PINE COVE CONSULTING

Montana Cyber Security Report

REPORTING ON 2019 DATA BREACHES IN MT

A record number of organizations faced cyber-breaches in 2019, affecting hundreds of thousands of Montanans.

pine cove
CONSULTING

www.pinecc.com

Contents

Diligence in Cyber- Security 3

Montana Cyber-Security Laws 4

- Montana Code Annotated 5
- Montana Cyber-Security Investment 6
- Montana Student Data Privacy 7

Montanans Affected by Cyber Breaches 8

- 2019 Findings 8
- Montanans Affected Through the Years 9

Length of Cyber Breaches 10

- 2019 Findings 10
- Average Length of Cyber Breaches Through the Years 11

Organizations Affected by Cyber Breaches 12

- 2019 Findings 13
- Organizations Affected by Cyber Breaches Through the Years 13

Looking Ahead to 2020 14

- Security Measures for 2020 15

About Pine Cove Consulting 16

Diligence in Cyber-Security

By Brandon Vancleeve, President, Pine Cove Consulting

Cyber-Security is more of a marathon than a sprint. While implementing a solution quickly is possible; maintaining, managing, and upgrading is necessary as time passes. Threats evolve faster now than ever before. As security practitioners, we owe it to our organizations and end users to acknowledge the evolution and combat it with necessary security measures. Those that don't, will fail. In 2019 we saw a record number of organizations face a data breach that affected nearly a quarter-million Montanans.

There is reason for optimism as organizations across Montana are embracing the challenge and implementing the necessary changes. Organizations are realizing that proactive protection is better than reactive regret. Large and small organizations are realizing the threat is real and local. We have worked with many organizations across the state that have battled cyber-attacks in the last year and come out victorious.

As cyber-attacks have become more sophisticated, so has the security. We now can offer managed threat hunting, detection, and response (MTR), which enables organizations of all sizes to have access to a premier cyber-security operations center (SOC-As-A-Service). This solution, coupled with a holistic cyber-security strategy, allows for peace of mind for IT teams across the state.

In 2020, I invite you to join me in diligently prioritizing your cyber-security efforts. I hope you find this report informative and that it assists you in whatever role you play in securing your assets.

Montana Cyber-Security Laws

Here are a few notes regarding Montana's cyber-security laws. In 2015, Montana implemented a law requiring all organizations to send a copy of consumer notifications, sent to consumers when that organization faces a data breach, to the Office of Consumer Protection (COP). This information is compiled and shared on the Montana Department of Justice (MTDOJ) website. When received, the MTDOJ publishes this information online including the names of the organizations that suffered data breaches, the notification documents that are sent to affected individuals, the date the breach started and ended, the date the breach was reported, and the estimated number of Montanans affected by the breach.

A few things to note about this information:

1. The information isn't all there. Many entities report that an "unknown" number of Montanans were affected.

2. This information is only as accurate as what they receive from organizations which have suffered a breach. We assume some organizations simply don't report their breaches to the MTDOJ.

3. When it comes to the start and end date of the breach, this is estimated in many instances.

4. The law requiring organizations to report cyber-breaches to the MTDOJ went into effect mid-2015. We don't have complete information for the year 2015.

We, at Pine Cove Consulting, have analyzed this content dating back to the implementation of the law in 2015. We break down 2019 statistics individually and relative to each year since the information was made available. We are proud to make this report available and hope it assists you in 2020.

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 their website for transparency reasons. Pine Cove Consulting has 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.

Montana Cyber-Security Investment

Montana's State Legislature and governing body made an investment in cyber-security in 2019. In House Bill 2- The General Appropriations Act- The Montana State Legislature created the "Montana Cybersecurity Enhancement Project" which appropriates $3.1 Million dollars to improve its cyber-security protection.

As dictated in the General Appropriations Act:

> "The Montana Cybersecurity Enhancement Project is restricted to expenditures for: next generation antivirus software; cybersecurity staff; cybersecurity student programs; web application firewall; e-mail security gateway; security information and event management; analytics-driven security and continuous monitoring for threats; governance, risk, and compliance software; enterprise risk assessment; digital forensics lab; source code repository; security orchestration, automation and response; and outsourced professional services."

