ForgeRock

2021 ForgeRock Consumer Identity Breach Report

The Year Of the Great Digital Migration:
How Usernames and Passwords Found Their Way Into the Crosshairs of Attackers

Executive Summary

The year 2020 witnessed a massive digital migration. People did almost everything online – purchasing goods and services, consulting with healthcare professionals, arranging for meal deliveries, distance learning, and, of course, working from home.

Meanwhile, malicious actors did not skip a beat. This year's report notably reveals that attacks involving usernames and passwords increased a staggering 450% over 2019, translating into more than 1 billion compromised records in the U.S. alone. With users spending more than double the amount of time online,[1] their tendency to reuse common passwords continued to make this attack vector extremely attractive to cybercriminals.

Surprisingly, even with all this online activity, the number of mega-breaches decreased in 2020 and, correspondingly, so did the number of records compromised. However, the total number of breaches increased. Those involving less than 100 million records shot up by 50%. For smaller enterprises hoping to be ignored or biding their time in adopting Zero Trust security, 2020 shows us that they must not wait. Cybercriminals are working their way into organizations of all sizes with the intent to seize valuable assets.

For the third year in a row, unauthorized access was the most reported type of breach (43%). Questionable yet common security practices, like sharing or reusing passwords, gave bad actors an easy path to gaining access to personally identifiable information (PII), such as date of birth (DOB) and Social Security Number (SSN) information, which is found in one third of all breaches.

Since last year's report, the average cost of a breach in the U.S. increased 5.5% to $8.64M, making the U.S. the costliest place in the world to recover from a breach. Around the world, organizations with remote workers paid a higher average cost per breach than those without a remote workforce, underscoring the vulnerability of the digital economy.

So, what have we learned? The year 2020 marks the third consecutive year that the weakest link in internet security is identity. The world's move to remote life significantly contributed to the increases in stolen data, proving that malicious actors are adaptable, nimble, and relentless. But it's possible to turn the tables on attackers by taking a few simple steps to implement identity and access management (IAM) best practices to ensure optimal security hygiene.

> U.S. breach costs continued to rise along with the number of records compromised, making it the most expensive country for breaches at $8.64 million and 1.48 billion records exposed. More than 11 billion consumer records have been exposed over the past three years.

This report shares detailed insights and data on the breaches impacting consumers in 2020 and provides year-over-year comparisons to breaches affecting consumers in the U.S. in 2019. It also includes findings from other key regions, including Australia, Germany, the United Kingdom (U.K.)., and, for the first time, Singapore. It clearly demonstrates the need for organizations to adopt a comprehensive identity and access management (IAM) solution to help prevent identity-related data breaches, protect their brands, and preserve customer relationships.

Eve Maler
Chief Technology Officer

[1] https://www.forbes.com/sites/johnkoetsier/2020/09/26/global-online-content-consumption-doubled-in-2020/?sh=48f540672fde

Key U.S. Findings

+450%

Increase in Username/Password Breaches

Breaches containing usernames and passwords increased 450% in 2020, totaling 1.48 billion breached records.

43%

of Breaches are Unauthorized Access

For the third consecutive year unauthorized access was the most common type of breach, accounting for 43% of breaches.

34%

of Breaches Targeted Healthcare

Healthcare was the most targeted sector, accounting for 34% of all breaches. This sector also had the highest average cost per compromised record at $474.

$288 B

Aggregate Cost of Recovery

The technology sector paid the highest aggregate cost of recovery at $288 billion, with more than 1.6 billion records stolen.

$8.64 M

The Average Cost of a Breach in the U.S.

The average cost of a breach in the U.S. was the highest in the world, at $8.64 million, up 5% from $8.19 million the year before.

2X

The Amount of Time Spent Online

The amount of time people spent online more than doubled, totaling more than seven hours per person per day.

Rising Cost of Breaches Calls for Advanced Security Processes

Total Records Compromised

Fewer records were compromised in 2020 than in 2019. This shift was a result of more targeted attacks, compared to the high-volume, opportunistic attacks seen in previous years.

Average Cost of Breach in U.S.

While the number of records compromised fell, the average cost of each breach went up slightly from 2019. In addition, the cost showed **a significant uptick for organizations with remote workers** due to the difficulty in detecting and responding to attacks aimed at devices used outside corporate networks.

Not all breaches are alike. Mega-breaches, defined as those involving more than one million records, generally cost more than 25 times the average. Breaches of more than 50 million records cost more than 100 times the average. One trucking company claimed that a single breach cost it $7.5 million just in lost revenue. Costs to the company also included initiating response protocols, launching an

Stop, Drop, and Role

Three Things All Enterprises Should Be Doing to Reduce Breach Threats

1 Stop Using Static Passwords

Systems and applications protected with simple user-generated passwords are the ultimate attack vector for ransomware, phishing, and a host of other attacks.

2 Drop Into Your Users' Experience

Check out how your workforce and consumers are accessing their applications. Options now exist for passwordless, risk-based, and even contextual authentication that can improve security while also delivering a great logon experience for your users.

3 Role Cleanup

Examine your user roles. Too much access is a major contributor to breaches. Know what your user roles are, and remove any access that is not needed.

investigation, engaging forensic professionals, and assessing, containing, and remediating the attack.[2]

Future costs in the form of both fines and lawsuits may well impact the future costs of breaches. GDPR fines rose in 2020 by 40% to €158.5M. Most fines were levied for insufficient technical and organizational measures to ensure security. There is also a significant increase in the number and complexity of data breach lawsuits. In the U.S., 25 major data breach class action lawsuits were filed in 2020. Nearly every class action lawsuit for data breach claims negligence: failure to exercise reasonable care and failure to protect sensitive client and employee data.

