MONTANA CYBERSECURITY REPORT

EXPOSING THE 2022 BREACHES

A COMPREHENSIVE ANALYSIS OF CYBER THREATS IN MONTANA

SALES@PINECC.COM | WWW.PINECC.COM | +1800 - 432 - 0346

INDEX

How Will You Respond?

By Brandon Vancleeve, President, Pine Cove Consulting

IT professionals face unique challenges and immense pressure in theirroles. This pressure originates from both internal and external sources.Internally, executives and end-users often hold high expectations fortheir technology and can become frustrated when it doesn't function asexpected.

Externally, media attention on IT tends to focus on major data breachesand critical issues, while vendors use fear-inducing content to promotetheir products. Additionally, IT professionals must constantly stayvigilant about network security to protect against potential threats frommalicious actors.
Despite these external pressures, IT professionals have an opportunity torespond with either timidity or courage. Striking a balance betweenstaying informed and focused while filtering out unproductive externalnoise is crucial.

At Pine Cove Consulting, our mission is to alleviate some of this pressureby providing valuable content and personalized products and services tosupport your IT needs.
The Montana Cybersecurity Report presents factual information aboutdata breaches in Montana, accompanied by insightful commentary on theyear's observations and future expectations. We are confident that thisreport will offer valuable insights into the current threat landscape.

As we enter 2023 and 2024, I invite you to respond to these pressures bymaintaining a diligent and unwavering pursuit of security. By stayinginformed and proactive, we can effectively navigate the challenges thatlie ahead. Together, let's tackle these obstacles with courage and determination.

Montana Code Annotated

Montana law (see below) dictates that companies report breaches of data to the Montana Department of Justice. It's important to highlight that any company legally authorized to conduct business in Montana, even if they lack a physical presence within the state, is required to report breaches that affected a Montana Citizen.

"Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3), or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. (MCA 30-14-1704(8))"

The Montana Department of Justice shares this information publicly on its website for transparency reasons. We at Pine Cove Consulting have taken the time to analyze this data and present it in a way that may help you better understand the threats and what you can do to protect yourself.

The Data

At Pine Cove Consulting,

our foremost commitment is to deliver the highest level of accuracy in our data analysis. Below, we briefly outline our process.

In the dataset provided by the DOJ,

duplicates pose a common challenge that necessitates elimination. However, we do not remove the data for companies that experience multiple data breaches in the same year,

Every year,

Pine Cove Consulting undertakes the task of reanalyzing data from preceding years to ensure the ongoing integrity of the data. There are instances where companies have chosen not to disclose a breach owing to ongoing investigations concerning the incident. Once the investigation concludes, the companies will report the breach, and often, there will be a noticeable spike in the number of reported breaches for those specific preceding years.

When reviewing older reports,

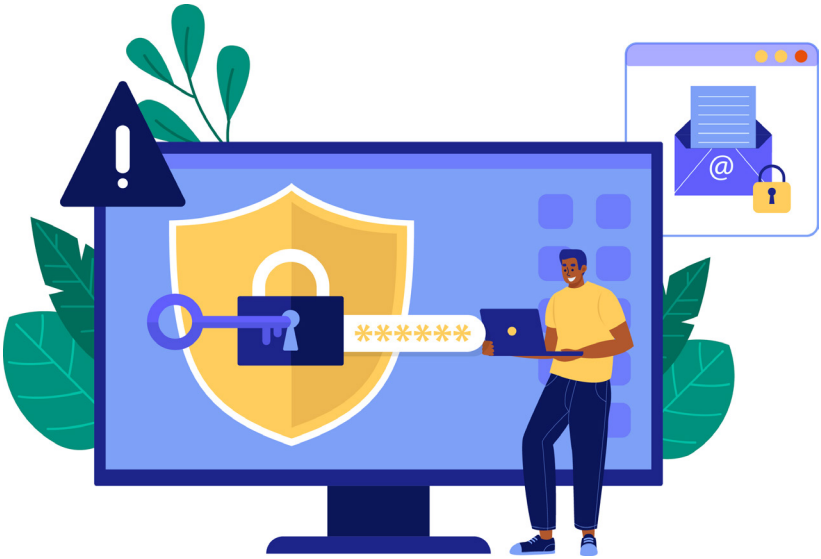
it is important to note that there might be disparities in the recorded figures. The optimal approach to access the most up-to-date and accurate information is by referring to the latest available report.

While examining the dataset,

we frequently encounter information gaps from the DOJ or breach letters. To ensure data integrity, we either accommodate these gaps without adding the missing data or categorize them under "other."

Our dedicated efforts span weeks of meticulous data examination,

culminating in creating an accurate report that remains unparalleled in its scope for the citizens of Montana.

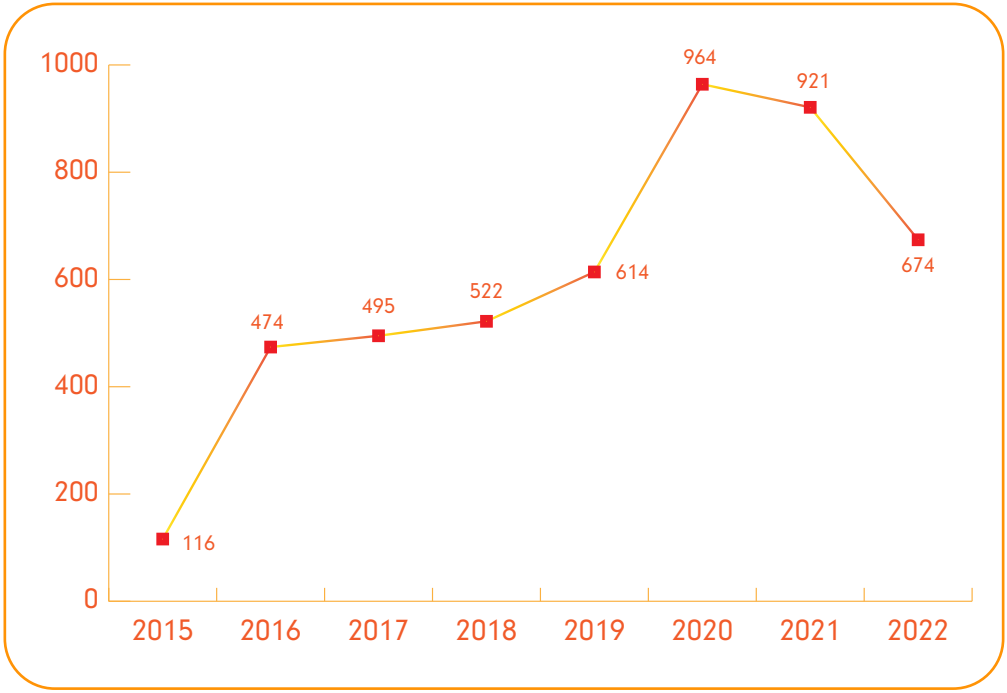


BREACHES

Number of Breaches

In 2015, Montana initiated the requirement for companies to report data breaches. This led to a relatively low number of reported incidents for that first year because companies were unaware of the new law. However, comparing 2016 (the first full year of mandated breach reporting) to 2022, a notable surge of 42.2% more breaches occurred. This substantial increase underscores the escalating concern and heightened awareness surrounding data breaches within the state.

In 2022, 674 breaches were documented for the year. This is 247 fewer breaches than in 2021 and 290 fewer breaches than in 2020.



Number of Breaches:

Exploring the Decline in 2022

This trend persisted into 2021, with 921 total recorded breaches. However, in 2022, a decrease occurred. But what led to this change? What were the primary factors driving the spikes in 2021 and 2022?

The 2021 American Community Survey highlighted a significant tripling in remote employees in the United States between 2020 and 2021 following the March 2020 shutdown. Montana was not an exception, experiencing an increase in breaches. McAfee's study revealed that 81% of global organizations faced a surge in cyber threats during the COVID-19 pandemic.

Yet, what vulnerabilities does remote work introduce?

Firstly, many employees resorted to personal devices while awaiting business-issued endpoints or for easier access to work accounts, such as email. Amid the pandemic, Trend Micro Incorporated's report indicated a tenfold increase (39%) in personal device usage for accessing company data. Although this was not a new phenomenon, Syntonic's research revealed that 87% of companies depended on personal mobile devices to access corporate applications. However, the pandemic amplified this necessity.

The use of personal devices can compromise security posture. A Sophos report disclosed that about 3% of Android devices come preinstalled with malware.

Moreover, when users neglect updates for their phones and applications, vulnerabilities remain unpatched. These updates are crucial for addressing weaknesses in the phone or application programming.

Additionally, the abundance of unsafe applications available for download contributes to the issue.

