ForgeRock®

2022 FORGEROCK CONSUMER IDENTITY BREACH REPORT

Unauthorized Access Remains a Top Threat — It's Time to Render Stolen Passwords Worthless for Launching New Attacks

Table of Contents

Executive Summary

The year 2021 saw consumers becoming accustomed to shopping, dining, traveling, learning, and caring for their health in an ever-more-digital fashion. Unfortunately, the personal data driving these experiences was put at greater risk than ever by a perfected loop of using previously breached data to drive new breaches and widen their impact.

Data records containing usernames and passwords are the perfect "seeds" for perpetrating new breaches — and two billion such records were compromised in 2021, an increase of 35% over 2020. Achieving unauthorized access is the king of attack vectors. It enables criminals to use previously stolen credentials to compromise accounts anew and scrape even more data. Unauthorized access was once again the top vector in 2021, representing fully half of all breach methods.

The new online business-as-usual proved to be a more costly environment for many industry sectors. Enterprises experienced a fourfold increase in breaches caused by security issues with their third-party suppliers. Healthcare and retail have been particular hot spots. The healthcare industry saw nearly a quarter of all breaches, and compromised health data — so valuable to bad actors on the dark web — exacted nearly a 30% higher per-record cost on the business, at $614. The retail industry also suffered a massive impact from breaches, with account takeovers (ATOs) and fraud contributing to the average cost of a single breach rising by nearly 63% to $3.27 million.

What can we learn from the situation? The classic security measures used by many U.S. enterprises — and the regulatory regimes demanding such measures — haven't stemmed the tide of compromise, and the flood has come. Password-based protection has been failing prodigiously. And many approaches that strengthen security, such as multifactor authentication, are also creating usability issues and leading to new types of threats. Likewise, erecting barriers to resource access for employees has often only slowed business. When attacks scale up, prevention and mitigation methods need to scale up too, leveraging layers of intelligence to apply the right access controls at the right time.

Read on for detailed insights and data on the breaches impacting consumers in 2021 and year-over-year comparisons to the breaches affecting consumers in the U.S. in 2020. We also share findings from other key regions, including Australia, Germany, the United Kingdom (UK), and Singapore. You'll learn exactly why organizations need to adopt a comprehensive identity and access management (IAM) solution to help prevent data breaches, protect their 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, with a passion for fostering successful ecosystems and individual empowerment. She has 20+ years of experience innovating and leading standards such as SAML and User-Managed Access (UMA) and has also 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, along with driving ForgeRock's industry-standards leadership.

About this Report

This report is based on data from a variety of sources. Principal among them is the 2021 Identity Theft Resource Center[1], with data on several thousand breaches[2], and the IBM Ponemon report on the cost of data breaches. Additional research into the largest breaches of 2021 included TechCrunch[3] and Forrester Research[4], as well as UpGuard[5] and IdentityForce[6]. This research yielded up-to-date information on the attack vectors, number of records impacted, and industries most affected.

Note: Sums and percentage calculations in charts may not exactly add up, as some rounding may occur.

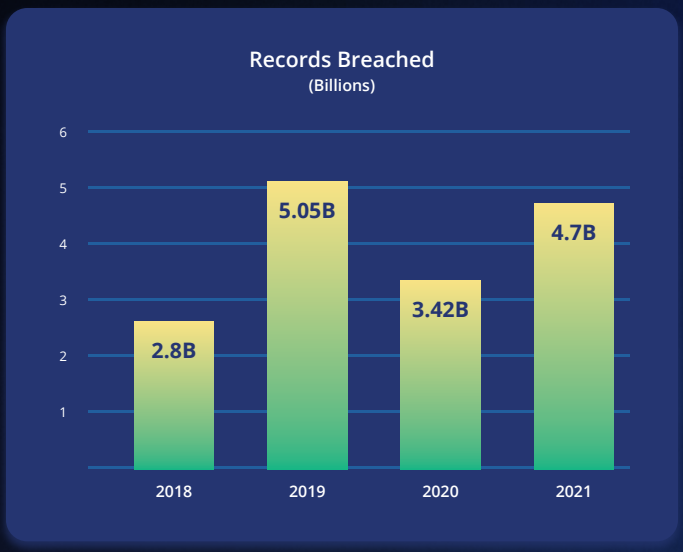
About Data Breaches

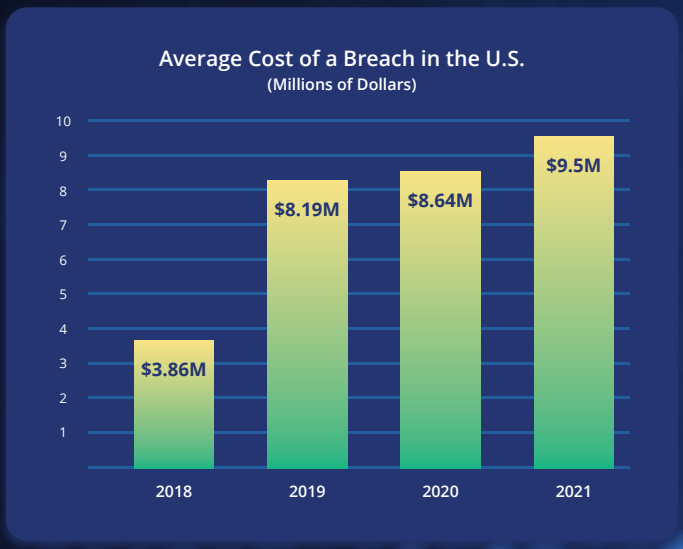
Our report focuses on confirmed breaches in which confidential data is exposed and/or stolen. A confirmed breach can refer to a single record being stolen — and such a breach must be analyzed and remediated to determine the source — but because most breaches are financially driven, attackers target large caches of data that they can hold for ransom or sell on the dark web.

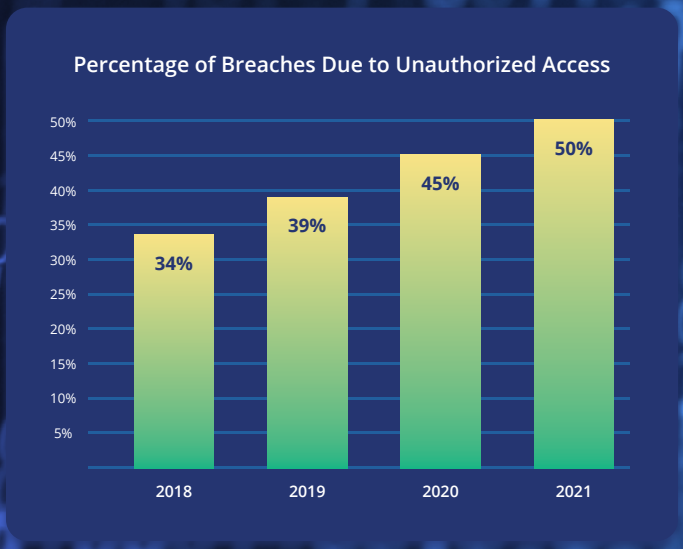
Our report distinguishes between number of breaches and number of records breached. As we all know, the institutions with which we interact online — our healthcare providers, government agencies, retailers, financial institutions — hold a great deal of sensitive data about us in their databases. Some of the largest breaches of this century, according to CSO Online[7], involve hundreds of millions — or billions — of records. The costs associated with breaches are staggering and include regulatory fines, staff costs for detection and remediation, notification, loss of business, and more.