There is a ray of hope, however. Organizations that use modern identity and access management (IAM), make use of artificial intelligence (AI) to detect unexpected activity, implement strong compliance controls, and insist on multi-factor authentication (MFA) have shown that they can reduce the cost of breaches. A Forrester report found that automated on-premises and cloud-based IAM solutions implemented over a three year time period provide a combined 776% ROI.[3] Advanced security processes such as these must be the focus going forward. Any measures that reduce the attack surface and enable quick response are must-haves in the arsenals of today's hybrid IT organizations.

solarwinds

The SolarWinds Attack

What We Know (So Far)

In early 2020, hackers broke into the SolarWinds systems and inserted malicious code into its software. Updates containing malware were then distributed to more than 30,000 customers around the world, including Fortune 500 companies and government agencies. This massive breach, resulting from unauthorized access, had a devastating impact: the malware created a backdoor to organizations running the SolarWinds software, allowing hackers uncontrolled access to their networks.

Undoubtedly, more information will be revealed over the coming months.

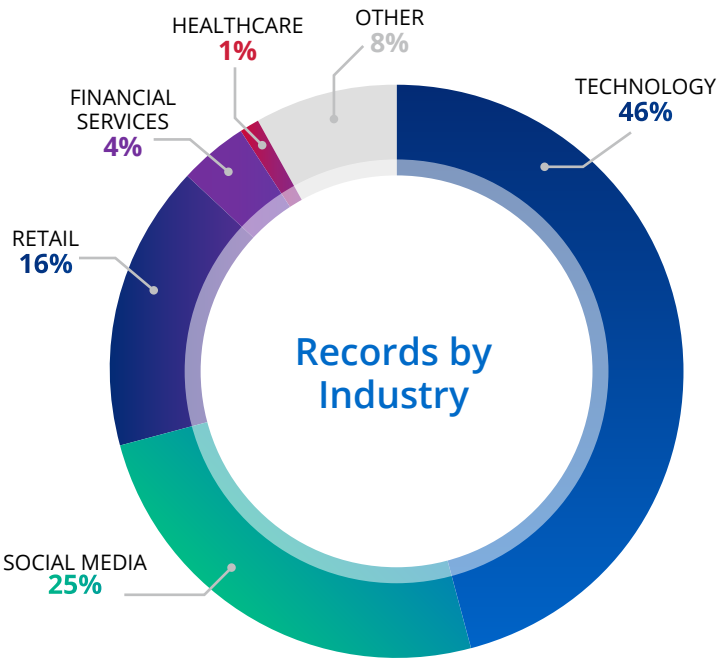
What It Taught Us

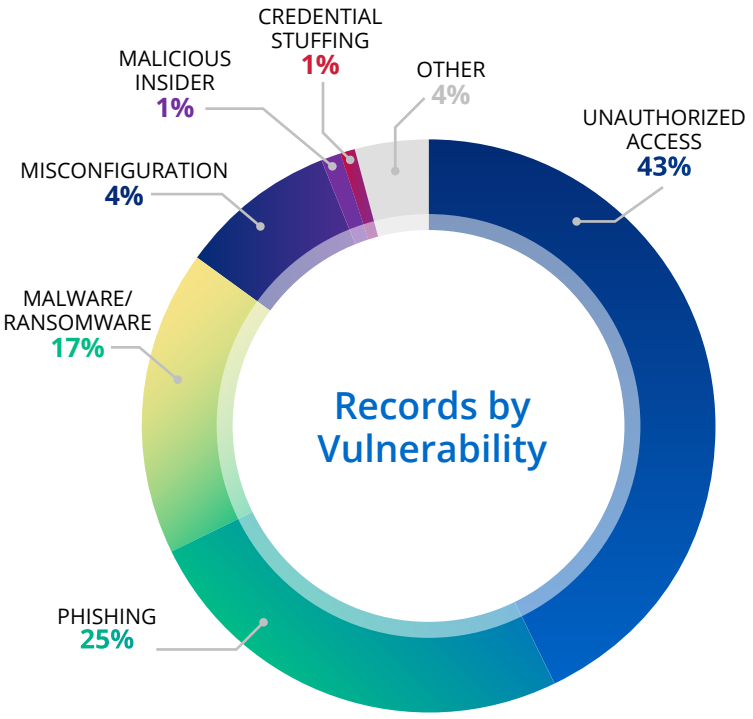
- **The SolarWinds hack introduced a new dimension.** It became apparent that the security practices of one organization may not just affect its own reputation and bottom line – they could also harm other businesses.
- **Trust but verify.** Even highly trusted credentials, like digital certificates, can be compromised and could become the delivery vehicle of the dangerous malware. It can no longer be taken for granted that all aspects of your digital supply chain are secure.
- **Implement IAM best practices.** This will contribute to "digital herd immunity." We also need to take time to understand how third parties secure the things that are used to establish mutual digital trust.
- **Secure each and every application with a "Zero Trust" approach.** Assume that insiders – such as employees and contractors – pose as much threat as external malicious actors.
- **Attacks can come from anywhere: consumers, the workforce, or IoT, and on any network.** You can't secure your network exclusively at the perimeter because there may no longer be a real perimeter.
- **The "network" is most likely hybrid, spanning on-premises, private cloud, public cloud, and multi-cloud environments.** End users are now often remote, engaging with applications over the public internet. It's important to ensure that your IAM vendor provides identity and access management control to every type of user in every environment.

[2]https://www.infosecurity-magazine.com/news/us-shipping-loses-75-million/#:~:text=US%20Shipping%20Giant%20Loses%20%247.5m%20in%20Ransomware%20Attack,-Phil%20Muncaster%20UK&text=Tennessee%2Dheadquartered%20Forward%20Air%20describes,%2Dtruckload%20(LTL)%20shipping.

[3]Making The Business Case For Identity And Access Management (forrester.com)

Attack and Data Types 2020





In 2020, unauthorized access was again the most common attack method, representing 43% of breaches (up from 40% in 2019 and 34% in 2018).