Furthermore, many people do not have a VPN (Virtual Private Network), essential for creating a secure and encrypted connection between your device and a remote server. Another issue is the absence of content blockers on personal devices, leaving users susceptible to clicking on malicious links or visiting unsecured websites.

Personal devices can connect to various networks—homes, cafes, libraries, malls— without guaranteeing network security. A study by the Ponemon Institute, in collaboration with Keeper Security, found that 67% of respondents saw a negative impact on their organization's security due to remote workers using personal mobile devices.

Number of Breaches:

Exploring the Decline in 2022

However, the rise in cyber threats during the pandemic cannot be solely attributed to personal devices. The shift to remote work also involved utilizing existing home internet systems. In terms of security, home routers and corporate networks differ significantly. Home routers have basic firewalls with limited customization, while corporate networks use advanced, customizable firewalls capable of blocking specific applications and sites. Likewise, home routers often lack or have limited Intrusion Detection/Prevention Systems (IDS/IPS), while corporate networks employ sophisticated systems for real-time threat detection. Network segmentation is another contrast, as home networks usually lack proper segmentation, making lateral attacks easier. In contrast, corporate networks isolate segments, reducing breach impact. Encryption varies, too: home routers offer basic Wi-Fi encryption, while corporate networks use robust encryption methods for wired and wireless connections and may deploy VPNs for added security.

Moving on, 2022 witnessed a notable reduction of 247 data breach incidents compared to 2021. This decrease marked a significant milestone, representing the first instance of declining breach incidents since the implementation of data breach reporting mandates by the MT DOJ. Nonetheless, 2022 remained significantly higher than all previous years, excluding 2020 and 2021, indicating an ongoing upward trend in breaches.

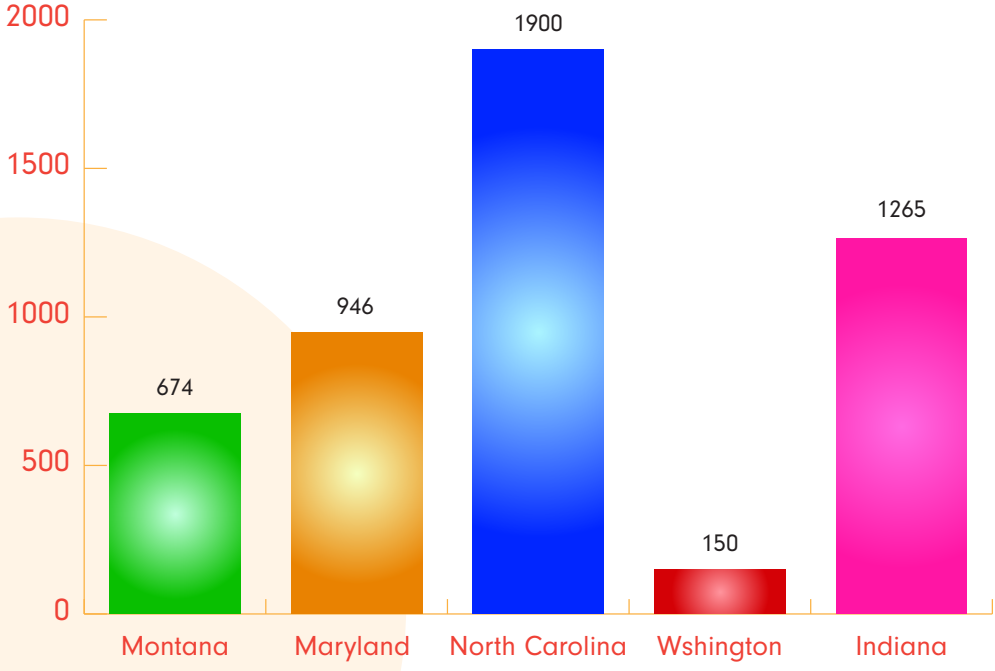
Multiple factors converged to explain the decline in breach occurrences. Companies enforced stricter regulations for employee access to work accounts and data, reinforcing security measures. More significant investments were directed towards endpoint security for employees' computers, enhancing protection for critical systems. The heightened awareness of cyber threats also played a pivotal role.

Additionally, the gradual return of employees to physical office spaces added another layer of security, minimizing vulnerabilities inherent to remote work setups. These collective efforts undoubtedly played a pivotal role in the positive shift observed in data breach statistics for 2022.

Number of Breaches:

MT Compared to Other States

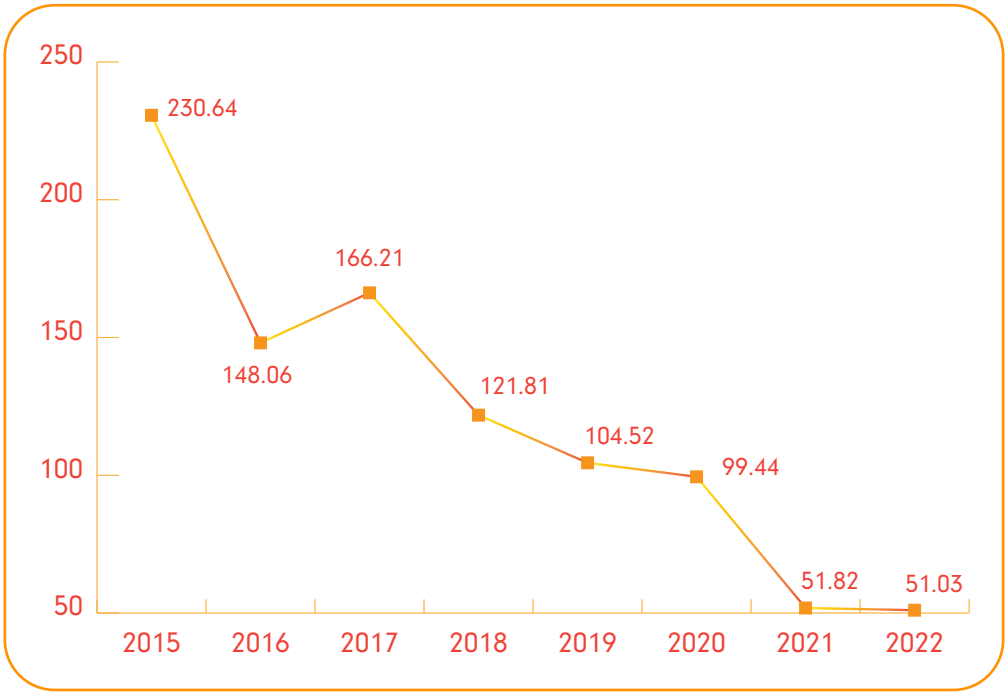
When comparing the number of breaches in Montana with those in other states, no correlation was observed between the number of breaches and the extent of residents affected. For example, Washington experienced 524 fewer breaches than Montana; however, the attorney general's report for the state of Washington indicated that the number of affected individuals was 4,537,000. The quantity of breaches is essential, but it is equally important to analyze the scale of those breaches. The following states were selected based on their practice of publishing reports rather than any specific criteria. Notably, Montana is among the 18 states that make their data breach lists available to the public.ft observed in data breach statistics for 2022.



Average Length of Breaches

The average breach duration is calculated based on the time span between a breach's start and end dates, and this average is determined by averaging the lengths of all breaches within a specific year.

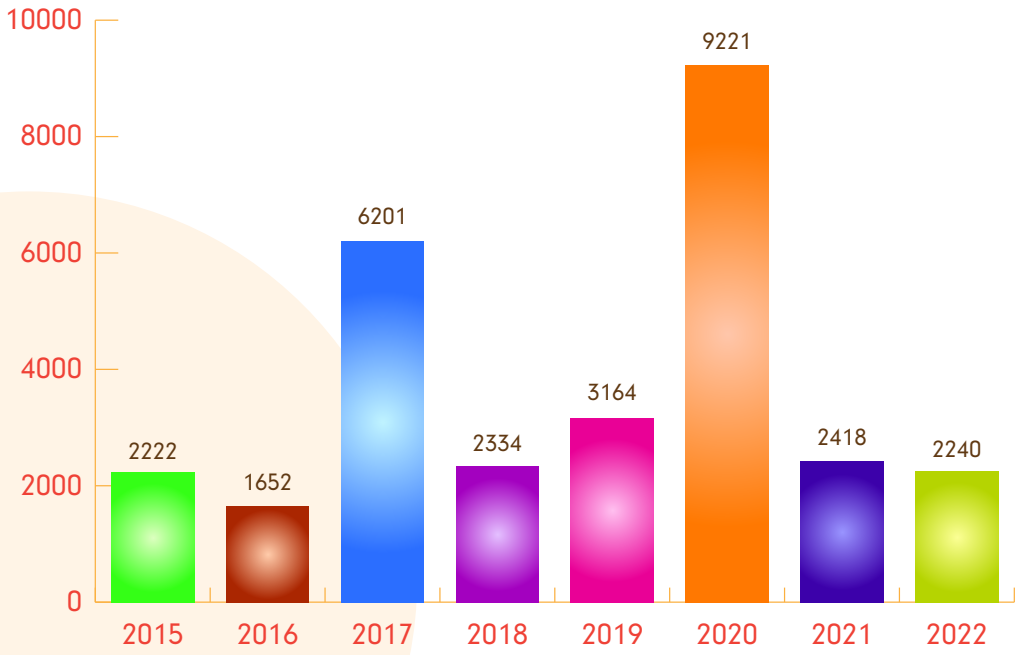
Throughout both 2022 and 2021, this average duration remained stable at approximately 51 days. Notably, there has been a consistent decline in breach duration since 2015, indicating that companies have improved their ability to detect and halt breaches, preventing further unauthorized data access and impact.



