PINE COVE CONSULTING

Montana Cyber Security Report

REPORTING ON 2020 DATA BREACHES IN MT

A record number of organizations faced cyber-breaches in 2020 affecting tens of thousands of Montanans.

pine cove CONSULTING

www.pinecc.com

Contents

How Will You Respond?

By Brandon Vancleeve, President, Pine Cove Consulting

IT professionals typically experience more pressure than most employees. This pressure comes both internally and externally. Internally, executives and end-users alike often have unrealistic expectations for their technology and can be quick to frustration when it's not working properly.

Externally, news outlets only talk IT when there is a major data breach or something seriously going wrong, vendors constantly create fear-inducing content to push product, and IT professionals have to always worry about how secure their network is from bad actors.

Amidst all of this outside pressure, IT professionals have an opportunity to respond timidly or courageously. The tricky part is finding the balance between remaining educated and diligent in your efforts and blocking out the external noise that is not productive.

At Pine Cove Consulting we strive to takeaway from your pressure by providing both valuable content and personalized products and services.

The Montana Cybersecurity Report is designed to report the facts regarding data breaches in Montana, along with basic commentary on what we've observed in the year and what we expect to see in the upcoming year. I am confident the information provided in this report will be beneficial to you and will assist you in understanding the threat landscape.

In 2021, I invite you to join me in responding to the pressures by remaining diligent and resolute in your pursuit of security.

Montana Code Annotated

Montana law (see below) dictates that companies report breaches of data to the Montana Department of Justice regardless of whether the breach came because of hacking, criminal cyber-attacks, or human error.

> "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.

Montanans Affected by Cyber Breaches

According to 2018 U.S. Census data, there are just over one million residents in the state of Montana. The data gathered from the MTDOJ show that, over the course of the last six years, 899,058 Montanans have been affected by a cyber-breach. Assuming each one of these individuals is unique, that would mean that 89.4% of all Montanans have fallen victim to a data breach in the last six years.

These data breaches can result in as little as passwords being shared and as much as social security numbers being compromised.

Montanans should demand better security from the companies that hold their precious data.