It's important to know how such breaches can occur. Some are due to vulnerabilities that attackers are able to exploit in software or outdated operating systems. But most attacks rely on end users. You will see in the report that the majority of breaches occur as a result of unauthorized access, which is directly related to user identity. Whether through brute-force attacks, phishing, password spraying, or other attack methods, unauthorized access to a single account can lead to unbridled network access, enabling attackers to search for and steal valuable data, such as customer records, intellectual property, or financial information.

It's also important to know how breaches can be prevented, and throughout the report, we've provided "best practices" sections to describe how to add layers of security that can thwart increasingly sophisticated attack methods.







How 2021 Compares to Prior Years

Because this is our fourth annual breach report, we can now see how trends are shifting. It's not always possible to ascertain why certain industries or geographies are trending upward or downward, but it's useful to evaluate the data based on what we do know:

- Billions of records are being exposed or stolen every year
- The cost of a data breach in the U.S. has risen each year, more than doubling between 2018 and 2021
- Unauthorized access continues to be the leading cause of breaches and has trended upward each year

Key U.S. Findings

297%

Increase in number of breaches due to third-party/supply chain

Almost 500 breaches in 2021 were caused by security issues associated with third-party suppliers, up from only 126 in 2020. This represents almost 25% of all breaches.

>2 billion

Usernames/Passwords breached

Records compromised containing username/password increased 35% in 2021 to more than two billion. Almost half of all records breached included some form of login credentials.

50%

Records breached by unauthorized access

For the fourth consecutive year, unauthorized access was the leading cause of breaches — 50% of all records breached — up from 45% in 2020.

$614

Per-record cost for healthcare

Healthcare continues to be the biggest target of breaches — at 24% — and the average cost per record was up sharply from $474 in 2020 to $614 in 2021.

$9.5M

Average cost of breach in the U.S.

The average cost of a breach in the U.S. was still the highest in the world, at $9.5 million, up 16% from $8.2 million in 2020.

63%

Increase in retail breach costs

The average cost of a retail breach jumped from $2.01 million in 2020 to $3.27 million in 2021.

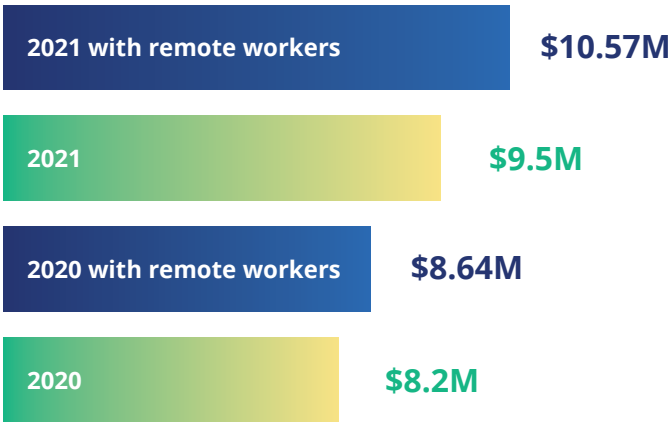
Data-Rich Breaches are Rising — In Numbers and Cost

Total Records Compromised

The total number of records compromised rose by 37% — and they are increasingly data-rich: 99% contained name/address, 59% Social Security number (SSN), 53% date of birth (DOB), 34% Protected Health Information (PHI), and 28% payment or banking information.

Average Cost of a Breach

The average cost of a breach in the U.S. increased by 16%. There was a greater cost for organizations with remote workers. It's clear the remote working trend is here to stay; more than 50% of American workers now work remotely, at least part-time.[8]



Mega breaches — those in which more than a million records become compromised — cost more than the average breach

The largest breaches, involving more than 50 million records, cost an average of $401 million, and even the relatively small breaches of one million records saw a cost increase of 4%, from an average of $50 million per breach in 2020 to $52 million in 2021.[9] We found 54 mega breaches — fewer than last year — meaning that many more small companies (500 employees or fewer) were breached. Smaller organizations can no longer afford to convince themselves that they won't be targeted by cybercriminals.

Breach costs include detection and escalation, notification, lost business, and post-breach response. The cost of, and the difficulty of recovering from, reputation harm is hard to quantify, but is no less real for organizations that find themselves in the headlines for negative reasons.

BEST PRACTICES:

Reduce the Cost of Breaches with AI

Organizations can reduce the cost of breaches by nearly 80%[13] by using artificial intelligence (AI) to quickly identify and contain unauthorized access. Identity and access management (IAM) solutions infused with AI can help you:

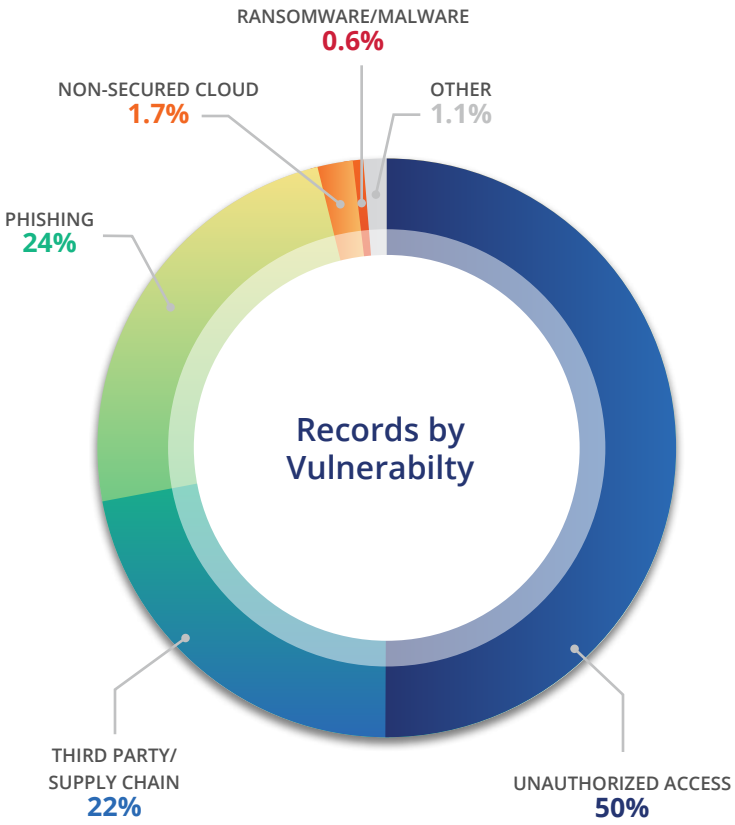
1. **Prevent infiltration –** Leverage AI and machine learning (ML), advanced pattern recognition, and behavioral analytics to stop known bad actors in real time, at the point of user authentication.

2. **Prevent data exfiltration –** Ensure that the right access roles, entitlements, and policies are in place within your organization to protect against unauthorized or overprovisioned access. You can use AI and ML along with identity governance to identify high-risk or unnecessary access (such as bad or duplicate roles, overprovisioned entitlements, etc.) and automate the revocation of these types of high-risk access.