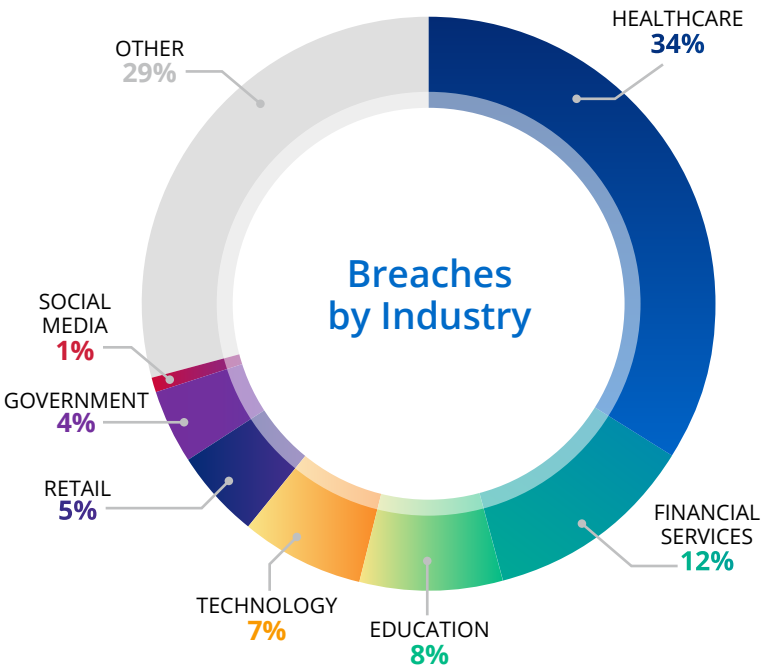
- This steady increase underscores the obligation for organizations to adopt a comprehensive IAM strategy to reduce risk and avoid costly recovery expenses. A solution that employs AI to identify anomalous and potentially risky access would further strengthen an organization's security posture.

Malicious actors employed more phishing attacks in 2020, targeting remote workers and consumers who had turned to the internet to get things done during the pandemic. In 25% of attacks, phishing was used to gain access to user credentials – up from 14% in 2019.

- In last year's report, we predicted that phishing would likely continue to be a top attack method, and this has proven to be the case. Cybercriminals preyed on consumers with false information about the COVID-19 pandemic, stimulus payments, and lockdowns. Organizations should use two-factor authentication (2FA) or multi-factor authentication (MFA) to prevent stolen or compromised credentials from being used to criminally access customer data.

Ransomware accounted for 17% of all attacks in 2020 – up from 10% in 2019. The healthcare sector was particularly vulnerable to ransomware attacks due to the pandemic. Cybercriminals exploited healthcare organizations, knowing many would rather pay a ransom than put patients at risk with a disruption of service.

Industry Breaches 2020



For the third year in a row, healthcare was the biggest target with the highest number of breaches (314), accounting for 34% of all breaches.

The second most targeted industry was financial services at 12%, followed by education at 8%, technology at 7%, and retail at 5%.

Retail had 16% of the total records compromised in 2020, up significantly from 2% in 2019. That's not surprising, given the amount of time people spent shopping online due to the pandemic. A study in August 2020 showed an estimated 129% increase in the number of consumers in the U.S. who made most or all of their household purchases online.[4] Retail data breaches are expected to continue to rise as ecommerce sites and retailer servers are attractive targets with large volumes of PII and behavioral data.[5]

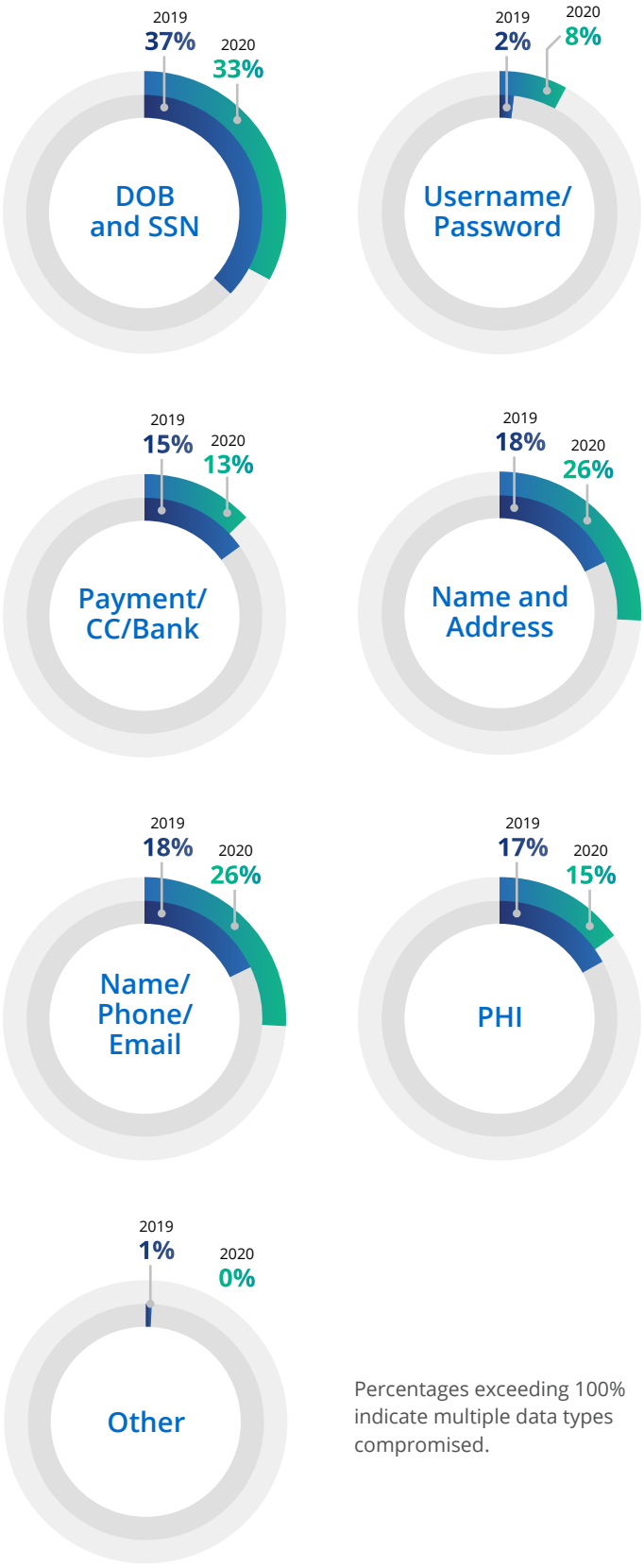
The technology sector saw the largest number of records compromised (1.6 billion) – a 15% increase over 2019. Although technology companies did not experience the largest number of breaches, they saw an 84% increase over 2019. The total cost of those breaches was $288 billion, or $183 per record.