Lengthiest Breach

The lengthiest breach on record persisted for an astonishing 9,222 days, equating to a cyber-attack spanning 25 years. This occurrence came to light in 2020, surpassing the previous record set in 2017, which endured for 6,202 days, or nearly 17 years.

When examining the longest breaches for each year, these calculations encompass breaches that were either initiated or concluded within the respective year. The data reveals a discernible pattern of peaks and valleys, signifying a lack of steady progression. This pattern suggests that, overall, there has been no significant improvement in the duration of the longest breaches. Notably, the lengthiest breaches remain undetected for an average period of about 1,968 days, equivalent to roughly 5.39 years.



Lengthiest Breach in 2022

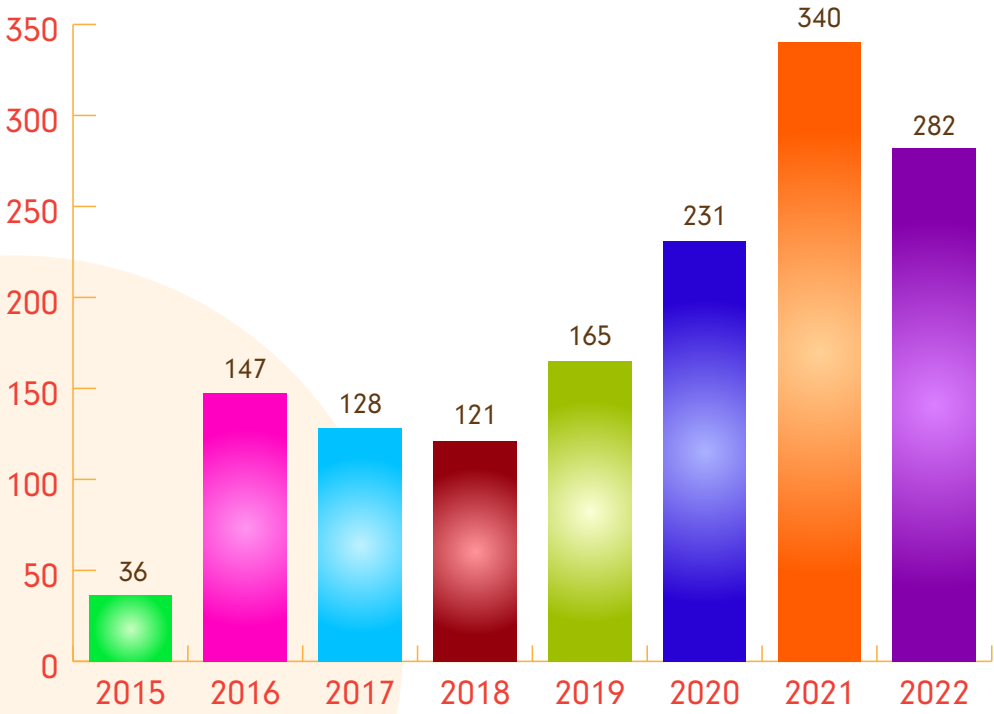
In 2022, the longest breach persisted for 2,240 days. The company was Mscript, a provider of mobile and web-based prescription management solutions for pharmacies. This breach, stemming from 2016, was linked to cloud storage segments lacking proper access controls, facilitating unrestricted entry. Unfortunately, authentication requirements for accessing data through their web and mobile applications were absent. Such incidents can transpire even among secure companies. Thus, a well-structured disaster recovery plan becomes equally crucial for swift mitigation and resolution.

Breaches Resolved the Same Day

In 2022, 282 breaches were successfully resolved on the same day they commenced, constituting 41.8% of the year's overall breach count. This reflects a 4.9% rise compared to the preceding year's proportion of breaches resolved the same day.

The rapid identification and subsequent resolution of breaches hold immense importance in mitigating the potential harm inflicted upon organizations.

When companies identify and halt breaches swiftly, they can substantially diminish the costs associated with mitigation. A more detailed exploration of this topic will be undertaken later in the report.

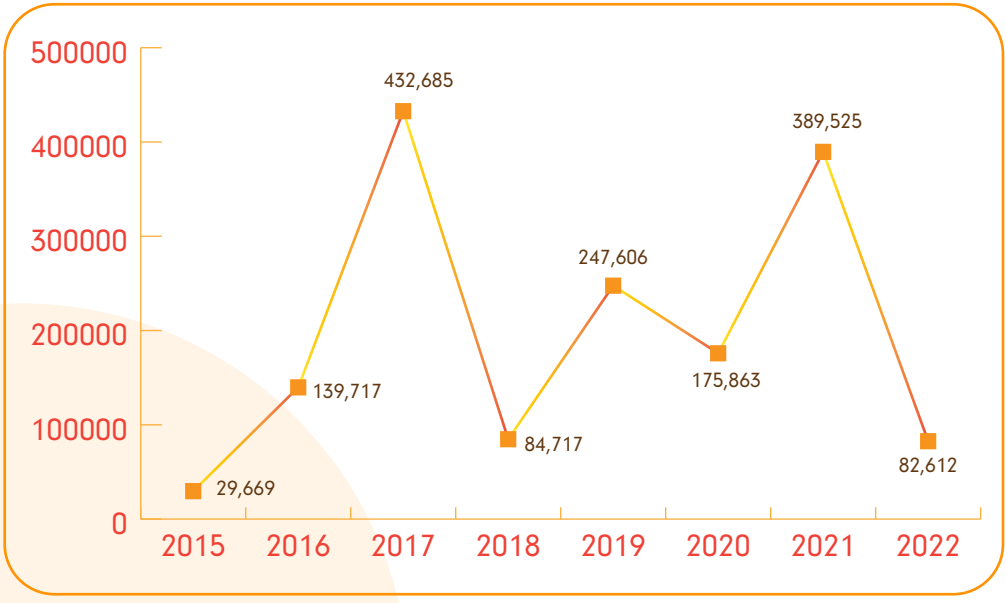


MONTANANS Affected

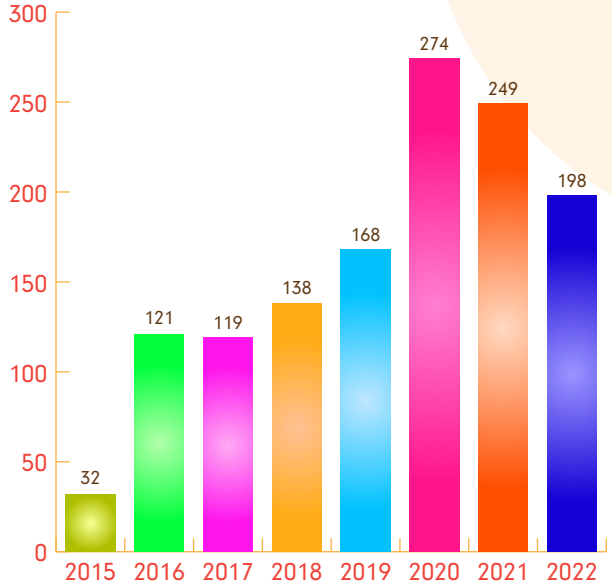
Impact of Breaches on Montana's Population

Every business obligated to report a breach to the Montana Department of Justice (DOJ) must provide the count of affected Montanans. Nonetheless, a few breaches lacked precise data on the number of impacted Montanans and are not part of this dataset. Therefore, the actual count of affected Montanans might surpass the reported figures. In 2022, data breaches affected 82,612 Montanans, signifying a