Future costs also need to be factored in. One factor is the expectation of larger fines related to the EU General Data Protection Regulation (GDPR) privacy law, which increased in 2021. The number of fines increased, as did their size, to €1.1 billion in 2021, up from €158.5M in 2020.[10] Lawsuits will also continue to factor into rising costs. The $1.4B Equifax data breach class-action settlement of $425M was upheld in June 2021[11] — and two class-action suits against T-Mobile are being litigated on behalf of more than 50 million affected customers.[12] Most of these lawsuits claim that the organization failed to secure and safeguard sensitive client and employee data.

Attack and Data Types

Unauthorized access was once again the most common attack method, representing 50% of records breached. Supply-chain attacks often involve the compromise of outdated systems. Organizations need to make sure their suppliers have secure, up-to-date systems, lest they fall prey to attacks such as that of Accellion, a U.S.-based software provider whose 20-year-old file-sharing software was targeted by cybercriminals.[14]



Unauthorized Access

Unauthorized access is the attack vector responsible for almost half the number of records breached last year. Individuals can gain unauthorized access to data, networks, applications, or devices due to weak passwords, shared credentials, or compromised accounts.

Third-Party and Supply-Chain Attacks

Third-party and supply-chain attacks accounted for 25% of the records breached. Ransomware and phishing continued their seemingly inexorable rise in terms of number of records breached, the former driven "to levels we haven't seen in more than a decade,"[15] according to the U.S. Internal Revenue Service (IRS). This rise was in part related to the many COVID scams and fraudulent promises of stimulus payments. Phishing was responsible for 23% of the records breached (compared to less than 1% in 2020).

Social Media

Social media is fast becoming a weak link in security. As people overshare information in their own social media accounts, they make it easy for cybercriminals to find data that helps breach businesses. And as businesses increasingly use social media to connect with customers, they face two types of risks. First, they are at risk of criminals targeting their employees and businesses by impersonating the brand in order to steal credentials.

Second, scammers often try to infiltrate the business' social networks by using mutual connections and acquaintances to develop a false sense of security. Given the wealth of information obtainable, it's no wonder that more than 40% of the records breached came from the social media sector compared to 25% in 2020.

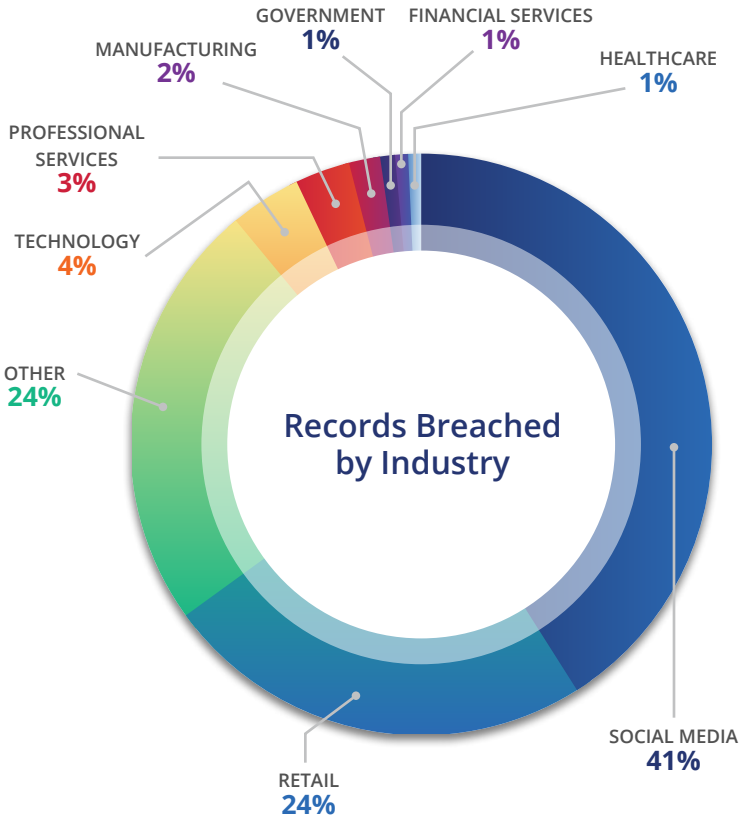
Retail

E-commerce sales grew by 50% during the pandemic, according to the U.S. Department of Commerce Retail Indicator Division.[16] At the same time, retail data breaches became more prevalent — and more costly. Retail accounted for more than one-quarter of all records breached in 2021. While the average cost of a retail breach in 2020 was $2.01 million, it jumped to $3.27 million in 2021, a 63% increase.[17]

The biggest target was customer information, such as credit card and payment information, along with personal information. As e-commerce sites and applications increasingly strive for an effortless user experience, they often omit security features such as two-factor authentication (2FA). And when the massive amounts of personal information collected by retail sites is poorly protected, it creates perfect conditions for breaches and subsequent fraud.

Healthcare

Healthcare accounted for less than 1% of all records breached, but those records contained valuable information including name, address, SSN, date of birth, and, in two-thirds of the breaches, actual medical history information. Armed with this data, cybercriminals have access to information on the patient's medical issues, diagnoses, treatments, and much more.



BEST PRACTICES:

Reduce Risk with MFA

Multifactor authentication (MFA) is a key weapon organizations wield to increase security. While consumers are becoming accustomed to MFA, requiring them to respond to an MFA prompt (such as a one-time passcode) after every login attempt creates clumsy and annoying user experiences that lead to more problems.

Attackers are weaponizing consumers' MFA fatigue through tactics such as "MFA prompt bombing,"[18] which sends multiple prompts in the hopes that a user will ultimately accept one of them, granting account access to the attacker. Good MFA requires strong phishing-proof methods, such as passwordless authentication, and an IAM solution that has enough intelligence to know how and when to require added authentication. Layering on AI, machine learning, and advanced pattern recognition provides these capabilities to make access easy for legitimate users while blocking attackers.

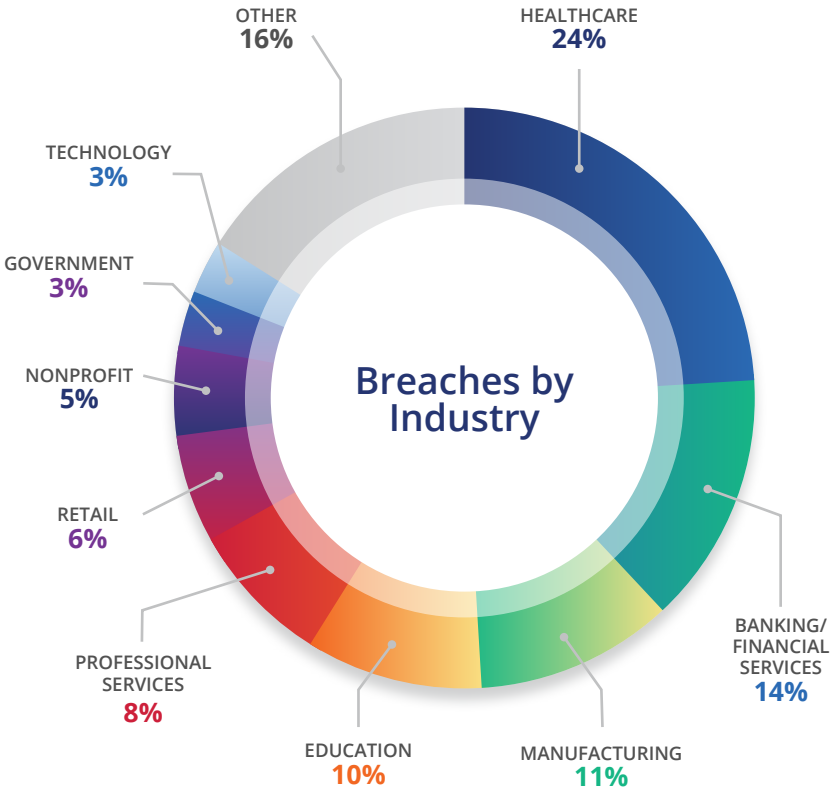
Vulnerabilities by Industry

It would be a mistake to assume that all industries were affected equally. Certain industries were much more vulnerable to one kind of attack than others.