Healthcare recorded just 1% of record thefts, but at the highest cost per record: $474. Healthcare is an attractive target because its data is extremely valuable to cybercriminals. Stolen healthcare records can be used to perpetrate medical identity theft, insurance fraud, and other crimes.

Social media accounted for 25% of records compromised. These records include a wealth of personal information. The theft of social media data can be both costly and personally embarrassing as contacts, birthdates, and even control of accounts may be hijacked.

[4]U.S. online shopping categories growth after COVID-19 2020 | Statista
[5]10,000 Breaches Later: Top Five Retail Data Breaches (idtheftcenter.org)

Types of Data Compromised



Percentages exceeding 100% indicate multiple data types compromised.

- Thefts in some high-value record categories declined as a proportion of all losses in 2020. Dates of birth (DOBs); Social Security numbers (SSNs); payment, credit card, and banking information; and personal healthcare information (PHI) all saw improvement.
- The number of breaches in 2020 involving SSNs and DOBs accounted for one-third of all breaches in the U.S. – down from 37% in 2019.
- Attacks that netted usernames and passwords were up 450% from 2019. While the percentage of breaches was relatively small, the yield was substantial: almost 1.5 billion records containing usernames/passwords were impacted in 2020.
- Also up this year were name and address thefts – 44% higher than 2019.

What does this mean for organizations trying to prevent breaches?

A cybercriminal armed with login credentials, including full name and address, SSN, and DOB can use this data to open a new account or apply for a loan. Even a few pieces of PII can lead to a ransomware attack or allow cybercriminals to gain access to a corporate network and move laterally in search of sensitive data or systems.

- A Zero Trust strategy, that is not trusting a person or device without a full understanding of identity and context, is becoming a requirement in many organizations. The organization needs to be able to verify the authenticity of users, devices, and things – not just initially, but also throughout the session, mitigating risk when an anomaly is detected.
- Zero Trust can help immeasurably in protecting data and resources by granting access only on a limited basis and in the right context. It can also prevent attackers from gaining higher privileges and access and keep them from moving laterally through a network in search of valuable data and assets to steal.

International Perspectives

U.K. Data Security in Focus

As the adoption of digital channels has grown exponentially in all sectors of the U.K. economy due to the ongoing disruption caused by the COVID-19 pandemic, so has the threat posed by cybercriminals.

According to the U.K. Department of Culture, Media, and Sport (DCMS), 96% of businesses in the U.K. now have "some form of digital exposure," offering more opportunities than ever for cybercriminals to breach digital defenses by exploiting the rapid and seismic shift to digital and remote working.

In recent years, CISOs and CEOs have been working hard to secure their networks and prioritize cybersecurity. Seventy-seven percent of businesses treat security as a priority at the board level, according to the same research by DCMS. Nonetheless, the changes wrought by the pandemic present new and complex challenges for business and security leaders alike.

Organizations in every industry are vulnerable to these threats, with severe consequences. According to IBM research, the average cost of a data breach in the U.K. is £3.17M. But the resulting reputational harm is often even greater, especially for organizations in highly regulated sectors, such as financial services and healthcare.

This year's report by ForgeRock looks at data from U.K. regulatory bodies, such as the Information Commissioner's Office (ICO), to help businesses remain well informed. The report highlights key gains made last year when the General Data Protection Regulation (GDPR) celebrated its first anniversary. In the last year, the country saw a boost in breach reporting (19% more than the previous 12-month period) and in strengthened privacy behaviors, partly as a result of regulators issuing 40% more GDPR-related fines.

Equipped with this information – and a next-generation IAM system, which can secure and unify digital identities across a wide range of IT environments fit for the modern post-pandemic enterprise – U.K. businesses will have confidence that their data is appropriately secured and feel able to take advantage of the vast opportunities the digital shift offers.

2.5X
Increase in Breaches
due to unauthorized access

471%
Increase in Ransomware Attacks
on financial services organizations

Lockdown Effect? U.K. Healthcare Sector Vulnerable, Attacks More Targeted and Frequent

According to an analysis of the ICO's data security incident reports, which break down cyber, non-cyber, and security breaches across 21 sectors throughout Q1 and Q2 2020 (the only quarters available as of April 2021), healthcare was the most vulnerable U.K., sector with the largest number of breaches: 16.2% of the time period's total. Hackers also sought to compromise the systems of healthcare organizations during the pandemic.

While this matches the top-line U.K. findings in last year's report, note that non-healthcare sectors have increased their representation as a proportion of total breaches. According to the same source, U.K. data breaches are now more evenly distributed across sectors rather than being dominated by one.

In last year's report, U.K. healthcare sector data breaches accounted for over 51.5% of total breaches in 2019. This year, education, financial services, and retail have fallen prey to many more incidents, now

comprising 13.5%, 11.7%, and 11.5%, respectively, of total data breaches in the first six months of 2020.

It is surely no coincidence that so many other sectors have seen such dramatic increases in breach incidents at the very moment when ubiquitous digitalization was spreading across almost every conceivable sector of activity. Indeed, ForgeRock's own research and others have shown that education, financial services, and retail in particular were some of the sectors most impacted by the pandemic-driven digital transformation, suggesting that cybercriminals were exploiting the early chaos caused by sudden lockdowns and a lack of cybersecurity preparedness. The data supports this. Lockdowns officially began in the U.K. near the start of Q2 2020, and we can see increased breaches both from Q1 2020 to Q2 2020 (79%) and year-over-year from Q2 2019 to Q2 2020 (36%).