This marks a significant, and warranted, increase in budget for cyber-security protection for the state. In 2019, we saw a significant number of government entities across the nation suffer from crippling data breaches. The State Information Technology Division has recognized the need for increased cyber-security measures. Hopefully Montana organizations can see this example and ensure that they too are protected with necessary cyber-security.

Montana Student Data Privacy

In the 2019 legislative session, legislators grappled with policy proposals to secure student data in K-12 institutions. HB745 was passed and signed into law. This bill requires schools and associated vendors to complete a data privacy agreement. Specifically, the new law specifies the proper use and protection of student data while also establishing consequences for improper use of student data. This is the first effort of its kind to mandate student data protection at a state-wide level by the Montana State Government.

Schools are currently trying to figure out the best way to implement this law across the state. While it is difficult to accurately estimate the number of students affected by data breaches in any given year, experts agree that the number is significant. Once the data is obtained by the wrong people it is often held for ransom or sold on the dark web to those who may pursue identity theft.

“Student data deserves and needs protection,” said Justin Barnes, Anaconda School District superintendent. “We have sought this out in our own school district by collaborating as a school with our vendors and community, in conjunction with our implementation of cyber-security mechanisms to stop these breaches from happening.“

We will continue to monitor this law as it is implemented.

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 five years, 816,527 Montanans have been affected by a cyber-breach. Assuming each one of these individuals is unique, that would mean that 81% of all Montanans have fallen victim to a data breach in the last five years.

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

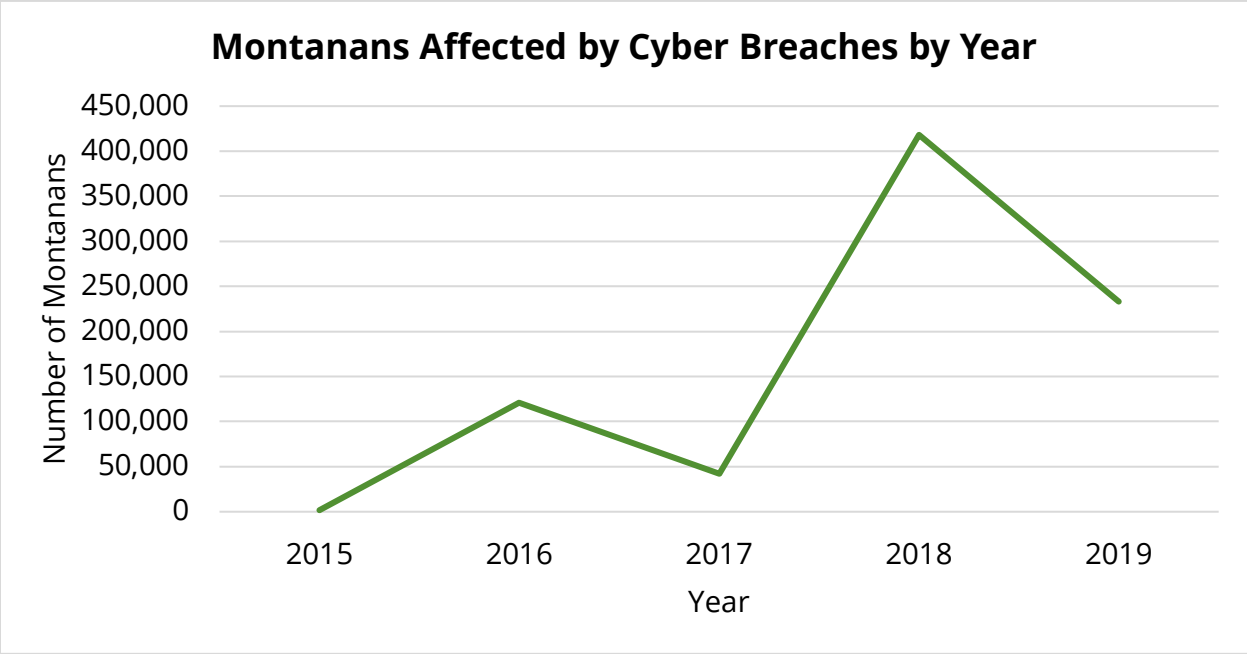
Montanans should demand better security from the companies that hold their precious data.