- Retail experienced 99% of all records breached due to third-party attacks.
- Social media was the target of 85% of records breached due to unauthorized access.
- Healthcare represented 70% of all records breached by ransomware attacks.
- The financial services industry saw 10% of all records breached by ransomware attacks, but experienced 22% of all phishing attacks and 19% of unauthorized access attacks.

Number of Breaches by Industry in 2021

The previous section examined records breached by industry. Now the focus shifts to the number of breaches, regardless of how many records were involved in each breach. This is an important metric because any breach, even one that involves relatively few records, must be dealt with quickly and vigorously by the affected organization. Each requires the same discovery, mitigation, and reporting requirements, regardless of size. Here, the data shows that for the fourth year in a row, healthcare was the biggest target. It experienced the highest number of breaches at 467, accounting for 24% of all breaches. The second-most-targeted industry was financial services at 14%, followed by manufacturing at 11%, education at 10%, and retail at 6%.



Retail

Retail saw a slight uptick in the number of breaches, 6% in 2021 vs. 5% in 2020, yet it represented 26% of all records compromised (up from 16% in 2020 and a mere 2% in 2019).

Social Media

Social media represented less than 1% of the breaches in 2021, yet, due to the very large number of records involved, the sector paid 34% of the total $744 billion in breach costs.

Healthcare

Healthcare accounted for 24% of breaches. In addition to being the most popular target, it was the costliest industry per record. The per-record cost to recover from a breach in healthcare rose from $474 in 2020 to $614 in 2021, by far the highest of any sector.

Government's Role in Protecting Consumers

Organizations need to reduce post-breach customer churn, which represents 38% of the recovery cost.[20] By providing timely notification, consumers are more likely to stay with a business.[21] Unfortunately, despite governmental regulations around the world that require quick notification of affected parties, the typical time from breach identification to customer notification is 90 days. Yet, more than 60% of consumers want organizations to notify them immediately and take measures to ensure that a similar breach won't occur in the future.[22]

The U.S. is taking steps to increase transparency: President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 with mandatory requirements to report to the federal government within 72 hours if any substantial cybersecurity incident occurs, including unauthorized access.

Implemented in 2018, GDPR has been effective in making organizations pay attention to data protection law and enforcement. Fines jumped seven-fold in 2021 over the previous year.[23]

The Australian Federal Government has pledged AU$1.67 billion toward cybersecurity over ten years and has increased its investment in technology. These steps have been taken to provide greater support for businesses wishing to invest in digital technologies and create greater avenues for cybersecurity investment.

Singapore has likewise implemented new frameworks and regulations. The Personal Data Protection Regulations 2021 have been amended to clarify what constitutes significant harm for data breach reporting, and what steps should be taken to prevent mishandling of personal data.

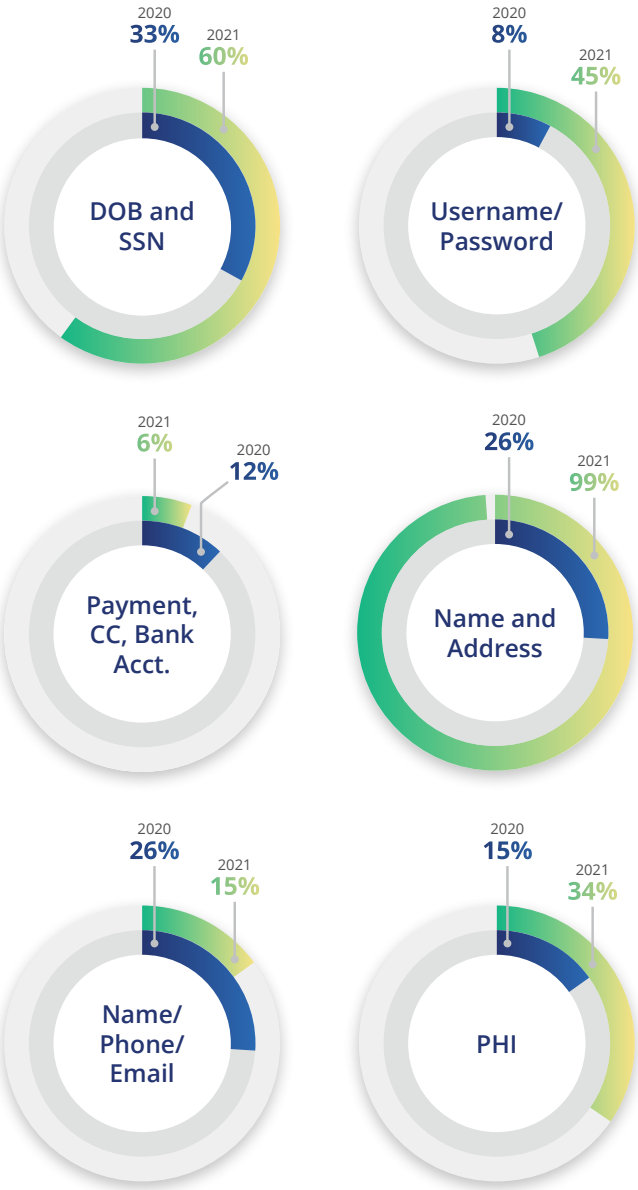
Based on the findings of this report and the simple reality that data breaches are not abating — far from it — there is much more to be done. Government and industry must work together to create stronger protections for consumer data and ensure transparency in the event of a breach.

BEST PRACTICES:

Reduce the Attack Surface with Zero Trust

To stem the tide of breaches, every organization should implement a Zero Trust approach, where all implicit trust (such as being on the network) is removed and access is evaluated dynamically and continuously. In a Zero Trust model, organizations operate under the assumption that their networks and services, regardless of location, are already compromised, and that every user and resource must be authenticated and authorized by evaluating multiple signals over time. This continuous assessment weakens the ability of attackers to infiltrate your network and move laterally because it instantly revokes any "trust" granted, giving attackers nowhere to go.

IAM best practices, such as MFA and AI-powered access management, authentication, and authorization are fundamental factors for achieving Zero Trust. If you, like most organizations, operate a hybrid IT environment, choose an IAM solution that can provide full visibility and advanced identity capabilities across legacy and cloud-delivered systems.[19]



Types of Data Compromised

We saw a huge increase in the amount of valuable personally identifiable information (PII) contained in breached records in 2021.

A full 60% of all records breached included SSN, DOB, or both — a sharp rise from the 33% seen in 2020. In 2020, 1.5 billion records containing login credentials were breached. The number rose to more than 2.1 billion records in 2021.