This upward trend, which started in early Q2 2020, is discernible in other countries too. For example, the

Industries sectors most impacted by cybercrime as a result of the pandemic: Financial services, Retail, Education

FBI's Internet Crime Complaint Center reported in April 2020 that it had recorded a 300% spike in cybercrimes. That the issue is cross-border is partly a reflection of increasing activity from state-sponsored hackers, who perpetrated attacks on SolarWinds, Supermicro, and EasyJet in the U.K. in early 2020 – some of the largest and most sophisticated attacks in years.

Reported ransomware attacks also rose sharply across all sectors from 65 in Q1 to 152 in Q2, as did unauthorized access breaches – 87 in Q1 to 190 in Q2 – an increase of roughly 2.5 times in both cases.

The financial services sector was particularly hard hit by ransomware attacks, recording a huge increase of over 471%: from only seven reported incidents in Q1 2020 to 40 in Q2 2020. One of the most notable U.K. cybersecurity incidents in 2020 was the ransomware attack on U.K. foreign exchange firm Travelex, which was forced to shut down its network due to a rampant computer virus. In April, it emerged that the company had paid a £1.8M ransom to the hackers – a move that was criticized by some, as potentially encouraging more ransomware attacks. Given that the cost of ransomware attacks is projected to rise to £14.9B this year, this is definitely a trend worth defending against.

Finally, in 2020, phishing continued to be the most common form of data breach reported in the U.K. – even though phishing incidents declined from the previous year and other types of attacks increased. For example, NHS Digital, one of the most frequent targets of phishing attacks, reported a decline in suspected phishing emails in 2020 compared to 2019.

Conclusion

Overall, it is reasonable to conclude that the pandemic and the digital dislocation caused by lockdowns have led to worsening cyberattacks across all sectors in the U.K. The data above – and general consensus from industry professionals, media reports, and other sources – support this conclusion, with cyberattacks becoming more targeted and frequent.

Healthcare and financial services remain key sectors of concern, especially given that these two sectors often handle the most sensitive and valuable PII and are cornerstones of the U.K.'s economic and public health security. A large increase in ransomware and unauthorized access breaches in these sectors suggests that unscrupulous cybercriminals are specifically targeting these sectors for data and payments at the moment when they are at their most vulnerable.

As companies reengineer workflows and business models around remote work, the increased cybersecurity risk from the digital revolution precipitated by the pandemic may become systemic. Emergent and devastating threats like software supply chain attacks, exemplified by the SolarWinds cyberattack, which affected thousands of companies, amplify the threat. AI, a Zero Trust security posture, and a modern hybrid IAM system

system are essential for today's security-conscious and increasingly remote organizations.

This is especially true for the U.K.'s National Health Services (NHS), a frequent target of phishing and ransomware attacks. The NHS is one of the world's largest organizations, with ambitions to further embrace the cloud. For this organization, a modern IAM solution that balances privileged access requirements, healthcare productivity, and cybersecurity concerns, and works flexibly across cloud and IT environments is vitally important.

One final note – as in last year's report – the lack of comprehensive data from the U.K. regulator has hindered efforts to analyze these incidents. While the pandemic may account for some delay, this issue predates COVID-19. More granular data and a reliable timeline for publishing data sets are clearly needed.

Germany Data Security in Focus

At a time when individuals and organizations are more reliant than ever before on information systems, cyber attacks are increasing in number and sophistication. COVID-19, GDPR, and the second Payment System Direct (PSD2) all played a role in data breaches in Germany in 2020, impacting major sectors, including healthcare, financial services, government, transportation, and critical infrastructure. This report analyzes data from a variety of sources – including the 2020 report by the Federal Office for Information Security, or Bundesamt für Sicherheit in der Informationstechnik (BSI) – to paint a picture of the key findings in this turbulent year.

Malicious Attacks

Most data incidents in the country (57%) were due to malicious attacks.[6] These included behavior by a malicious individual, insider, or group launching phishing, malware, ransomware, credential compromise, and brute-force attacks. The number of malware program variants seen in Germany rose to 117.4 million in 2020, an increase of 3.4 million over 2019, with an average of 322,000 new malware variants per day. Bot infections also became common in 2020, with up to 20,000 bot infections of German systems per day.[7]

Phishing remains a major vector for cyberattacks. In Germany, phishing attacks are no longer focused only on bank customers. In 2020, these attacks also targeted customers of online retailers and payment systems. Phishing campaigns were still geared to social events and issues, such as tax refunds or Black Friday discount campaigns. However, they also played on fear and emotion surrounding the COVID-19 pandemic. These campaigns, which were well written in German so as to appear authentic, exploited the temporary closure of bank branches, as well as the applications for emergency aid and short-term financial assistance.[8]

€4.5M
Average cost of a data breach in Germany

57% Percentage of breaches caused by malicious attacks

67% Increase in security reports of critical infrastructure organizations

Previous attacks used the uncertainty surrounding the topic of GDPR. During 2020, the focus was on the implementation of the PSD2. Phishing emails asked bank customers to confirm their customer data – allegedly because of PSD2. Some of the major banks issued warnings to their customers to be alert to these types of attacks, which were aimed at obtaining personal information and access credentials.[9]

System Errors

Another 24% of data breaches in Germany were the result of system errors due to technical failures, leading to unintentional disclosure of, or access to personal information.[10]

Among the companies most affected by data leaks were well-known banks and payment service providers, technology companies, medical practices and hospitals, universities, a company in the electronic mail order business, and a massive breach discovered in January 2020 involving a car rental company.

[6]IBM: https://www.infopoint-security.de/ibm-veroeffentlicht-neue-cost-of-a-data-breach-studie-2020/a24468/
[7]BSI Report https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2
[8]Ibid
[9]Ibid
[10]IBM, op. cit.
[11]BSI, op. cit.

