection, identity governance, contextual authentication and authorization, and passwordless authentication to help prevent fraud and enhance the end-user experience. By leveraging these technologies, you can implement risk-based authentication and offer high-value personalized offerings to your customers. Finally, ForgeRock's support for NIST digital identity guidelines enables you to comply with industry standards and effectively communicate your security requirements to partner organizations.

## Conclusion

This year's report highlights three themes that are crucial to your ability to understand and address data breaches. First, stolen identity data leads to more significant problems for victims, who must stay vigilant against identity theft for years to come. Second, the increase in breaches impacting third-party service providers amplifies the scope of impact, underscoring the need to thoroughly assess and validate the data protection measures of these partners. Third, the varying levels of vulnerability and resilience across different industry sectors emphasize the need for constant evaluation and adaptation of security approaches. While the total number of breach victims decreased dramatically between 2021 and 2022, the battle against data breaches is far from over. Incorporating Zero Trust principles — especially when integrating with third-party service providers — should be every organization's priority.

The significance of protecting workforce end-user accounts — employees, contractors, and partners — cannot be overstated. Compromising any of these accounts paves the way for unauthorized access and the potential exposure of sensitive data, including customer data. Implementing single sign-on (SSO), passwordless multi-factor authentication (MFA), and effective identity governance practices is vital for preventing unauthorized access and safeguarding your organization against data breaches.

It is evident that vulnerability and resilience vary across industries. With its high-value data and potential for ongoing fraud using healthcare records, the healthcare sector continues to be vulnerable to ransomware and unauthorized access. On the other hand, sectors such as retail have embraced enhanced security practices, including the adoption of embedded finance payment methods. Drawing inspiration from Open Banking practices mandated in the EU, the financial services sector has incorporated strong customer authentication (SCA). These measures have resulted in multi-year decreases in breaches within these industries. However, the education sector, increasingly reliant on remote learning technologies and third-party service providers, often lacks the necessary capabilities to handle data breaches and protect sensitive student data.

Despite these challenges, the progress made over the years, including in 2022, demonstrates that security does not have to be an unending scramble to catch up with the bad guys. Security is a journey of continuous adaptation and improvement. While we recommend ongoing vigilance against emerging trends, such as AI-perpetrated fraud, we see room for optimism as organizations progress in staying ahead of evolving threats. By implementing the best practices outlined in this report and understanding the tangible consequences, we can turn the tide in the fight against data breaches.