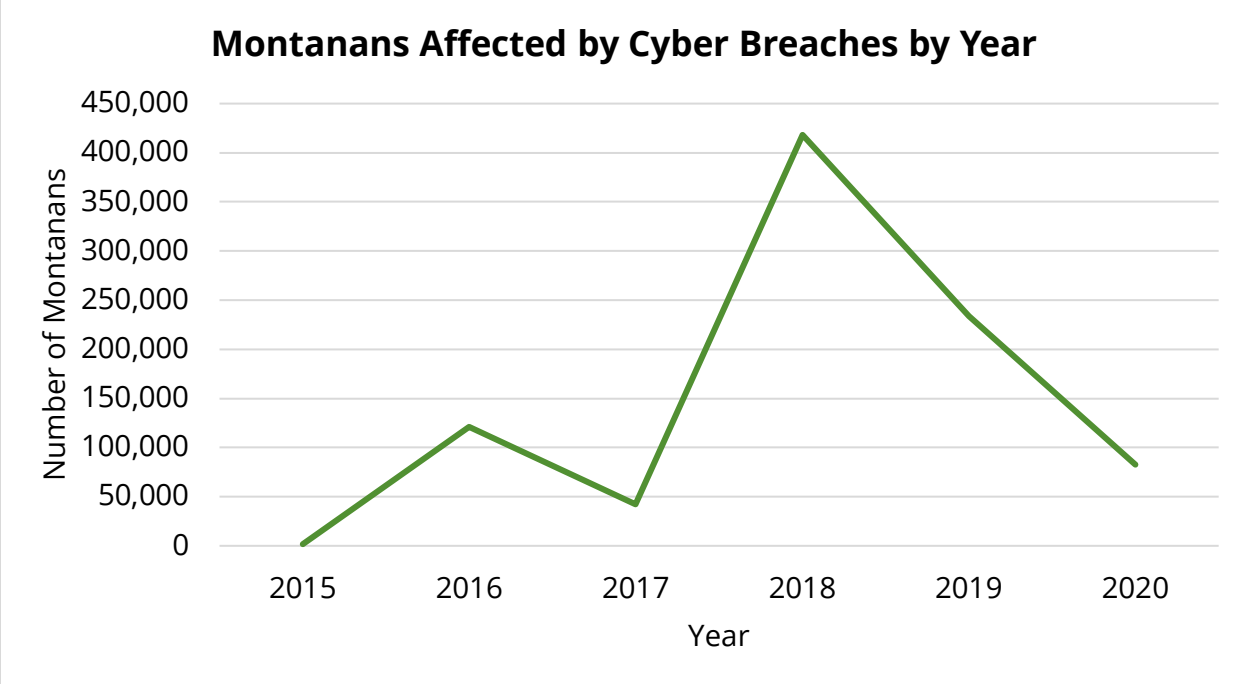
2020 Findings

A few interesting notes from our 2020 observations. First, **a total of 82,531 Montanans were affected by a data breach in 2020**. This number is down from 233,485 Montanans in 2019. This is a significant drop compared to previous years. In previous years there have been 1-5 major data breaches from large companies that affect more than 100,000 Montanans. This year the largest data breach affected 32,370 Montanans. Interestingly, although the number of Montanans affected by data breaches decreased, the number of organizations suffering a breach increased (more on that later).

Montanans Affected Through the Years

As mentioned above, the number of Montanans affected by a data breach was lower in 2020 compared to 2019 and 2018. Overall, looking at the past six years, we see a lot of variability in the number of Montanans affected by a data breaches. It's difficult to understand why this is. Our best guess is that the handful of large data breaches that affected 100,000+ Montanans in 2018 and 2019 negatively skewed the data those years. Nevertheless, we are happy to report the decline but also acknowledge that 82,531 is nothing to write-off.

It is important for businesses to stay vigilant and educated with regards to the threats and the products and services to protect them from those threats.



Length of Cyber Breaches

In analyzing the last six years of data breaches affecting Montanans, only 31% of the attacks lasted one day. The other 69% of cyber-attacks lasted more than one day, with the longest reported breach lasting 9222 days (that is a 25 yearlong cyber-attack!). That attack, reported in 2020, broke the previous record, set in 2017, of 6202 days (nearly 17 yearlong cyber-attack). The length of cyber-attacks is something that we believe needs to be discussed more. Sometimes organizations spot a breach in their network and it takes days, months, or even years to remove the threat. Other times, organizations are suffering a data breach and don't even realize it until days, months, or years later. Both of these situations are disastrous.

Organizations, both small and large, are now realizing the need for an improved cybersecurity operation that can hunt down and remediate threats that plague their organizations.

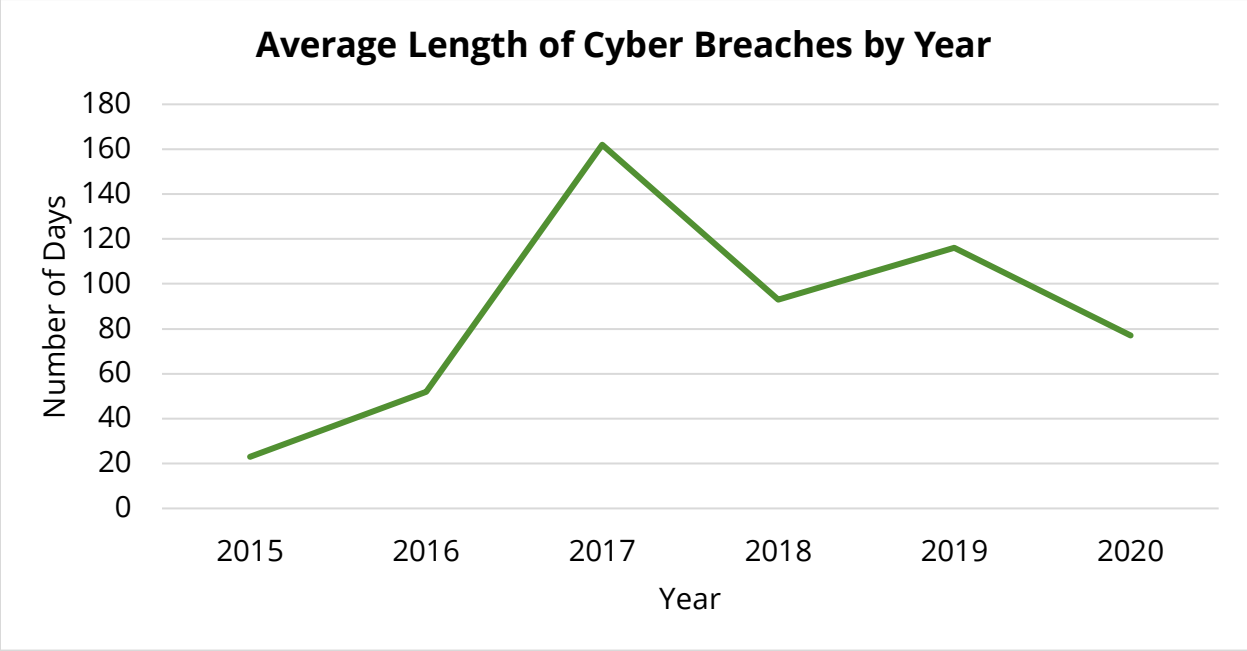
2020 Findings

In 2020, the average number of days an organization suffered a cyber-attack was 77 days. The 77-day average is down from 116 days in 2019 and 93 days in 2018. It is good to see this trending in the right direction, but a data breach lasting even a few hours can be catastrophic, let alone a 77-day data breach.