Another notable data breach involved the publication of large volumes of private medical data. Internationally, it is estimated that 23.4 million patient health records were freely available on the internet. In Germany alone, about 15,000 health/medical records were publicly available in the period from July 2019 to September 2019.[11]

Critical Infrastructure at Risk

An alarming trend in 2020 was the reported data incidents of critical infrastructure companies. A total of 419 reports of data breaches at critical infrastructure organizations were reported in 2020, a 67% increase over 2019.[12] Hackers actively scanned for existing vulnerabilities to exploit in the energy sector, while distributed denial-of-services (DDoS) attacks on the IT systems and online services of banks led to disruptions in payment transactions. These attacks took place over several days in Q1 2020, and initial mitigation measures were only partially effective. Increased measures at the application and network level stopped them. Other breaches were caused by internal threats to security, such as technical failures, application or configuration errors, or failures of external services.

Massive Data Leak Affects 3 Million Customers

- Personal data of three million customers of a German car rental company was freely accessible on the internet.
- Because of configuration error, no password was required for access: anyone could download 10 TB of data.
- Data available included names, addresses, dates of birth, drivers' license numbers, and often cell phone numbers and email addresses.
- More than 3,000 employee and customer passwords were visible in plain text, along with payment information and bank details.

Impacts and Costs

One in four Germans has been a victim of crime on the internet in the past.[13] The average cost of a data breach is €4.5 million, and it takes an average of 160 days for an attack to be discovered and contained.[14] A total of 283 fines, in the total amount of €48.1 million, were imposed by authorities, an increase of about 50% over 2019. In the face of increasing risk to organizations and citizens, BSI recommends using strong two-factor authentication (2FA) to increase consumer protection and comply with the Strong Customer Authentication (SCA) provisions of PSD2.

Conclusion

Many of the reported breaches in the past year have shown an increased sophistication in the attack schemes. At the same time, the dependency of companies, the state, and citizens on IT is growing, thereby increasing the potential for damage. The pandemic created a perfect storm in cybersecurity – everyone and everything is vulnerable to an attack. In this Zero Trust world, protecting the endpoint and the identity of people, devices, and things has become a central challenge.

As more private companies and government agencies take on digital transformation projects and rely on IT systems, outdated password schemes that can be easily broken must become a thing of the past. Additionally, the idea that each application needs to do its own form of authentication needs to be abandoned in favor of a single source of truth for identity. Once that is in place, MFA and authentication trees can be built around this single source of truth. It needs to be clear to all stakeholders that identity and authentication is not a one-time shot but an ongoing process to sustainably increase cybersecurity across all industries.

[12]BSI, op. cit.
[13]BSI, op. cit.
[14]https://de.statista.com/infografik/19071/finanzieller-schaden-fuer-unternehmen-durch-datenlecks/

Australia Data Security in Focus

According to the Office of the Australian Information Commissioner (OAIC) as part of its notifiable data breaches (NDB) scheme, the total number of disclosed breaches in 2020 was 1,057[15] – up from 997 in 2019.[16] This is an increase of 6% year-over-year. With 812 data breaches reported in 2018, the period from 2018 to 2020 has seen the number of data breaches reported to the Office of the OAIC rise by over 30%.[17]

Like 2019, 2020 saw health service providers, finance (including superannuation), and education as the top three industry sectors most affected by data breaches.

Health service providers (the health sector) reported 238 data breaches in 2020. This sector has consistently reported the most data breaches compared to other industry sectors since the start of the Notifiable Data Breaches (NDB) scheme, with a full 40% of the attacks due to malicious or criminal activity from January to June 2020. The healthcare industry saw increased consumer activity throughout the pandemic, largely due to factors like increased e-health consultations, leading to more potential attack vectors for breaches to occur as well.

The finance sector (including superannuation) reported the second highest number of data breaches, with 155 reported in 2020. Malicious or criminal attacks were responsible for 59% of the breaches in the finance sector between January and June 2020. With some Australians opting to access their superannuation during the pandemic, this may have also created more potential attack vectors for breaches to occur.

The Australian government also emerged as one of the top industry sectors affected by data breaches in 2020. These findings show that data breaches against a number of large organizations and government bodies are becoming more commonplace, and the sectors involved in these attacks are also expanding.

Contact information like home addresses, phone numbers, and email addresses remained the most frequently sought-after information involved in data breaches in 2020, with 926 data breaches including

30%

Increase in data breaches
from 2018 to 2020

49.8%

Identity information breached
Year-over-year increase

61 to 365+ days

Time to discover a breach
for 11% of reporting organizations

[15]https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2020/ and https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020/

[16]https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-quarterly-statistics-report-1-january-31-march-2019/, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-april-to-30-june-2019/ and https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2019/

[17]https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-january-to-31-march-2018/, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-april-to-30-june-2018/, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-july-to-30-september-2018/ and https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-october-to-31-december-2018/

contact information (an increase of 13.3% from a year ago). Data breaches involving identity information saw the biggest increase in 2020, with a 49.8% increase year-over-year. Data breaches involving Tax File Numbers also saw an increase of 17% year-over-year.

Ransomware attacks increased 150% from January to June 2020 and expanded from simply encrypting data to copying and exfiltrating sensitive information. Additionally, from July to December 2020, the most common method used by malicious actors to obtain compromised credentials was email-based phishing (54 reported incidents), highlighting how email-based vulnerability remains something that Australian organizations must consider as they work toward boosting their security posture.

In Australia, the length of time it can take for an organization to detect and report a breach varies. Across the reporting period from January to June 2020, approximately 77% of notifying entities were able to identify a breach within 30 days of it occurring. In 47 cases during the same period, it took between 61 and 365 days to become aware of a breach, and in 14 organizations it took more than a year. From July to December 2020, 78% of entities notified the OAIC within 30 days of becoming aware of a breach. However, 23 entities took longer than 120 days after they became aware of an incident to notify the OAIC.