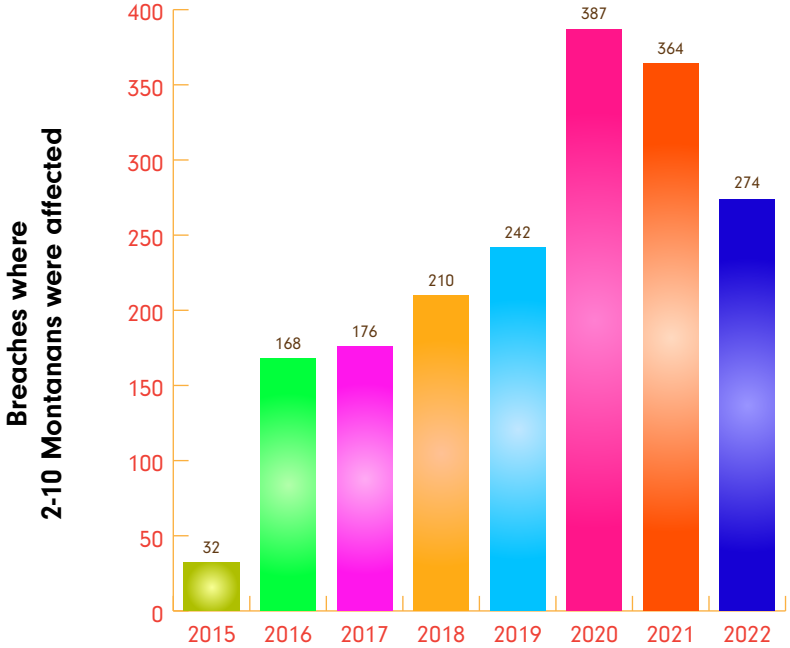
In 2022, data breaches affected 82,612 Montanans, signifying a substantial 78.8% reduction from 2021 and a 53% decrease from 2020.



Breaches that Impacted less than 100 Montanans



Breaches where only 1 Montanan was affected

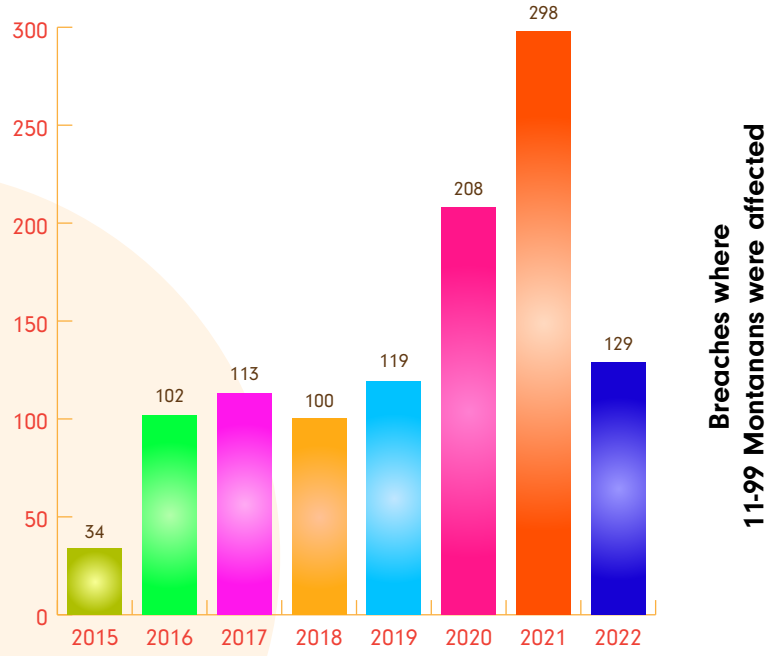


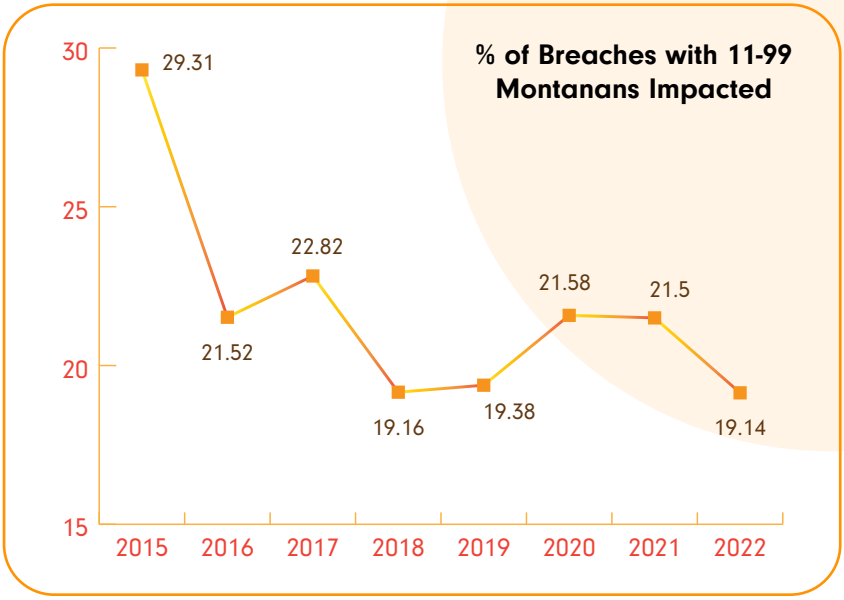
Breaches where 2-10 Montanans were affected

Breaches that Impacted less than 100 Montanans

IIn 2022, the 674 breaches impacted a total of 82,612 Montanan. Each breach affected a distinct number of Montanans. During 2022, we witnessed a rise in breaches that impacted ten or fewer Montanans. This trend might indicate that breaches are being swiftly addressed or that companies are concentrating their security efforts on preventing major attacks.

Asaf Kochan, the author, shared insights on smaller breaches, stating, "An effective data security regime prevents and mitigates the most likely attack vectors and outcomes, and for the vast majority of corporations, the odds of a devastating, multi-million-dollar attack are minimal. On the other hand, the odds of a smaller breach taking place are almost guaranteed. For every attack we hear about in the media, there are

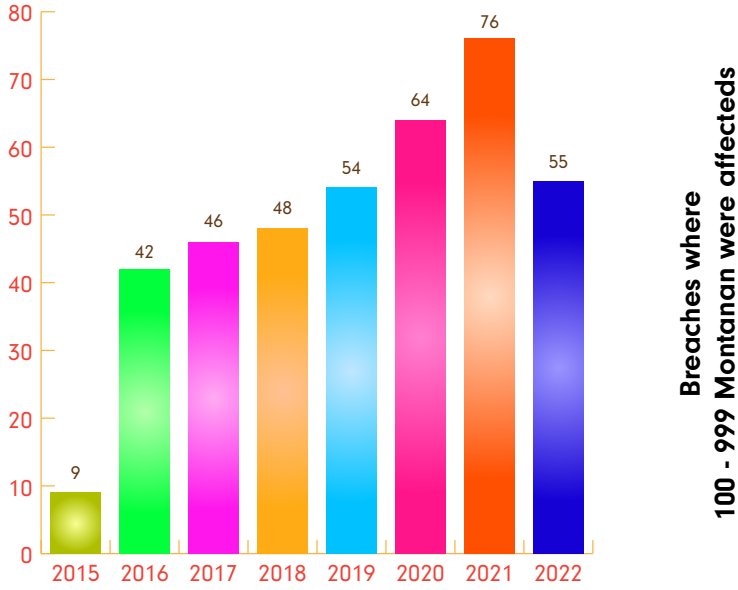


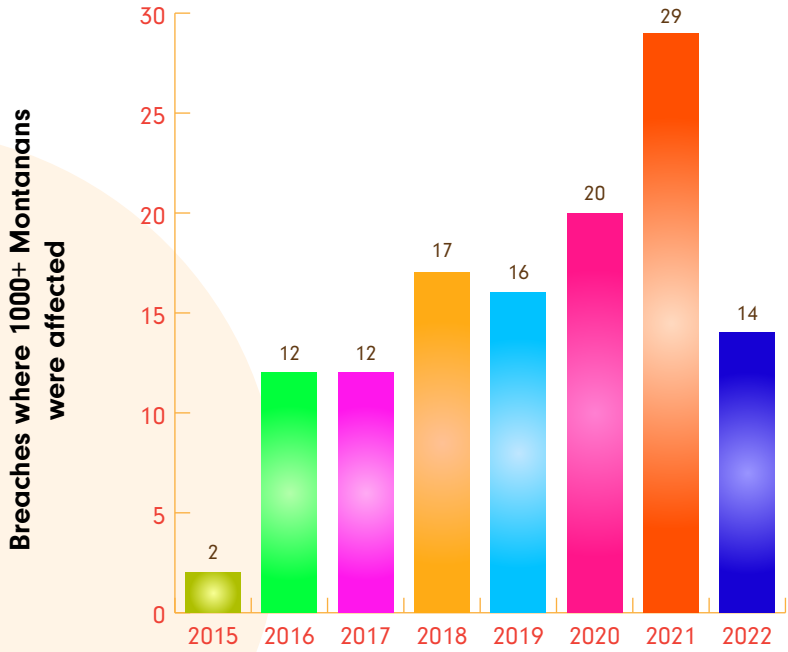


many more that never come to light. No company is eager to admit they were breached, even though small-scale breaches will affect every organization regardless of the strength of their security posture."