Usernames, passwords, and anything that can serve as a unique identifier (or easily be combined with other data to make one) could directly drive new breaches. This is especially true if the data constitutes a visibly true fact about someone (meaning it makes a poor secret) or is otherwise reused/reusable (as passwords often are, making them poor secrets as well). Personal data can be used in social engineering attacks to crack open a door to sharing credentials or other valuable data. Cybercriminals can perpetrate fraud using poorly protected data: for example, personal health information combined with other personal information can drive insurance fraud.

The only categories to decrease in 2021 were payment/ credit card/banking information, where the number of records breached dropped by 47%, and those containing name/phone/email dropped from 26% to 15%.

BEST PRACTICES:

Creating Strong Security and a Smooth User Journey

Organizations are in a bind: they need to provide a seamless online experience (expected by 60% of users) as well as security (a top priority for 55% of users).[24] However, the same report that revealed this data showed that consumers will abandon a transaction if they have to wait more than 30 seconds.

To provide a low-friction user experience with strong security, businesses should orchestrate secure and personalized login experiences using an IAM platform infused with AI, which detects unexpected activity and blocks inappropriate access using precision techniques that preserve access — and online experiences — for legitimate users.

UK Data Security in Focus

An accelerated national digital transformation in 2021 brought on by continued COVID disruption has kept the UK on high alert for hacker activity

The UK is no stranger to cyberthreats. Reported attacks in 2021 have continued at the same pace as they did in 2020 when a huge digital shift caused by the pandemic saw an unprecedented surge of malicious online activity.

Leading brands are deploying resources to make precautionary assessments of the problem:

Tesco,[25] for example, conducted a cyberattack "stress test" and found that a breach could cost the company up to £2.4B in fines.

As a consequence of the continuing threat level and the assets at stake, more UK businesses are treating cybersecurity as a priority issue within senior management discussions — the UK Government Cyber Security Breaches Survey 2022[26] found 82% of businesses did in 2021, compared to 77% in 2020.

Healthcare systems fight both medical and cyberthreats as IT systems become a key target for cyberattacks

The threat landscape facing businesses in the UK is complex. Analysis of data from the UK's independent data regulator, the ICO, covering breaches across 21 sectors over the period January to September 2021 shows that retail was the most vulnerable area, comprising 20% of all attacks. This period coincided with the UK's third national COVID lockdown, a time of mass online migration as brick-and-mortar shop fronts closed sometimes temporarily and sometimes for good.

According to the Office for National Statistics (ONS),[27] 37% of retail sales took place online in January 2021, compared to just 20% at the same time in 2020. This increase forced a digital shift across business functions: 82% of UK companies used online bank accounts in 2021 compared with 75% in 2020, while the percentage accepting online payments increased from 23% to 30%.[28] Inevitably, this digital shift brought with it a corresponding increase in malicious actors prowling the digital corridors — and vulnerability on the part of retailers as they scrambled to adapt.

Other sectors faced similar challenges. Healthcare, finance, and education accounted for 9.4%, 12%, and 11% of attacks, respectively. Healthcare merits a closer look: the COVID pandemic has led to massive organizational stress on the UK's National Health Service (NHS), including in IT, where cybersecurity teams have had to protect an unprecedented quantity of sensitive patient and public data in addition to their BAU remit.

Cybersecurity stakes are always high, but perhaps never more so than in healthcare.

65 out of 100[29] surveyed cybersecurity managers in the UK healthcare sector believe that a cyberattack on their system could lead to loss of life.

No wonder then that leaders of integrated care systems in the NHS were served with a reminder in September 2021 by their technological arm, NHSX[30], to ensure that all digital projects were "cyber secure by design."

The UK must watch out for phishing attacks as the leading threat vector that is putting identity data at risk

Analysis of threat types reveals an informative picture too. The most common threat type for 2021 was phishing, which accounted for 38% of all incidents between January and September. Again, circumstance provides the explanation: text and email notifications were widely used in the UK's national vaccine rollout and phishers didn't fail to notice this opportunity.

The National Cyber Security Centre Annual Report[31] reveals the scale of the problem: its defense program took down 442 phishing campaigns using NHS branding, and 80 illegitimate NHS apps hosted and available to download outside of official app stores. Of course, phishing is not exclusive to healthcare, and over the summer of 2021, Ofcom[32] found that almost 45 million

people had received a scam text or call, with 82% of adults receiving a suspicious message via text.

Key Takeaways for the UK

Looking at the big picture, the cybersecurity landscape remains challenging across verticals. Behavioral shifts fueled by the pandemic have accelerated many businesses' digital transformations and encouraged a continuation of very high levels of malicious activity. Every sector has been affected, but retail and healthcare are key areas of concern in the UK due to the rapid acceleration of online interactions with patients resulting from the pandemic.

How businesses respond will be crucial. Many sectors will likely face a period of constrained spending power, so efficiency and power multiplication tools will be key. Organizations that harness AI to add to cybersecurity teams' firepower by monitoring login requests in real time and blocking malicious requests can streamline journeys for legitimate users. AI tools also allow businesses to maintain a suitable security posture without needing unsustainable increases in human resources.

Germany Data Security in Focus

The overall IT security situation in Germany was under extreme pressure in 2021. The year was characterized by attacks on critical infrastructure, public infrastructure, and administration and supply chains. German authorities recorded a noticeable expansion of cybercriminal extortion methods. The number of recorded cybercrimes in Germany increased by more than 12% in 2021 over 2020.[33] Phishing attacks specifically increased by 40%.[34]

With the rise in cybercrime, the potential damage of ransomware attacks also grew rapidly, from around €5.3 billion in 2019 to €24.3 billion in 2021, a staggering rise of more than 350%.[35]

The German Federal Office for Information Security (BSI) observed targeted IT attacks related to COVID across the healthcare sector. These included attacks on the European Medicines Agency (EMA), foreign vaccine manufacturers, a DDoS attack on the vaccination portal of the German state of Thuringia, and a ransomware attack on a German manufacturer of antigen tests. The EMA attack also demonstrates the growing importance of the "human vulnerability" as a gateway for cyberattacks. In this specific case, two-factor authentication was used for service provider access to the EMA system, but the user of the attacked client had stored both factors on the client, thereby undermining the security effect.[36]

"Big Game Hunting": The BSI observed numerous hacking groups shifting their focus to financially strong targets in a tactic often called "Big Game Hunting." In this attack scheme, cybercriminals focus on companies with high-value data or assets in industries such as healthcare, government, or manufacturing. They target companies that are sensitive to downtime and will be more likely to pay a ransom, regardless of the cost.[37]

The first cyber-disaster case: One of the most prominent attacks on public infrastructure in 2021 unsurprisingly included ransomware. The district administration of Anhalt-Bitterfeld (Saxony-Anhalt) was paralyzed by a cyberattack to the extent that it could not pay social and maintenance benefits to citizens (e.g., student aid, parental and child benefits) for more than a week. The administration installed an emergency infrastructure system in an attempt to work around the attack. However, even months later, regular operations were not functioning. The attack led to the first declaration of a cyber-disaster case in Germany.[38]

Combination of ransomware and data leaks: Attacks using ransomware typically carry the risk of a data leak, usually accompanied by the outflow of personal data and corresponding hush-money extortion. In practice, the two outcomes are becoming increasingly blurred, as cybercriminals tend to publish the stolen data from a ransomware attack on DarkNet platforms as a second dimension in their attack scheme.[39] This trend is reflected by the number of monthly active data leak sites, where stolen data is made available to the public and other attackers for further cyberattacks. The number of such sites increased by almost 360%.[40] According to the Hasso Plattner Institute, which has been recording data leaks

of compromised accounts since 2006, approximately 184.65 million user accounts were compromised in 2021.[41]

Massive data leak in German online shops: More than one million data records of an estimated 700,000 users throughout Germany were affected by a massive data leak in 2021. The haul of personal data included postal addresses, order information, telephone numbers, and, in some cases, bank details. The data leak was detected during troubleshooting by an outside IT specialist in the summer of 2021, and the gap in protection was subsequently closed. However, it had been open for three years and left the data virtually unprotected on the internet during this time.