Conclusion

While system faults remained the smallest cause of data breaches in 2020, they rose slightly between 2019 and 2020, highlighting the importance of Australian businesses spending time to properly invest in technology and IT portfolios for both customers and employees to ensure they are secure at all levels of operation. Alongside this, as the OAIC found some organizations can take more than 30 days to discover a data breach has occured, this investment must also be focused on ensuring that stronger systems are in place to catch them sooner.

With human error also the cause of 380 data breaches in 2020, the development of more consolidated digital identity management platforms will only go so far for workforces and services accessed by the public daily. More needs to be done to educate Australians on how to best manage their digital identities. This includes: strengthening their passwords; incorporating additional measures like MFA; employing emerging methods of passwordless authentication; avoiding the use of too many different devices to access sensitive banking or health information; and being more vigilant to spot potential malicious attacks carried out via email or text message.

Singapore Data Security in Focus

For the first time, the "ForgeRock Consumer Breach Report" has expanded this year to include information on data breaches in Singapore. This important country is ranked by the World Bank as one of the world's most competitive economies.[18] Less than three years ago, Singapore was named the safest country in the world by the World Justice Project, a designation that relates to physical security, crime, and civil conflict. Yet for the past several years, corporations and individuals have not been immune to the menace of data breaches. Phishing scams, ransomware attacks, misconfigured servers that allow unintended access, and passwords reused for multiple accounts have resulted in a huge increase in unwanted access to sensitive information. According to the most recent report, released in July 2020 by the Cyber Security Agency (CSA) of Singapore, an agency in the Ministry of Communications and Information, there was a 30% increase in 2019 in the number of cases of e-commerce scams over 2018.[19]

Twenty-eight percent of Singapore residents reported they had suffered at least one cybersecurity lapse in the previous 12 months.[20]

The trend continued in 2020. In the banking world alone, phishing scams saw a 20-fold increase in the first half of 2020[21] as cybercriminals raced to exploit the confusion and panic of the pandemic to trick victims into disclosing their banking credentials, personal identification numbers (PINs), and the like. Singapore is at the forefront of virtual banking, with the Monetary Authority of Singapore issuing virtual bank licenses to non-banks in order to serve under-served segments of the domestic market. In order to obtain a license, the virtual (digital) bank needs to ensure strict security measures are in place.[22] Ransomware saw similar trends: Compliance, Safety, and Accountability (CSA) reported a 75% increase in the number of incidents in the first 10 months of 2020 compared to all of 2019.[23] Most of the organizations targeted were small and medium enterprises, from a variety of sectors including healthcare, retail, and manufacturing.

Why Is the Risk so High?

According to CSA, Singapore is one of the most connected countries in the world and has a very high internet adoption rate, making it a target for cyberattacks. Cybercriminals play on citizens' trust in government, running phishing campaigns that impersonate government organizations. Such impersonation can provoke fear and urgency in the email recipient, causing them to disregard normal security practices and click through to allow malware to be implanted on their systems or hackers to gain access to their credentials.

The pandemic and the move to remote working has made telecommuting applications very popular, yet some of these apps contain vulnerabilities that can be exploited. During 2020, people spent a lot more time on the internet than ever before, doing the majority of their shopping, business, and personal transactions online rather than in person. Retail sites thus became a big target for hackers who sought to obtain access to a wealth of customer data. In Singapore, the personal details related to 9.5 million customers were made available for unauthorized access.[24]

The biggest breaches in Singapore, however, are due to lapses in cybersecurity practices and technology and have led to the disclosure of thousands and, on occasion, millions of records. A misconfiguration at an

[18]Singapore Overview (worldbank.org)
[19]https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2019
[20]More than a quarter of Singapore residents suffered at least 1 cybersecurity lapse in past year: CSA survey - CNA (channelnewsasia.com)
[21]https://www.straitstimes.com/singapore/courts-crime/banking-related-phishing-scams-move-to-messaging-apps-and-social-media-see-20
[22]Digital banks in Singapore - Discover the brand new banks | Finder SG
[23]https://www.csa.gov.sg/singcert/publications/global-local-ransomware-trends-2020-q1-q3#:~:text=SINGAPORE%20RANSOMWARE%20TRENDS,in%20cases%20reported%20to%20CSA.
[24]Data from research conducted on breaches in Singapore - Lazada, Love, Bonito, Eatigo, Foodoro Lazda And Eatigo Suffer Data Breach; Millions Of Account Details Sold Online | Information Security Buzz
[25]https://vulcanpost.com/715666/data-breaches-cybersecurity-singapore/

electronics and gaming hardware vendor in Singapore led to the disclosure of approximately 100,000 records, while unauthorized access at an online shopping service resulted in five million records being subject to unauthorised access.[25] The cost of a breach can be massive – the cost of discovering and mitigating the breach, damage to the brand, subsequent lost business, and fines levied by regulatory bodies can all be significant.

Singapore Government Tightens Regulations

The Personal Data Protection Act (PDPA) was passed in 2012, providing some level of protection for citizens. While the PDPA encourages organizations to make voluntary notification of a breach, until recently there was no mandatory breach notification required. All that is changing. An amendment introduced in Parliament beefs up the cap on financial penalties. In 2019, the Personal Data Protection Commission levied fines of S$1.29 million,[26] a figure that may rise significantly once the new caps are in effect. More importantly, the amendment requires mandatory data breach notification if the breach is likely to result in significant harm to the individuals impacted or is of significant scale (example: involving 500 or more individuals).[27] The amendment was passed on November 2, 2020 and takes effect in phases starting on February 1, 2021.[28]

Best Practices for Avoiding Breaches

Consumers trust companies to manage and protect their private information, and companies must implement strong cybersecurity practices to earn that trust. As digital transformation opens new entry points such as cloud, social, and mobile, the risks increase correspondingly. To address increased risk, organizations need to make use of AI and machine learning (ML) technologies to spot abnormal behavior and institute a Zero Trust policy that ensures accurate identity and access management (IAM). A modern hybrid IAM system should be implemented to ensure that adequate protections exist both in on-premises environments and in the cloud.