According to the Verizon Data Report, small-scale instances of data loss involving fewer than 100 files still incur costs ranging from $18,000 to $35,000. This cost estimation does not account for the potential long-term impacts on the business reputation, potentially resulting in the business facing closure.

Number of Montanans Affected

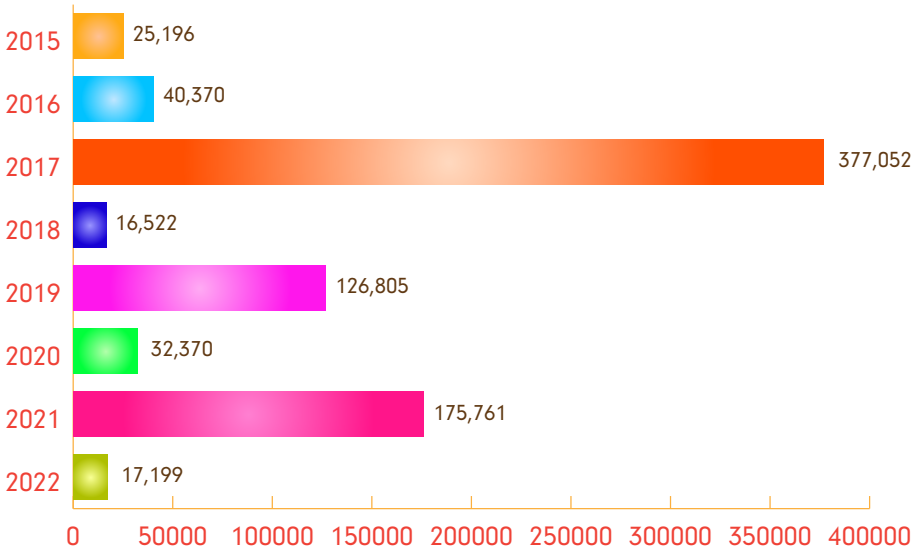




Breaches that Impacted Over 100 Montanans

When analyzing data breaches that impacted 100 to 999 Montana residents and those affecting 1000 or more, a decline was evident in 2022. Specifically, for breaches involving 100 to 999 residents, there was a 0.09% reduction compared to 2021 but an increase of 1.52% compared to 2020. In contrast, a discernible pattern for breaches exceeding 1,000 residents is not apparent.

However, 14 breaches individually affected over a thousand Montana citizens a piece.

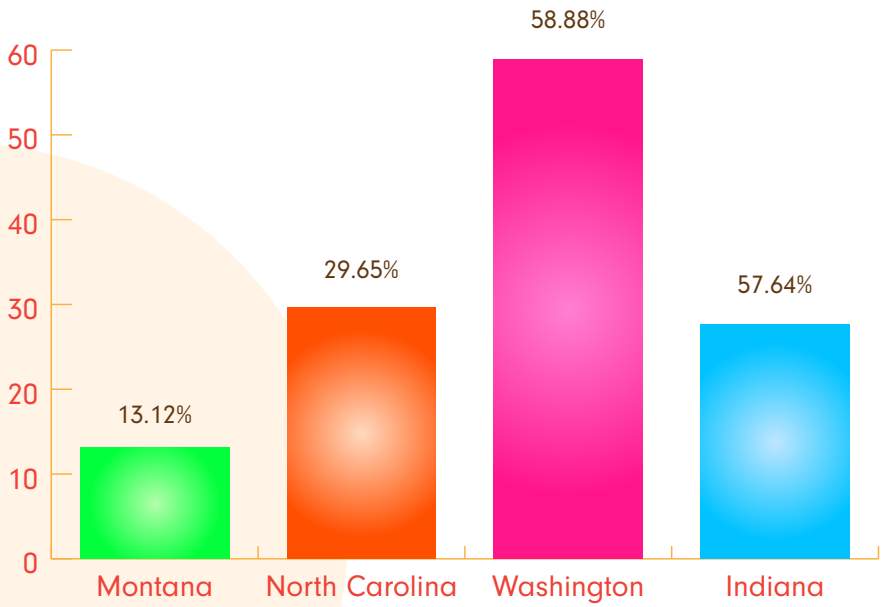


In 2022, the most extensive breach impacted 17,199 Montanans. In 2019, 2020, and 2021, the most significant breach affected hundreds of thousands of Montanans. But still, that means over 1% of the population was affected by a single breach in 2022.

Breach Impact Probability

When gauging the probability of a resident being impacted by a breach, Montana showcases a comparably lower percentage when contrasted with other states in 2022. In 2022, there was a 13.12% chance a Montanan would be affected by a data breach. This disparity can be ascribed to several factors. By considering data from the state governments of North Carolina (NC) and Montana (MT), North Carolina boasts 837,781 more small businesses than Montana. This divergence in the business count could contribute to the observed disparity in breach likelihood between these two states.

Additionally, Montana's lower population density, potential cybersecurity awareness, and regional economic factors might contribute to its reduced breach risk. However, further research is needed to confirm these potential explanations.



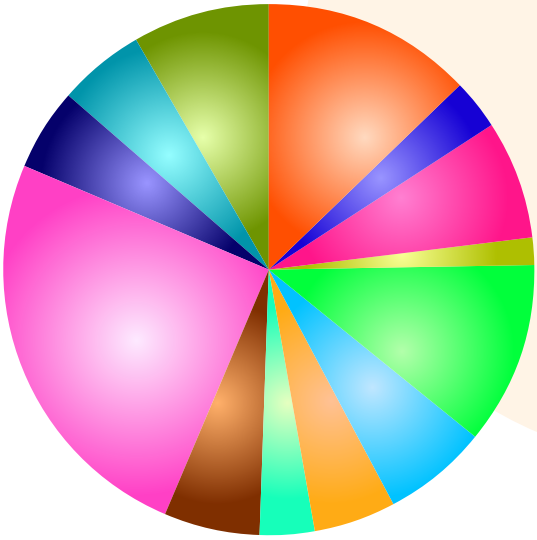
Industry Trends

Industries Affected

In 2022, data breaches made the finance sector the most impacted industry. This encompasses banks, accounting services, investment firms, loan companies, and other financial institutions. However, the 2023 Verizon data breach report identified finance as the second largest industry affected by data breaches, with healthcare ranking third. The Public Administration sector held the top position in this regard.

The graph presented below captures a variety of industries that are more specific than the broad public administration category. Substantial findings emerged after conducting a thorough analysis of companies that fall under Verizon's public administration scope.
Notably, within Montana, 19% of breaches originated from organizations falling within the realm of public administration, establishing it as the most prominently affected category.

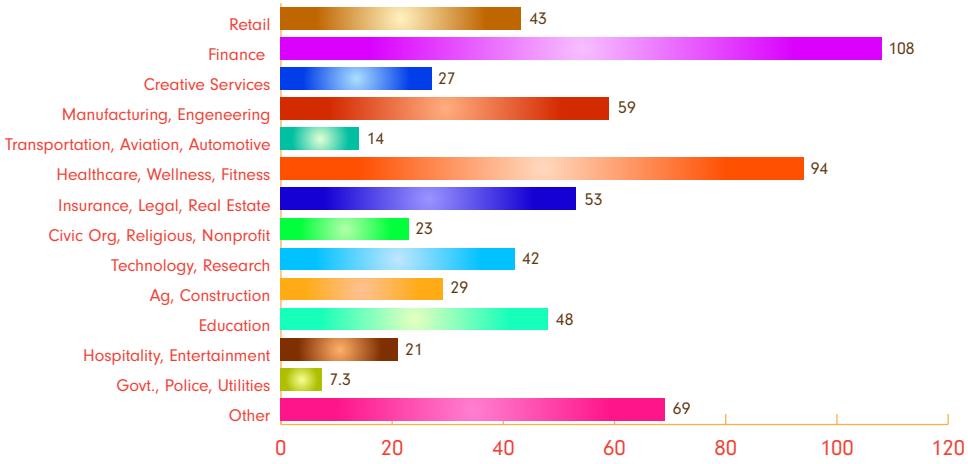
It's noteworthy, though, that data breaches impact all industries.
The "Other" column also accounts for companies for which industry information was not found.