The marketplace provider for a number of leading German retailers had unwittingly been granting all of its customers access to the entire database, including the data of other retailers, meaning the retailers could view all customer orders, including the ones from their competitors. Moreover, the data required for server access had been stored in plain text in the software. Outsiders were thus able to download the information from the marketplace provider's website, and practically anyone could have accessed the highly sensitive user data.[42]

As in many other countries, the cost associated with a data breach has gone up in Germany in the last year — from $4.45 million to $4.89 million (equal to around €4.64 million). In the last year, a new record was set for GDPR fines issued against companies that didn't adhere to compliance policies. Across the EU, companies paid approximately €1 billion due to GDPR violations, a stark increase compared to just under €170 million the previous year. In Germany, specifically, GDPR fines totaling around €50 million were issued last year.[44]

Principal Points for Germany

The German data from 2021 clearly indicates that the risk of theft of credentials and the loss of sensitive data is higher than ever. The increasingly popular combination of ransomware attacks and leaked data on DarkNet sites makes passwordless authentication with mobile authenticators, FIDO2 security keys, and fingerprint readers or cameras imperative for corporations and individuals who want to significantly reduce the usefulness of stolen passwords. An additional component to mitigate the risk of data breaches is the adoption of a Zero Trust strategy. Passwordless authentication should be incorporated into any Zero Trust strategy with no compromise. Such strategies incorporate geo-fencing and other parameters into authorization decisions and grant read-only access or invoke additional authentication from untrusted devices.

Australia Data Security in Focus

According to the Australian Government's Office of the Australian Information Commissioner Notifiable Breaches Report,[45] the total number of disclosed breaches dropped 15% in 2021. The country reported 900 successful breaches last year, compared to 1,057 the year before.

Despite the decrease, this number is still higher than 2018's total reported breaches, at 812, a 10% increase in the years between 2018 and 2021.

The top industries affected by data breaches were healthcare, at 168 reported breaches, followed by finance at 113, and legal, accounting, and management services at 86. The healthcare industry has continually reported the highest number of breaches since the start of the Notifiable Data Breaches (NDB) scheme.

What the decrease in breaches may tell us, however, is that Australian businesses and government agencies, alongside individuals, are becoming more vigilant when it comes to cybersecurity.

Both the healthcare and finance reporting numbers decreased by 29% (238 in 2020) and 27% (155 in 2020), respectively. On the other hand, the legal, accounting, and management service reports increased by 34% (64 in 2020), replacing the education sector from 2020 as the third-most-breached industry.

For a third year, personal contact information (home addresses, phone numbers, or email addresses) remained the most frequently sought-after information in data breaches, comprising 803 reported breaches. This was followed by identity information at 432, health information at 256, financial details at 376, and tax file numbers at 184. In four out of five categories, the number of breaches reported decreased year-over-year, with the largest decrease of 13% for contact information reports. Tax file number breach reports stayed the same across 2020 and 2021.

COVID-related scams seen in 2021 by the Australian Competition and Consumer Commission[46] included those impersonating the government and phishing scams. These were predominantly via text or email, claiming to be a government department asking for personal details to confirm eligibility for a government payment or because the person may have been exposed to COVID. In addition, Scamwatch[47] received more than 6,000 scam reports mentioning coronavirus, with more than $9,800,000 in reported losses. Unfortunately, older Australians were the most likely to fall for these scams.

Increase in Investment in Cybersecurity

The decrease in overall reports of data breaches could be explained through the rise in cybersecurity spend in 2021. Given that there was an uptake in online services throughout 2020 as the physical world shifted online, we also saw an increase in cybercrime. As a result, in 2021, businesses began to increase their use of cybersecurity systems, as Australian businesses were expected to spend AU$4.9B on cybersecurity in 2021.[48]

The rise of remote work has pushed more businesses in Australia to invest in third-party hybrid working solutions, such as digital identity access and collaboration tools, hosted on more secure platforms potentially through the cloud, adding more layers of security.

Additionally, the Australian Federal Government has invested more into minimizing security risks, developing a series of Cyber Security Strategies. The most recent is a pledge of AU$1.67 billion[49] towards cybersecurity over ten years in 2020. The country has also invested more in technology in 2021, with an AU$1.2 billion investment into digital economies[50] and cybersecurity, offering greater support for businesses wishing to invest in digital technologies and creating greater avenues for cybersecurity investment.

Despite these investments, it's important to note that the number of incidents is still high relative to pre-pandemic days, with an increase of 10% over 2018. These numbers show that there is still a piece of the puzzle missing, and there is space for greater knowledge around cybersecurity and investment in the future.

Human error was the cause of 324 breaches, down from 380 in 2020. Yet, given it was the second-largest cause of breaches, there is still a need for greater education on security and password protection since there is a lack of knowledge around the importance of multifactor authentication and generating strong passwords in Australia.

Key Australian Insights

Although the total number of disclosed data breaches in Australia was down by 15% in 2021, breaches are still prevalent, and business and government must remain diligent in their efforts to prevent them. With the technology to combat cyberthreats evolving through developments in AI and the use of deeper methods of multifactor authentication, continued investment in cybersecurity measures will be crucial to protecting data moving forward.

Singapore Data Security in Focus

Singapore saw a dramatic 43% increase in cybercrime year over year. According to the most recent information, the 2020 Singapore Cyber Landscape report[51] released in July 2021,[52] shows more than 16,000 reported cyberattacks. [Note: The data for 2021 will not be released until July 2022, too late for use in this report.] The biggest contributor to these attacks was phishing scams, accounting for more than 12,000 incidents. The next leading attack method was unauthorized access, which was used in more than 3,600 cases in 2020 compared to 1,701 in 2019. Cyber extortion was the third-most-common approach, used in 245 attacks versus 68 the previous year.

Singapore saw a significant rise in ransomware targeting the manufacturing, retail, and healthcare sectors, with a total of 89 cases reported to the CSA in 2020, an increase of 154% over the 35 cases reported in 2019.

Website defacements, on the other hand, saw a sharp decrease in 2020. Just under 500 ".sg" websites were defaced a year ago, down 43% from 873 cases in 2019.

About 47,000 unique phishing URLs were observed in 2020, a slight decrease compared to the three-year record high of 47,500 URLs seen in 2019. In 2020, government bodies in Singapore commonly spoofed included the Ministry of Education (MOE), Ministry of Manpower (MOM), and the Singapore Police Force (SPF), while technology, the banking and financial services industry, and social networking firms were the main sectors attacked. These include large technology or social networking firms and entities in the banking and financial sector.