Organizations thinking about protecting themselves should also think about what to do if they do suffer a data breach and what its response looks like once the organization is compromised. Remediating cyber-attacks in a timely manner is necessary.

Average Length of Cyber Breaches Through the Years

In the last six years we have seen the average length of these cyber breaches fluctuate a bit. The lowest average number of days was 23 days in 2015 with the highest average number of days suffering from a data breach clocking in at an average of 162 days in 2017. This is a significant number of days to have an unauthorized user in your network. The cybersecurity solutions on the market designed to help companies remediate cyber-attacks after they have been infected are fairly new and becoming more and more powerful. We are optimistic that as adoption of these technologies increases, the average length will decrease.



Organizations Affected by Cyber Breaches

There are many reasons organizations choose not to invest in cybersecurity. These rationalizations are often the downfall of these organizations. According to multiple news sources, cyber-attacks cost organizations more than $200,000 on average and put many organizations out of business. The $200,000 doesn't represent the full extent of damages caused by most of these cyber-attacks. Organizations should also consider the damages caused from shutting down operations for an extended period of time while they remedy the attack, loosing precious data, and the reputation damage resulting from leaking end-user and/or client data.

According to CNBC, of the businesses that are hit with cyber-attacks, 60% go out of business within 6 months because they simply can't recover from the damages.

There exists a misconception that organizations should find a healthy balance between risk of cyber-attacks and investment in cybersecurity. If you have invested in some cybersecurity protection but holes still exist, hackers can often subvert any cybersecurity protection you have implemented once they enter your network through an unsecured aspect of your network. The costs resulting from data breaches are significantly higher than that of protecting your organization in the first place.

Another common misconception we hear in Montana is, because Montana is a rural state, we aren't as susceptible to cyber-attacks compared to states with a larger population. This is **NOT TRUE**. The data presented in this report will combat this misconception and hopefully encourage action from organizations with this belief. Hackers do not care where you live, they only care if you don't have your assets secured with necessary cybersecurity protection.

2020 Findings

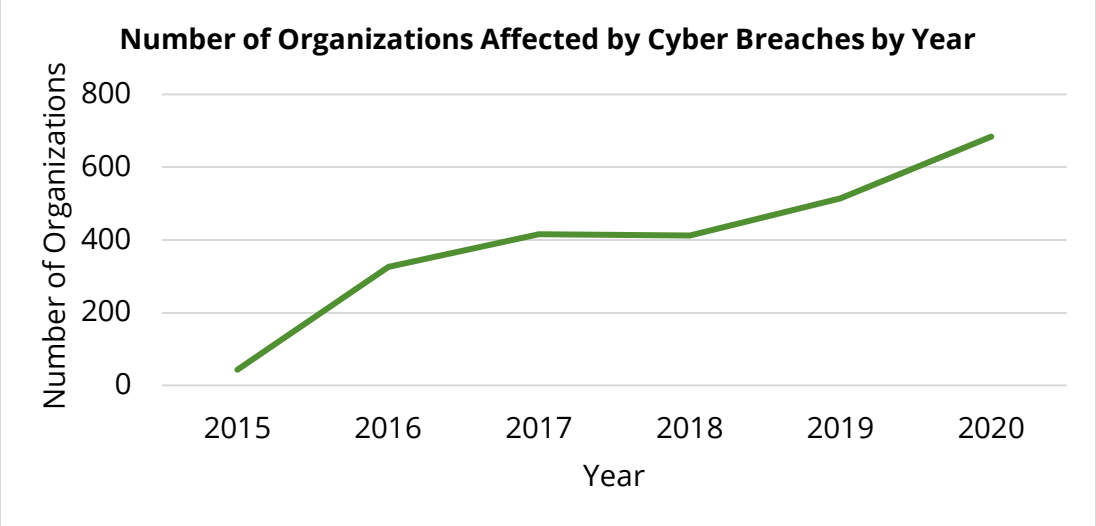
In 2020, we saw yet another record number of organizations get hit with cyber-attacks that affected Montanans. In fact, we saw a 33.1% increase in successful cyber-attacks in 2020 compared to 2019 and a 66% increase in successful cyber-attacks in 2020 compared to 2018. **684 organizations fell victim to a cyber-attack in 2020**. These organizations ranged from global financial institutions to small businesses.