% of Industry Prevalance

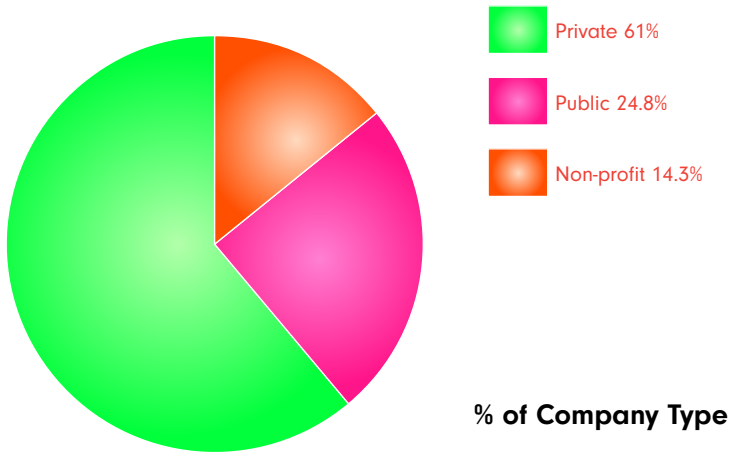
- Other 10.2%
- Retail 6.4%
- Govt, Police, Utilities 6.5%
- Hospitality, Entertainment 3.1%
- Education 7.1%
- Agriculture, Construction 4.3%
- Teachnology Research 6.2%
- Insurance, Legal, Real Estate 7.9%
- Healthcare, Wellness, Fitness 13.9%
- Aviation, Automotive, Transportation 2.1%
- Manufacturing, Engineering 8.8%
- Creative Services 4%
- Finance 16%

Number of Breaches in each Industry



Company Type & Age

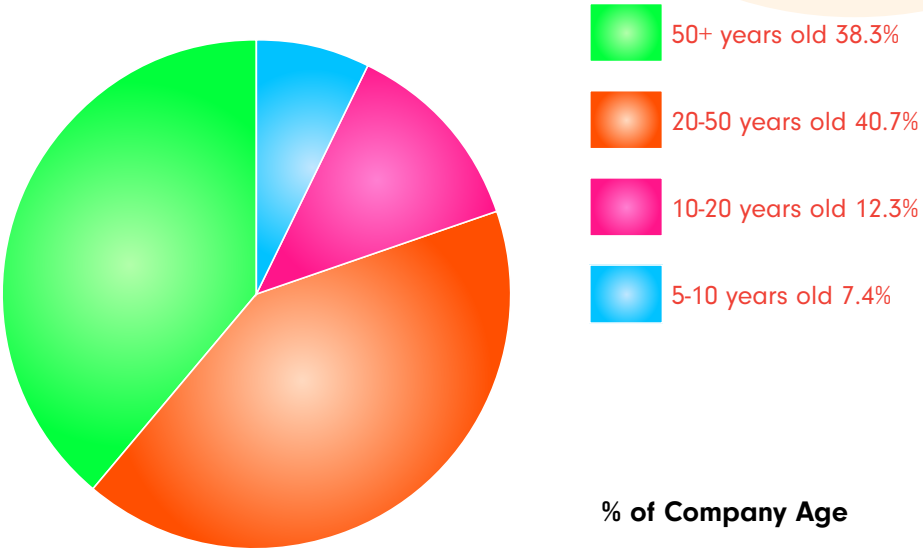
The data breach landscape in Montana during 2022 showcased a prominent trend: the majority of breaches were associated with private sector companies, constituting 61% of the impacted entities. However, it's important to acknowledge that public institutions and schools remained susceptible targets for attackers. This vulnerability can be attributed to the wealth of highly-sensitive data they house, making them appealing targets despite the prevailing trend toward private sector breaches.



% of Company Type

In the year 2022, a significant pattern emerged: a majority of breached companies had been established for at least two decades. This trend is likely linked to the prevalent technological challenges faced by older companies, as they often require modern technology to stay resilient in today's landscape. Budget constraints can be a significant factor limiting their ability to invest in necessary technology upgrades. Moreover, insights from MSSP Alert corroborate these findings, highlighting additional factors contributing to technological stagnation.

Employee resistance to adopting new software versions and a reliance on legacy software for device and operating system upgrades were identified as noteworthy reasons hindering technological progress. This data underscores the complex interplay of budgetary constraints, employee attitudes, and legacy systems that shape the technology landscape for these mature companies.



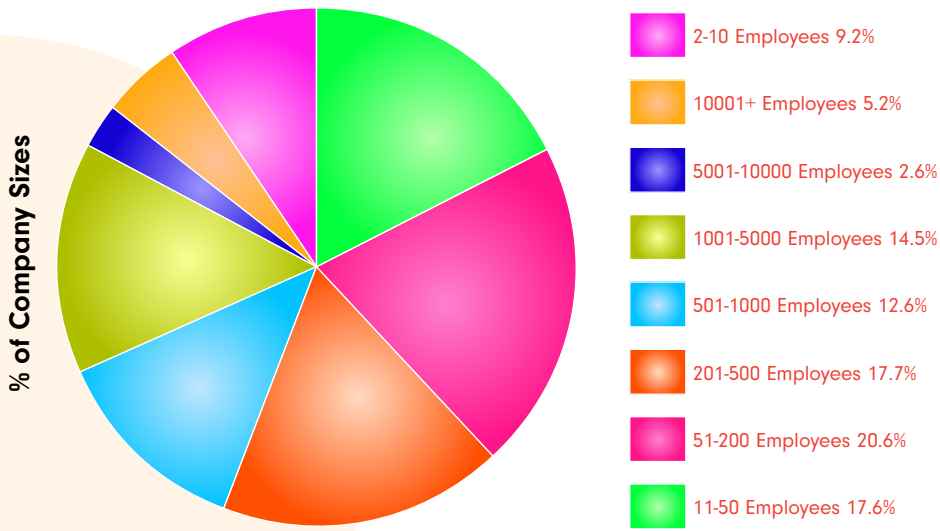
Company Size

IIn 2022, breaches predominantly affected companies with 50 - 500 employees, constituting 55.9% of cases. This result implies that small and medium-sized businesses (SMBs) are 1.23 times more prone to data breaches than very small (1-10 employees) and larger companies (501+ employees) in the state of Montana.

Possible reasons for this trend include:

- Budget constraints are hindering SMBs from investing in robust cybersecurity.
- Their tendency to collaborate with third-party entities rather than building their solutions.
- Hackers target them due to perceived lower sophistication.

Yet, both large and tiny companies remain at risk of data breaches. The 2021 Thales Data Threat Report disclosed that nearly half (45%) of US companies encountered breaches in the past year, emphasizing the widespread nature of the risk.

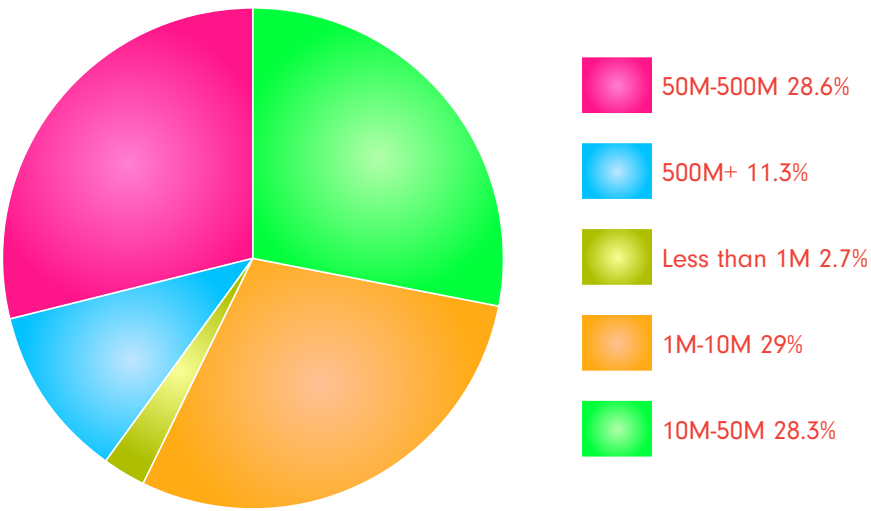


Company Revenue

The chart above shows that data breaches impacted companies across all revenue sizes in 2022. Notably, the most affected were those with revenue ranging from 1 to 10 million.

A survey conducted by Kaseya revealed that nearly one-third of IT professionals reported needing an increased IT budget or resources to fulfill their company's technology needs. This survey encompassed insights from 943 global IT professionals.

These findings underscore that many companies don't consistently allocate sufficient budgets for proactive cybersecurity solutions irrespective of company revenue.