Why is the Risk so High?

As people and businesses continued to balance work-from-home or hybrid arrangements, and businesses adopted digital technologies to ensure business continuity, these trends led to more cyberattack vectors and attempts.

Over the years, we have seen several Singapore-based businesses targeted by hackers, resulting in a series of data breaches involving sensitive customer data, from the SingHealth data breach in 2018 to the OCBC phishing scam earlier this year. There were several attempts to exploit individual vulnerabilities by posing as government or health agencies, creating websites for credential theft, malware distribution, and fraudulent peddling of fake cures and vaccines.

COVID also played a role. The Ministry of Manpower (MOM)[53] highlighted three major scams that impacted Singaporeans in regard to COVID vaccinations, false-positive COVID results, and phone calls claiming to be from the MOM. Scammers sought contact details, personal information, and banking details of individuals; they also encouraged the downloading of fake positive-result email attachments of foreign workers.

As ransomware cases continue to impact individuals and businesses in Singapore, people and organizations need to be vigilant against cyberthreats, looking beyond backing up data and storing it online. Companies need to focus on implementing preventive measures, such as protecting their infrastructure through passwordless authentication to improve end-user experience.

New Frameworks and Regulations Being Introduced

Businesses should take note of the amendments to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 and Personal Data Protection Regulations 2021 that were made in October 2021. These include minor clarifications to what constitutes significant harm for mandatory data breach reporting, defenses for egregious mishandling of personal data, and on the ways that organizations may provide the business contact information of their Data Protection Officers.

To meet the challenges posed by cybercrime, in 2021 Singapore announced an update of its cybersecurity strategy[54], outlining plans to take a more proactive stance to address cyberthreats, raise the overall level of cybersecurity across the nation, and advance international norms and standards on cybersecurity. The 2021 updated strategy comes five years after the launch of the first strategy in 2016, addressing new and emerging threats in the wake of strategic and technological shifts.

In February 2022, the Monetary Authority of Singapore (MAS) also shared a new framework[55] that looked into equitable sharing of losses arising from scams. It announced measures to strengthen the security of digital banking and highlighted how all parties have a responsibility to be vigilant and take precautionary measures against scams.

In February 2022, the Monetary Authority of Singapore (MAS) also shared a new framework[55] that looked into equitable sharing of losses arising from scams. It announced measures to strengthen the security of digital banking and highlighted how all parties (organizations and people) have a responsibility to be vigilant and take precautionary measures against scams.

In April 2022, the Cyber Security Agency of Singapore (CSA) kicked off a licensing framework[56] for cybersecurity service providers to better safeguard consumers' interests.

Key Singapore Insights

Singapore has one of the highest internet adoption rates.[57] In 2020, close to 90% of the Singapore population was using the internet. By 2025, adoption is projected to grow to more than 93%. The country is also working towards nationwide 5G coverage by 2025.

With digital services continuing to see adoption and growth by both individuals and businesses, cyberattacks are expected to continue to increase.

However, we are seeing several agile measures being introduced by the Singapore government to deal with the constant, always-on threat of these attacks to provide better assurance of security, safety, and privacy to consumers.

Conclusion

In 2021, the world saw a massive escalation in data breaches, both in number and in severity. Cybercriminals took advantage of the unstoppable trend of consumers living their lives online to gain unauthorized access by using stolen credentials and leveraging weaknesses in authentication and authorization. Using previously breached data, including usernames, passwords, dates of birth and Social Security numbers, they were able to tap into a rich vein of additional personal information held in online shopping, social media, healthcare, and other sites.

Consumers have been educated to avoid clicking on suspicious links, to think twice before opening an attachment, and to safeguard their credentials — yet inattention and fatigue often get in the way of good security practices. Anything people do by rote is susceptible to carelessness. That's why giving consumers more control over authentication methods and notifications invests them further in the process and increases their awareness. Multifactor authentication (MFA) is another way to increase authentication security and its usage is increasing. But requiring MFA after every login attempt creates a tedious experience, raises the risk of customer frustration and abandonment, and even leads to a new attack method, MFA prompt bombing.

While these efforts seem to have resulted in progress in some industries — witness the 75% drop in the number of financial services industry records breached — other industries such as professional services are rapidly becoming a primary target of cybercriminals. The healthcare sector continues to be a rich target, perhaps due to the amount of personal information contained in medical and health insurance records.

It's clear that we need to do more to attack both sides of the identity challenge: increase consumer data security while providing a seamless user experience. The keys to ensuring smooth online access to trusted users while preventing unauthorized access are available today: artificial intelligence (AI), passwordless authentication, and a Zero Trust approach.

AI-Based Access Management

Ensure a frictionless user journey: don't penalize legitimate users just because cybercriminals continue to attempt unauthorized access. Stop fraudulent access before it happens by using an AI-based access management system to detect anomalous behavior. AI/ML functionality incorporated into IAM can provide rich contextual insight into potential risks associated with attempted access on the basis of massive amounts of data. When fraudulent access is being attempted, it can be cut off, while providing legitimate users a seamless online experience.

Passwordless Authentication

The world has moved far beyond the point where a simple password could provide sufficient protection. Spurred by the FIDO2 WebAuthn standard, the move to passwordless authentication is gaining momentum; it improves both security and ease of use for online access, while greatly diminishing the usefulness of stolen credentials by cybercriminals. The industry's biggest players — Apple, Microsoft, and Google — have helped with expanding the FIDO2 standard, announcing plans to enable passwordless authentication across multiple devices, browsers, and platforms.[58]

Zero Trust

Wise organizations operate under the assumption that their networks are already compromised. That's why they take a Zero Trust approach, in which each transaction or activity is assessed individually, based on a continuous evaluation of multiple signals rather than network location. A Zero Trust strategy should include both a comprehensive IAM solution and automated role-based access management capabilities that enforce least-privileged access.

These three approaches hold the promise of meeting consumers' stated desire for both security and a seamless online experience. They focused on reducing the number and severity of breaches while increasing customer trust in organizations with which they do business. Gartner predicts the following: "By 2025 adoption of CIAM with converged fraud detection and passwordless authentication will be able to reduce customer churn by more than half."[59]