1 <https://venturebeat.com/security/report-33-global-consumers-data-breach-victims-hacked-company-held-personal-data/>  
2 <https://www.helpnetsecurity.com/2020/11/26/how-consumers-feel-about-retail-data-breaches/>  
3 Measured as 2022 increase/decrease over average of 2018-21  
4 <https://www.idtheftcenter.org/>  
5 <https://www.ibm.com/reports/data-breach>  
6 <https://techcrunch.com/>  
7 <https://www.databreaches.net/>  
8 <http://www.hipaajournal.com>  
9 <https://topclassactions.com/>  
10 <https://businessresources.bitdefender.com/bitdefender-2023-cybersecurity-assessment>  
11 <https://sec.hpi.de/ilc/statistics>  
12 <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022>  
13 Parliament approves Government's privacy penalty bill | Our ministers – Attorney-General's portfolio (ag.gov.au)  
14 Compared to 2021  
15 <https://www.csa.gov.sg/>  
16 <https://www.idtheftcenter.org/>  
17 <https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html>  
18 DLA Piper GDPR Fines and Data Breach Survey: January 2023 | DLA Piper  
19 <https://www.sec.gov/ix?doc=/Archives/edgar/data/0001283699/000119312523010949/d641142d8k.htm>  
20 <https://blog.talosintelligence.com/recent-cyber-attack/>  
21 <https://blog.gitguardian.com/uber-breach-2022/>  
22 <https://www.hipaajournal.com/657-healthcare-providers-affected-by-ransomware-attack-on-professional-finance-company/>  
23 <https://www.idtheftcenter.org/post/first-ever-ai-fraud-case-steals-money-by-impersonating-ceo/>  
24 <https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/>  
25 <https://regulaforensics.com/news/one-third-of-global-businesses-already-hit-by-voice-and-video-deepfake-fraud/>  
26 <https://www.ibm.com/reports/data-breach>  
27 <https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>  
28 IBM, Op. cit.  
29 <http://www.hipaajournal.com/commonspirit-health-reports-150-million-loss-due-to-ransomware-attack>  
30 <https://www.securityweek.com/onetouchpoint-discloses-data-breach-impacting-over-30-healthcare-firms/>  
31 <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>  
32 <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>  
33 <https://www.hrw.org/news/2022/07/12/online-learning-products-enabled-surveillance-children>  
34 <https://thejournal.com/articles/2022/08/09/illuminate-education-booted-from-student-privacy-pledge-referred-for-potential-ftc-state-ag-action.aspx>  
35 <https://www.hackread.com/exposed-credit-card-transaction-records/>  
36 <https://www.bleepingcomputer.com/news/security/200-000-north-face-accounts-hacked-in-credential-stuffing-attack/>  
37 M-22-09 Federal Zero Trust Strategy (whitehouse.gov)  
38 [https://techcrunch.com/2022/12/02/florida-tax-bug-data-exposed/?guccounter=1&guce\\_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8&guce\\_referrer\\_sig=AQAAAL69IMfcRgFKXsD9dQ14HknMEXCrWyPqMv12NY7GITxBswL5bOQKlZGlynU7poiIm6Pp1WVYbpScG95Km\\_WHx2vd4bCCKh-e\\_ITZ8GyMyfTvPgPmLNqg-gNGqgHs1BejXRHBuavglfktvZytp3b5AD5enGalwQtuhlw7z1k-5](https://techcrunch.com/2022/12/02/florida-tax-bug-data-exposed/?guccounter=1&guce_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8&guce_referrer_sig=AQAAAL69IMfcRgFKXsD9dQ14HknMEXCrWyPqMv12NY7GITxBswL5bOQKlZGlynU7poiIm6Pp1WVYbpScG95Km_WHx2vd4bCCKh-e_ITZ8GyMyfTvPgPmLNqg-gNGqgHs1BejXRHBuavglfktvZytp3b5AD5enGalwQtuhlw7z1k-5)  
39 [BILLS-117s2520enr.pdf \(congress.gov\)](https://www.congress.gov/bills/117/s2520/enr/pdf)  
40 <https://www.digitalguardian.com/blog/top-security-considerations-insurance-companies>  
41 <https://www.ncsc.gov.uk/>  
42 Threats, Risks and Vulnerabilities - NCSC.GOV.UK  
43 NCSC, Op. cit.  
44 NCSC Threats, Op. cit.  
45 Alleged Teenage 'TeaPot' Uber Hacker Arrested In England (forbes.com)  
46 Microsoft confirms Lapsus\$ hackers stole source code via 'limited' access - The Verge  
47 NCSC, Op. cit.  
48 Cyber Security Breaches Survey 2022 - GOV.UK (www.gov.uk)  
49 <https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/>  
50 NCSC, Op. cit.  
51 [https://www.ncsc.gov.uk/files/Cyber\\_threat\\_report-UK-charity-sector.pdf](https://www.ncsc.gov.uk/files/Cyber_threat_report-UK-charity-sector.pdf)  
52 UK cracks down on ransomware actors - GOV.UK (www.gov.uk)  
53 Royal Mail refused to pay 'absurd' LockBit ransom, chat logs say | TechCrunch  
54 UK leads Western Europe's largest cyber warfare exercise - GOV.UK (www.gov.uk)  
55 <https://www.mordorintelligence.com/industry-reports/germany-cybersecurity-market>  
56 <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410>  
57 [https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts\\_Wirtschaftsschutz\\_Cybercrime\\_31.08.2022.pdf](https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf)  
58 <https://www.ibm.com/de-de/reports/data-breach>  
59 <https://sec.hpi.de/ilc/statistics>  
60 NVD - Vulnerability Metrics (nist.gov)  
61 BDSG - Bundesdatenschutzgesetz (gesetze-im-internet.de)  
62 <https://www.dlapiper.com/en-gb/en-gb/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023>  
63 <https://www.datenschutz.de/>  
64 <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2022>  
65 Identity information includes an individual's date of birth, passport details and driver license details  
66 [https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022#Executive\\_Summary](https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022#Executive_Summary)  
67 <https://www.bbc.com/news/world-australia-63056838>  
68 [https://www.theregister.com/2022/10/26/medibank\\_breach\\_update/](https://www.theregister.com/2022/10/26/medibank_breach_update/)  
69 <https://www.asd.gov.au/about/redspice>  
70 Parliament approves Government's privacy penalty bill | Our ministers – Attorney-General's portfolio (ag.gov.au)  
71 <https://itbrief.com.au/story/projected-5-8-increase-to-australia-it-spending-in-2023#:~:text=In%20the%20latest%20quarterly%20tech,AUD%20%24111.2%20Billion%20in%202022>  
72 KPMG global tech report 2022 - KPMG Global  
73 Singapore's data for 2022 will be released in July/August 2023; due to timing issues, this report focuses primarily on breach data pertaining to 2021, though some 2022 events that were covered in the media are included here.  
74 Singapore Cyber Landscape 2021 (csa.gov.sg)  
75 <https://www.csa.gov.sg/>

- 76 <https://www.todayonline.com/singapore/ocbc-phishing-scam-underscores-trade-between-convenience-and-security-bank-customers-risk-experts-1789236>
- 77 330,000 S'pore Starbucks customers' data leaked, info sold online for \$3,500 | The Straits Times
- 78 Hackers targeted 8 Shangri-La hotels between May and July, guests' data potentially leaked | The Straits Times
- 79 Probe under way after breach exposes data of 1.95m Carousell users | The Straits Times
- 80 Launches the National Digital Trust Centre and co-creates the future of AI standards and governance with global partners through A.I. Verify
- 81 Singapore and United States Expand Existing Cooperation on Cybersecurity
- 82 MAS' Cyber Security Advisory Panel Discusses Actions to Deal with New Financial Sector Cyber Risks
- 83 Singapore's Counter Ransomware Task Force Report
- 84 IBM, Op. cit.
- 85 To learn more, read the white paper, "[Combat Account Takeover and Fraud with AI-driven Access Orchestration](#)"
- 86 To learn more, read the infographic, "[The Road to Passwordless Authentication](#)"
- 87 To learn more, read the white paper, "[ForgeRock and NIST Special Publication 800-63-3](#)"
- 88 <https://www.forgerock.com/platform/access-management/sso>
- 89 <https://www.forgerock.com/platform/identity-gateway/application-service-gateway>



## About ForgeRock

ForgeRock® (NYSE: FORG) is a global digital identity leader helping people simply and safely access the connected world. The ForgeRock Identity Platform delivers enterprise-grade identity solutions at scale for customers, employees, and connected devices. More than 1,300 organizations depend on ForgeRock's comprehensive platform to manage and secure identities with identity orchestration, dynamic access controls, governance, and APIs in any cloud or hybrid environment. For more information, visit: [www.forgerock.com](http://www.forgerock.com).

## Follow Us