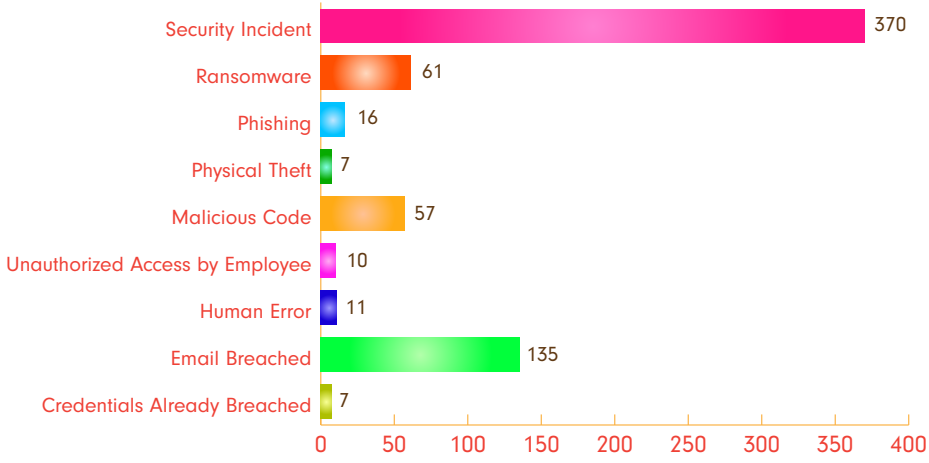


% of Company Revenue

Causes of Breaches

Causes of Breaches

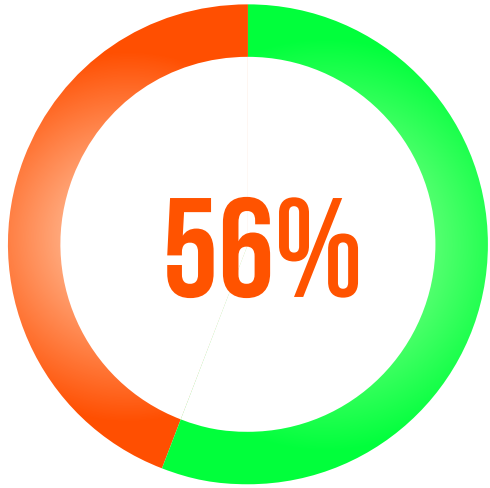
In Montana, companies afflicted by data breaches are not required to disclose the precise breach cause. Still, many organizations do include how they were breached, but when they don't, they can utilize the term "security incident" for reporting. Presently, HB 50 seeks to establish a definition for "security incident" to help with insights into the kind of attacks that affect Montanans. In our graph above, you will see that security incidents make up most of the attacks. However, if we knew the nature of these security incidents, they could easily fall under any category. Therefore, we advise focusing on the quantity of breaches outside the "Security industry" bar.



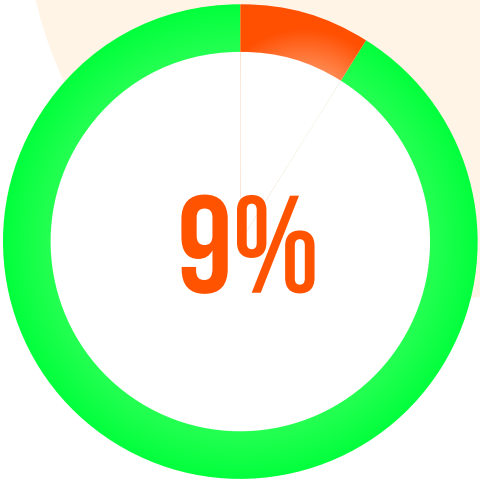
Security Incident

In 2022, 56% of data breaches were attributed to security incidents. As mentioned earlier, the term “security incident” lacks a specific definition in Montana, encompassing a range of potential causes. These causes include those listed within this report, such as ransomware, phishing, physical theft, malicious code, human error, compromised credentials, unauthorized employee data access, and unauthorized access to email or other account login credentials.

However, for cyber incidents that don’t align with any of the causes mentioned above, another potential factor could be the presence of malware. The term “malware” is derived from “malicious software” and encompasses any software meticulously crafted to infiltrate, impair, disrupt, or illicitly access computer systems, networks, or devices to cause harm and steal sensitive data. Malware encompasses many malicious programs, including viruses, worms, Trojans, ransomware, spyware, and adware.



Ransomware



Among the 674 incidents in 2022, 60 were attributed to ransomware, constituting 9% of breach causes. The impact of ransomware on these organizations occurred either through direct infection of the organization itself or via the infection of a third-party entity the company utilizes, where the attacks first gain access to the third party and then, from there, uncover credentials to access the company.

Ransomware attacks on organizations manifest through phishing schemes, system vulnerability exploits, or unauthorized access. Notably, while we have a designated section for phishing, not all successful phishing attempts result in ransomware incidents. Therefore, if an organization experiences a ransomware attack originating from a successful phishing scheme, it's categorized under ransomware in this data report. Refer to the phishing section for more insights.

But what is ransomware?

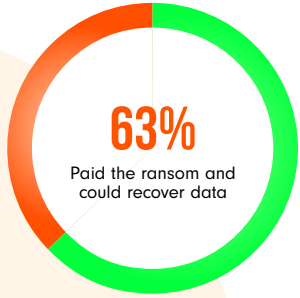
A ransomware attack initiates by gaining initial access, often achieved through phishing, exploiting vulnerabilities, emails, or human error. Yet, not all phishing or password breach cases lead to ransomware attacks. This distinction is crucial in this report; if a ransomware attack stems

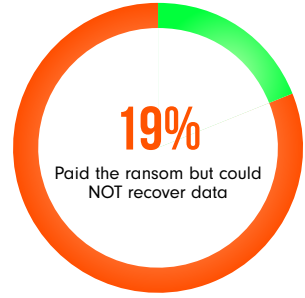
from a successful phishing attack, it's classified within the ransomware data rather than the phishing data.

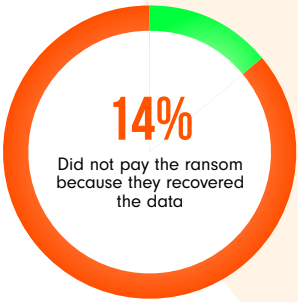
After gaining access, the attacker seeks to elevate their privileges. In practical terms, if a hacker infiltrates via an employee's email and that employee lacks access to highly sensitive corporate data, the hacker strives to find further vulnerabilities to expand their reach. They particularly target backup servers, security system control panels (e.g., Security Information and Event Management - SIEM or Endpoint Detection and Response - EDR), and virtualization platforms like VMWare VCenter.

Access to these crucial systems is sought because, during a data hostage situation, companies may have no other means of accessing their data. Following this, the attacker extracts data, eliminates backups, encrypts information, and ultimately demands a ransom for data release.

Nevertheless, it's important to note that paying a ransom doesn't guarantee the successful recovery of data, as highlighted by Veeam, a leading global backup solution provider:



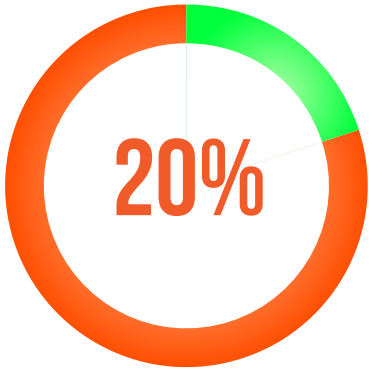




The amount an organization pays in a ransom is contingent upon various factors, including the ransom demand itself, the organization's size, and the compromised data type. While the 55 Montana-based organizations affected by ransomware haven't publicly disclosed their expenditure, the cost of ransomware comprises two components: the actual ransom and the expenses related to downtime and recovery. Notably, the ransom demanded is typically around 3% of the company's annual revenue, according to Check Point Research (CPR).

On average, a ransomware attack lasts for 22 days, according to Statista. In the context of the 60 ransomware attacks in 2022, the average duration to halt the breach was 31.58 days, surpassing the general average. These incidents impacted 10,588 Montanans, whose sensitive data was compromised.

Accessed Emails



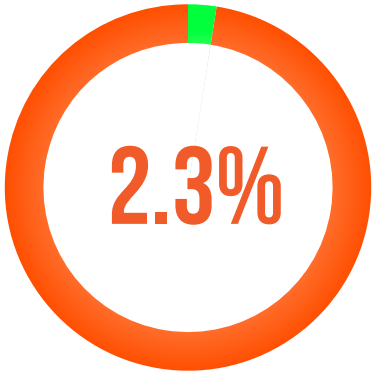
In 2022, breaches attributable to unauthorized access to email accounts accounted for 20% or more of the incidents. The nature of these email breaches—whether they resulted from phishing schemes or compromised login credentials—is uncertain.