[1] Identity Theft Resource Center. "2021 Annual Data Breach Report." IDTheftCenter.org. January 2022. Accessed June 2022.
[2] Ponemon Institute and IBM. "Cost of a Data Breach Report 2021." IBM.com. 5 August 2021. Accessed June 2022.
[3] Page, Carly. "The Accellion data breach continues to get messier." TechCrunch.com. July 8, 2021. Accessed June 2022.
[4] Maxim, Merritt. "Okta Lapsus$ Compromise: How to Make Sure You're Protected." Forrester.com. March 24, 2022. Accessed June 2022.
[5] Tyas Tunggal, Abi. "The 65 Biggest Data Breaches." UpGuard.com. Updated Jun 26, 2022.
[6] Bekker, Eugene. "2021 Data Breaches." IdentityForce.com. January 11, 2021. Accessed June 2022.
[7] Hill, Michael and Swinhoe, Dan. "The 15 biggest data breaches of the 21st century." CSO Online. 16 July 2021. Accessed June 2022.
[8] Verasai, Anna. "Remote Work is Here to Stay: Are You Ready?" TheHRDigest.com. 15 January 2022. Accessed June 2022.
[9] Ponemon Institute and IBM. "Cost of a Data Breach Report 2021." IBM.com. 5 August 2021. Accessed June 2022.
[10] Delić, Danka. "Record fines for breaches of EU privacy law in 2022 – over €1.1 billion in just a year." ProPrivacy.com. 21 January 2022. Accessed June 2022.
[11] Bronstad, Amanda. "11th Circuit Upholds $1.4B Class Action Settlement Over Equifax Data Breach." Law.com. 3 June 2021. Accessed June 2022.
[12] Bronstad, Amanda. "T-Mobile Hit with Two Class Actions Over Massive Data Breach." Law.com. 20 August 2021. Accessed June 2022.
[13] Ponemon Institute and IBM. "Cost of a Data Breach Report 2021," IBM.com. Accessed June 2022.
[14] Page, Carly. "The Accellion data breach continues to get messier." TechCrunch.com. 8 July 2021. Accessed June 2022.
[15] Rowan, Lisa. "Stimulus Check Scams Account for Highest Level of Phishing Attempts in More Than a Decade." Forbes.com. 1 September 2021. Accessed June 2022.
[16] United States Census Bureau. "Monthly Retail Trade (PDF)." Census.gov. Accessed June 2022.
[17] Ponemon Institute and IBM. "Cost of a Data Breach Report 2021," IBM.com. Accessed June 2022.
[18] Jenkins, Luke; Hawley, Sarah; Najafi, Parnian, Bienstock, Doug. "Suspected Russian Activity Targeting Government and Business Entities Around the Globe." Mandiant.com. 6 December 2021. Accessed June 2022.
[19] "Digital Identity: The Foundation of Your Zero Trust Strategy." ForgeRock.com. Accessed June 2022.
[20] Ponemon Institute and IBM. "Cost of a Data Breach Report 2021," IBM.com. Accessed June 2022.
[21] Davis, Jessica. "Prompt Notification Reduces Data Breach Fallout, Consumer Impact." HealthITSecurity.com. 5 September 2019. Accessed June 2022.
[22] Ablon, Lillian; Heaton, Paul; Lavery, Diana Catherine; and Romanosky, Sasha. "Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information." 2016. Accessed June 2022.
[23] Browne, Ryan. "Fines for breaches of EU privacy law spike sevenfold to $1.2 billion, as Big Tech bears the brunt." CNBC.com. 17 January 2022. Accessed June 2022.
[24] Experian. "2021 Global Identity and Fraud Report." Experian.com. April 2021. Accessed June 2022.
[25] Armstrong, Ashley. "Tesco fears £2.4bn hit from future cyberattack." TheTimes.co.uk. 14 May 2022. Accessed June 2022.
[26] Ell, Maddy and Gallucci, Robbie. "Cyber Security Breaches Survey 2022." Gov.uk. 30 March 2022. Accessed June 2022.
[27] Lewis, Rhys. "Retail sales, Great Britain: January 2022." ONS.gov.uk. 18 February 2022. Accessed June 2022.
[28] Cyber Security Breaches Survey 2022, Op. cit.
[29] Coker, James. "81% of UK Healthcare Organizations Hit by Ransomware in Last Year." Infosecurity-magazine.com. 20 October 2021. Accessed June 2022.
[30] NHS. "What Good Looks Like Framework." NHSX.NHS.uk/. 4 October 2021.Accessed June 2022.
[31] National Cyber Security Centre. "Record number of cyber incidents mitigated as NCSC protects vaccine rollout." NSCS.gov.uk. 17 November 2021. Accessed June 2022.
[32] "45 million people targeted by scam calls and texts this summer." Ofcom.org. 20 October 2021. Accessed June 2022.
[33] BKA. „Cybercrime – Bundeslagebild 2021". BKA.de. 2021. Accessed June 2022.
[34] "2022 ThreatLabz Phishing Report" (PDF). Zscaler.com. 2022. Accessed June 2022.
[35] BKA 2022, Op. cit. Accessed June 2022.
[36] „Die Lage der IT-Sicherheit in Deutschland 2021." BSI 2022 (The report covers the time period June 2020 until May 2021.)
[37] Ibid
[38] Heinrich Böll Stiftung; "Cyberangriff auf Landkreis Anhalt-Bitterfeld 2021 – KommunalWiki." Accessed June 2022.
[39] BSI 2022, Op. cit.
[40] BSI 2022, Op. cit.
[41] Hasso Plattner Institut (HSI), "Statistics." Accessed June 2022.
[42] Taggesschau. "Massives Datenleck Nutzerdaten jahrelang online." Accessed June 2022.
[43] Ponemon Institute and IBM. "Cost of a Data Breach Report 2021." Accessed June 2022.
[44] Statista 2022, and TÜViT, 2022. Accessd June 2022.
[45] Office of the Australian Information Commissioner. "Notifiable Data Breaches Report: January–June 2021." OAIC.gov.au. 23 August 2021 and "Notifiable Data Breaches Report: July–December 2021." OAIC.gov.au. 22 February 2022. Accessed June 2022.
[46] Australian Competition & Consumer Commission. "Current COVID-19 (coronavirus) scams" (PDF). ACCC.gov.au. June 2020. Accessed June 2022.
[47] Australian Competition & Consumer Commission. "Current COVID-19 (coronavirus) scams." ACCC.gov.au. Accessed June 2022.
[48] Karen, Sasha. "Aussie cyber security spend to hit $4.9B in 2021." ARNnet.com.au. 22 March 2021. Accessed June 2022.
[49] "Australia: Government allocates AUD 1.67 billion for 2020 Cyber Security Strategy." GlobalTradeAlert.org. 6 August 2020. Accessed June 2022.
[50] Bushell-Embling, Dylan. "Govt unveils $1.2bn Digital Economy Strategy." TechnologyDecisions.com.au. 7 May 2021. Accessed June 2022.
[51] CSA Singapore. "Singapore Cyber Landscape 2020." CSA.gov.sg. 8 July 2021. Accessed June 2022.
[52] The Singapore Cyber Landscape report is released in July of each year covering data from the previous year. The report for 2021 will not be available until July 2022, so this report covers data through December 2020.
[53] Ministry of Manpower Singapore. "Advisories on COVID-19." Mom.gov.sg. 2022. Accessed June 2022.
[54] CSA Singapore. "The Singapore Cybersecurity Strategy 2021." CSA.gov.sg. 5 October 2021. Accessed June 2022.
[55] Monetary Authority of Singapore. "A Framework for Equitable Sharing of Losses Arising from Scams." MAS.gov.sg. 4 February 2022. Accessed June 2022.
[56] CSA Singapore. "CSA Kicks Off Licensing Framework for Cybersecurity Service Providers." CSA.gov.sg. 11 April 2022. Accessed June 2022.
[57] DataReportal. Kemp, Simon. "Digital 2022: Singapore." DataReportal.com. February 2022. Accessed June 2022.
[58] Fido Alliance. "Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins." FidoAlliance.org. 5 May 2022. Accessed June 2022.
[59] Gartner. "Innovation Insight for Customer Identity and Access Management." Gartner.com. 9 December 2021. Accessed June 2022.

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**.

Follow Us