Conclusion

Singapore is one of the most connected countries in the world and has a very high internet adoption rate. With more people now working from home regularly and putting more of their information online for services like online banking and retail, the chances of these attacks will only continue to increase.

As a result, the Singaporean government's move to make data breach reporting mandatory in 2021 is coming at a crucial time and will be pivotal to ensuring businesses can identify weak points in their online experiences that may lead to cyberattacks for both employees and customers.

[26]https://vulcanpost.com/676006/pdpc-data-breach-singapore-2019/
[27]https://www.cms-lawnow.com/ealerts/2020/10/singapore-set-to-introduce-mandatory-breach-notification-under-data-protection-laws
[28]https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

Conclusion

More time online. Working remotely. Strained budgets. Supply chain security failures. Aging infrastructure. Unsecured databases. All of these – compounded by the burden of meeting GDPR, CCPA, Open Banking, and PSD2 mandates – exposed widespread systemic security vulnerabilities and made it increasingly difficult to protect sensitive information throughout 2020.

Cybercriminals made the most of the pandemic-induced confusion and chaos, exploiting these vulnerabilities around the globe. They increased their focus on valuable and easily accessible usernames, passwords, and personal health information. While there were not as many breaches in 2020 as in years past, they were highly targeted at specific industries, such as healthcare and education, where attacks had a high likelihood of yielding extremely valuable information including credentials. Breaches that revealed usernames and passwords rose by 450%, giving attackers a massive number of credentials to use in gaining further unauthorized access.

The trend of breaches targeting consumer PII continued unabated from years past. Many countries saw huge increases in the number of breaches involving identity information but this was most pronounced in the U.S., with a massive 450% increase over 2019 in breaches involving usernames and passwords. Criminals combined information from multiple databases and social media sites with stolen credentials to attempt access to healthcare, banking, retail information, and more. When consumers use the same credentials on multiple sites and applications and freely populate their social media accounts with personal information, they make the cybercriminals' job easier.

Unauthorized access continued to be the most common type of breach. Whether caused by malicious insiders, cybercriminals actively exploiting vulnerabilities, or inadvertent behavior on the part of employees or consumers, problems caused by poor access management were widespread in the U.S., U.K., Germany, Australia, and Singapore.

Phishing continued to rise as a favored attack method, representing 25% of all attacks in the U.S., up sharply from 14% in 2019. It was the most common data breach type in the U.K., as well as in Germany where attacks hit users of online retailers and payment systems. Phishing was the most common method used in Australia (36%) in the second half of 2020, while Singapore saw a 75% increase.

Phishing continued to rise as a favored attack method, representing 25% of all attacks in the U.S., up sharply from 14% in 2019. It was the most common data breach type in the U.K., as well as in Germany where attacks hit users of online retailers and payment systems. Phishing was the most common method used in Australia (36%) in the second half of 2020, while Singapore saw a 75% increase.

The U.K. saw a whopping 471% increase in ransomware attacks, followed by 150% in Australia, 75% in Singapore, and the U.S. not far behind with a 70% increase.

Healthcare was again among the most vulnerable and targeted sectors around the world, accounting for 34% of the breaches in the U.S., and among the top three targeted sectors in the UK, Germany, and Australia. The implications are frightening: a medical record follows an individual throughout their lifetime, holding

the key to vast amounts of personal information. Once compromised, it can be used to access insurance information, file claims, obtain prescriptions, and much more. The industry faces a number of challenges: a historical weakness in access control and authentication, tight budgets, with the simultaneous need to quickly scale online capabilities while ensuring a comfortable user experience.

Third parties and service providers played a major role in data breaches in 2020. The SolarWinds hack exposed the reality that an organization's responsibility for protecting information does not stop at its own boundaries, but instead extends to all the customers of all the enterprises it supports.

The cost of a breach remains significant. Since last year's report, the average breach cost in the U.S. increased to $8.64 million, maintaining that country's standing as the costliest place in the world to recover from a breach. The global average, in contrast, went down 1.5% to $3.86 million; yet for organizations with a remote workforce, the average cost increased by more than 2%, bringing the global average to $4 million.

These findings serve to highlight the fact that organizations need to not just maintain but improve their security posture if they are to protect consumer data, prevent damage to their brands, and avoid the direct and indirect costs of a breach.

What are the most important takeaways from this year's consumer breach report?

Understand that attacks can come from anywhere: consumers, the workforce, or "things." The right IAM solution needs to address all three, not just one or two. The modern hybrid IAM solution should be able to scale to meet ever-increasing needs, operating seamlessly across on-premises and cloud-based environments. It should allow the organization to orchestrate user identity journeys in a way that balances security and great user experiences. It should incorporate the strategy of Zero Trust, extending context from authentication into authorization to cover the entire session. This helps to mitigate risk and protect data by extending access only when and where it is needed.

Identity governance is a key factor in reducing risk and avoiding breaches. The ideal solution will make use of an organization's vast stores of data to predict good access. A solution that uses ML models and AI can detect unexpected behavior, working in conjunction with other IAM investments to reduce effort while delivering smart access recommendations.

In a nutshell – if you think you are a smaller target and therefore not so vulnerable, think again. No organization is immune from cyberattacks. Everything you can do to improve your security posture, such as passwordless techniques and other Zero Trust-friendly measures, helps keep you from being a statistic.

Eve Maler

Chief Technology Officer

Eve 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 leading standards such as SAML and User-Managed Access and publishing research in the field, and has also served as a Forrester Research security and risk analyst. As CTO, she is responsible for the Labs team investigating and prototyping innovative approaches to solving customers' identity challenges, along with driving ForgeRock's industry standards leadership. She hopes her duties still leave time to contribute to the rock 'n' roll outfit ZZ Auth and the Love Tokens.