Cybercriminals employ a range of tactics to compromise email accounts for malicious purposes. One prominent method is "credential stuffing," wherein attackers use leaked username-password combinations from previous data breaches to gain unauthorized access to email accounts. This tactic's success is fueled by individuals reusing passwords across multiple services. Once a hacker gains control of an email account, they access sensitive data encompassing personal information and financial records, which they can exploit against the account owner. Compromised email accounts also allow cybercriminals to execute additional crimes, such as Business Email Compromise (BEC) attacks. In these scenarios, hackers impersonate high-ranking executives to deceive employees into transferring funds or divulging sensitive information.

Furthermore, attackers can exploit compromised email accounts to launch targeted phishing campaigns. Utilizing the victim's contacts and the guise of legitimacy, cybercriminals substantially heighten the likelihood of success in these deceitful endeavors. Phishing emails sent from trusted addresses mislead recipients into clicking malicious links or downloading infected attachments, resulting in malware infections or more data breaches. Industries managing sensitive data, including

finance, healthcare, and government, constitute primary targets for compromised email attacks due to potential lucrative gains and substantial disruptions. Successful breaches can yield significant financial losses, tarnished reputations, and compromised confidential data, amplifying the ramifications across dimensions and causing widespread devastation.

Phishing



In 2022, at least 2.3% of breaches resulted from successful phishing campaigns, totaling 15 incidents.

When comparing our findings with the 2022 Verizon Data Breach Report, which indicates that phishing scams contribute to nearly 36% of all data breaches, we contend that this percentage is likely significantly higher but businesses chose to not include that information in the data breaches.

Phishing remains an ever-present and alarmingly effective cyberattack technique employed by malicious actors to illicitly acquire sensitive information from unsuspecting individuals. This cunning approach involves masquerading as trusted entities via emails, text messages, or social media, aiming to trick victims into divulging their login credentials, financial particulars, or personal data.

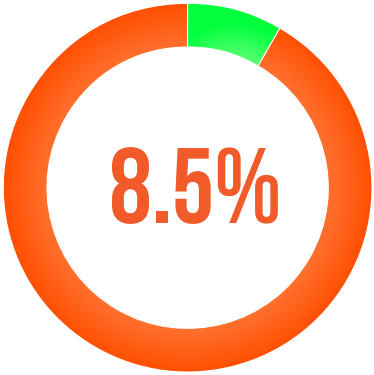
Phishing attacks hold a substantial share among the landscape of cyber threats, with phishing emails constituting a significant portion of global spam. The prevalence of identified phishing websites and URLs is on the rise, demonstrating heightened success rates during major events or holidays when users tend to be more susceptible to misleading links.

Industries dealing with sensitive information, most notably finance, healthcare, and government sectors, find themselves at the forefront of

phishing attacks. Successful instances of phishing lead to substantial financial losses, data breaches, and incidents of identity theft.

To counter the risks associated with phishing, maintaining a state of constant vigilance, regularly updating software systems, and implementing robust security measures are critical. These proactive steps are essential in safeguarding against the ever-evolving landscape of these cyber threats.

Malicious Code



In 2022, a minimum of 8.5% of breaches were attributed to the injection of malicious code into a company's website.

A notable incident involved a third-party vendor responsible for hosting numerous websites, which experienced the injection of harmful code into their clients' websites. As a result, a diverse array of industries were adversely impacted by this attack.

The persistent and concerning threat of malicious code injection into websites remains a critical concern within the realm of cybersecurity. This technique serves as a means for cybercriminals to compromise legitimate websites, potentially leading to severe repercussions for both users and website owners.

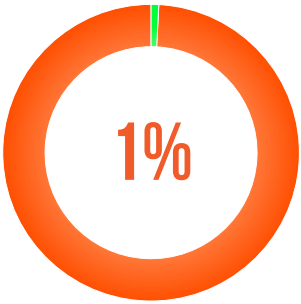
Code injection attacks typically exploit vulnerabilities within web applications to insert malevolent code into the underlying codebase of a website. This malicious code can manifest in various forms, including SQL injection, cross-site scripting (XSS), or remote file inclusion. Once embedded, this code can execute a range of detrimental actions, such as stealing sensitive data, disseminating malware to site visitors, or even commandeering the entire website.

The ramifications of such attacks are extensive. Unsuspecting website visitors may fall prey to data breaches or malware infections, exposing

their personal information and digital security to jeopardy. Concurrently, website owners face tarnished reputations and potential legal ramifications if their platforms unwittingly facilitate cybercrime.

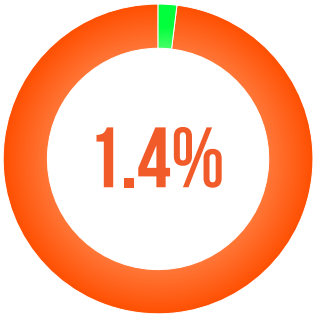
To counteract the threat of malicious code injection, a multifaceted approach to website security is imperative. Regular security assessments, swift rectification of vulnerabilities, and meticulous input validation practices collectively strengthen web applications against potential exploits. Moreover, the deployment of web application firewalls (WAFs) and intrusion detection systems (IDS) is essential in actively monitoring and thwarting suspicious activities, offering crucial layers of defense against this pervasive threat.

Physical Theft



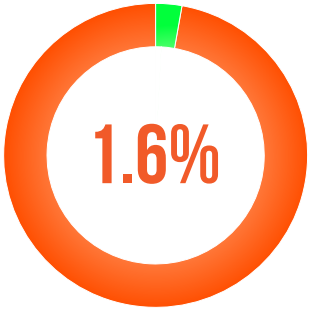
Throughout 2022, a total of 7 incidents involving physical theft occurred. In these cases, unauthorized individuals forcibly entered offices and absconded with devices containing individuals' data. These pilfered devices encompassed USBs, hard drives, and laptops. The motivations behind these thefts remain uncertain; it is unclear whether the objective was to access the data on the devices or to erase their contents for potential resale.

Unauthorized Access from Employee



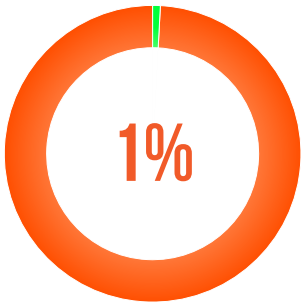
In 2022, a minimum of 9 instances were recorded wherein employees accessed clients' data without the requisite authorization or necessity. These occurrences encompassed various sectors, including

financial and healthcare institutions. Additionally, some cases involved employees forwarding clients' data to personal email addresses.



Human Error

In the year 2022, a minimum of 11 breaches resulted from human error. These instances encompass scenarios such as inadvertent retention of identifiable client data within emails or presentations.



Credentials Already Breached

In the year 2022, there were 7 reported incidents where a client's compromised credentials were exploited by hackers to gain unauthorized access to another account, consequently leading to a data breach within the affected organization.

Looking Ahead

In the years 2023 and 2024, organizations are anticipated to encounter a blend of familiar but evolved threats, including phishing, as well as emerging threats stemming from AI exploitation and vulnerabilities within supply chains.
Outlined below are three specific threats that warrant attention:

1. **AI-Powered Attacks:** The utilization of artificial intelligence by cybercriminals to orchestrate sophisticated attacks is anticipated to rise. AI-driven techniques could facilitate more precise targeting and evasion of traditional security measures.
2. **Supply Chain Vulnerabilities:** Organizations' reliance on complex supply chains creates new avenues for breaches. Attackers may exploit vulnerabilities within these networks to infiltrate and compromise multiple interconnected entities.
3. **Ransomware Innovation:** Ransomware attacks are expected to evolve with refined techniques and targeting strategies. The ransomware landscape may witness the introduction of new variants and methods.

These insights underscore the dynamic nature of cybersecurity threats and underscore the necessity of proactive strategies to protect sensitive information and critical systems. As technology evolves, cyber attackers adapt their tactics, underscoring the significance of sustained vigilance and preemptive security measures for safeguarding digital assets.

Questions?

Should you have any inquiries or seek to enhance your organization's resilience against cybersecurity threats, do not hesitate to engage with Pine Cove Consulting. Our team of seasoned cybersecurity professionals is poised to support you in establishing formidable security protocols and remaining vigilant against the ever- changing threat landscape. Your organization's digital assets and sensitive data warrant utmost safeguarding, and we are committed to aiding you in achieving precisely that. Reach out to us for tailored guidance and solutions that align with your unique requirements. Together, we can fortify your cybersecurity defenses, paving the way for a more secure digital trajectory for your enterprise.


www.pinecc.com/contact


+1800 432-0346


sales@pinecc.com