The breach that affected the most Montanans in 2020 happened to Morgan Stanley who suffered a data breach that released Social Security and account numbers to third parties. This breach affected 32,370 Montanans.

Organizations Affected by Cyber Breaches Through the Years

We have seen a steady increase in the number of organizations that have fallen victim to cyber-attacks that affect Montanans in recent years. In 2020 we saw a jump from 412 organizations breached in 2018 and 514 in 2019, to a total of 684 in 2020.

As tactics for hackers continue to evolve and become more sophisticated, so must cybersecurity protection. Traditional endpoint security, although still necessary, will not be the be end all answer for the attacks of 2021. Organizations need comprehensive cybersecurity protection.



Looking Ahead to 2021

In 2021 we expect organizations to face both familiar threats such as ransomware, and new threats resulting from an increased remote workforce and new technology. Here are three specific threats we want to highlight:

1. Ransomware- I'm not sure we could produce a truly factual cybersecurity report without mentioning the continued threat of ransomware. In 2020 we saw ransomware pillage across the globe with especially significant damage to the healthcare and education sectors. This threat continues to be prevalent and there is no reason to believe it is going away anytime soon.

2. Remote working concerns- The insurgence of remote working, has led to increased cybersecurity concerns. Cybersecurity practitioners now have to expand their organization's security perimeter to every home network being used by employees. This presents unique challenges. Hackers understand these challenges and have reinvested in email scams, spam, and malware.

3. Nontraditional threats- Users have been quick to embrace new smart technology that can be found in smart TVs, cameras, doorbells, and some brands of appliances. Although not traditional computing devices, they provide hackers another way to gain access to the network if not secured properly.

These three different highlighted attacks represent a small portion of the attacks we expect to see in 2021. To read more about 2021 cyber-threats click the button below to read Sophos' 2021 threat Report.

Read More

Security Measures for 2021

As companies grapple with cybersecurity in 2021, we would like to offer a few security suggestions that can help guide your strategy in 2021 and give you a greater peace of mind:

1. Attention to detail- Some of the most devastating cyber-attacks of 2020 were a result of negligence in regard to basic security hygiene. Make sure you pay close attention to your cybersecurity posture to ensure your solutions are up to date and installed where necessary.

2. Prioritize education- It's hard to understand if you are adequately secured from the threats if you don't know what the threats are. Set aside time each week to examine the latest threats. Also prioritize education on the latest cybersecurity products in the market. Both the hackers and the defenders are both evolving quickly and its important to remain aware.

3. Have a plan- Every year we are contacted by organizations who just fell victim to a cyber-attack. We mobilize quickly to remediate the threat and implement products and services to prevent an attack from happenings again. We recommend having a plan for if you do suffer a data breach. How would you continue your operations, who would you need to call to begin remediation, and what measures do you have in place to restore data that may become corrupted or lost? Prepare for the worst but hope for the best.

We hope you found this report helpful. Visit www.pinecc.com to learn more about Pine Cove Consulting and our products and services.

Cover image background courtesy of vecteezy.com.

pine cove CONSULTING

We are dedicated to providing our clients the very best that technology has to offer. We personalize our services for each individual client by completing a comprehensive assessment.

Our Process

- Complete IT Assessment
- Design Personalized Solution
- Deploy Product/Service
- Support/Help Desk
- Sustain Solution

Our Products

- Cybersecurity
- Network Infrastructure
- Communications
- Physical Security
- Student Safety

Our Services

- Budgeting
- Support Services

Technical Background

- 30,056 Cyber-Attacks Stopped Daily
- 25,103 Users Currently Supported
- 3,094 WAPs Installed
- 2,221 Server Installs/Configs
- 35 Technical Certifications
- 28 Years of Experience

THE CHANNEL CO. CRN MSP 500 2020

2020 AWARD WINNER Channel Partners. Excellence in Digital Services

Contact

Sales@pinecc.com
pinecc.com/contact

www.pinecc.com

Where We Work

We work with businesses, government agencies, and educational institutions across the rocky mountain region. We have employees stationed across the region ready to assess and address your technological needs.

• Client ☆ Pine Cove Employees/Office locations