2019 Findings

A few interesting notes from our 2019 observations. First, **a total of 233,485 Montanans were affected by a data breach in 2019**. This number is down from 418,151 Montanans in 2018. However, something important to note is of the 418,151 Montanans whose data was breached in 2018, 377,052 came from one single data breach, Equifax. In 2019, outside of one major data breach resulting in 126,805 Montanans being affected, there were more cyber-breaches and more Montanans were affected across a larger number of organizations.

Montanans Affected Through the Years

As mentioned above, the number of Montanans affected by a data breach was lower in 2019 compared to 2018. This number may be misleading as so many Montanans fell victim to the Equifax data breach in 2018. Overall, looking at the past five years, we see a increase in the number of Montanans affected by a data breach and expect to continue to see this number climb in coming years unless organizations take the necessary measures to prevent such attacks.



Length of Cyber Breaches

In analyzing the last five years of data breaches affecting Montanans, only 36.7% of the attacks lasted one day. The other 63.3% of cyber-attacks lasted more than one day, with the longest reported breach lasting 6201 days (that is a 17 year long 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 a cyber-security operations center that can hunt down and remediate threats that plague their organizations.

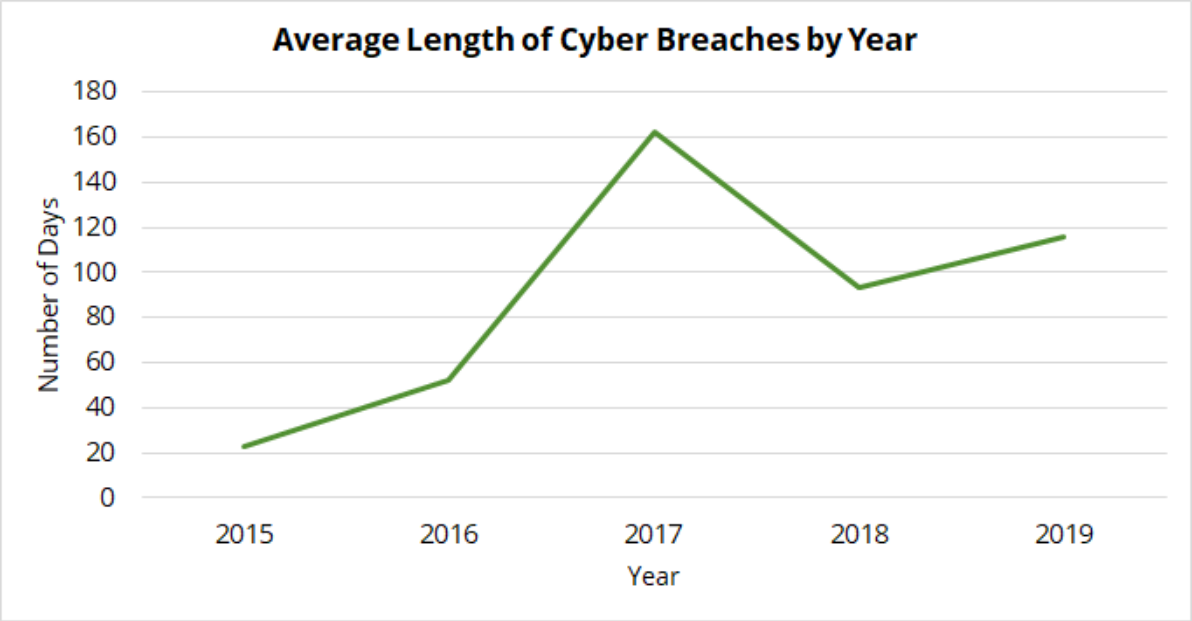
2019 Findings

In 2019, the average number of days an organization suffered a cyber-attack was 116 days (that is more than 1/3 of the year). The organization suffering the longest cyber-attack reported that its cyber-attack lasted 3164 days, nearly 9 years! The 116-day average from 2019 is up from 93 days in 2018.

Organizations that think 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 five 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. To combat this, organizations can invest in cyber-security operations which will enable them to hunt down and remediate threats once unauthorized activity penetrates their network.



Organizations Affected by Cyber Breaches

There are many reasons organizations choose not to invest in cyber-security. 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 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 resulting damage in reputation from leaking end-user and/or client data.

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 cyber-security. If you have invested in some cyber-security protection but holes still exist, hackers can often subvert any cyber-security 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 we live in 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 cyber-security protection.

2019 Findings

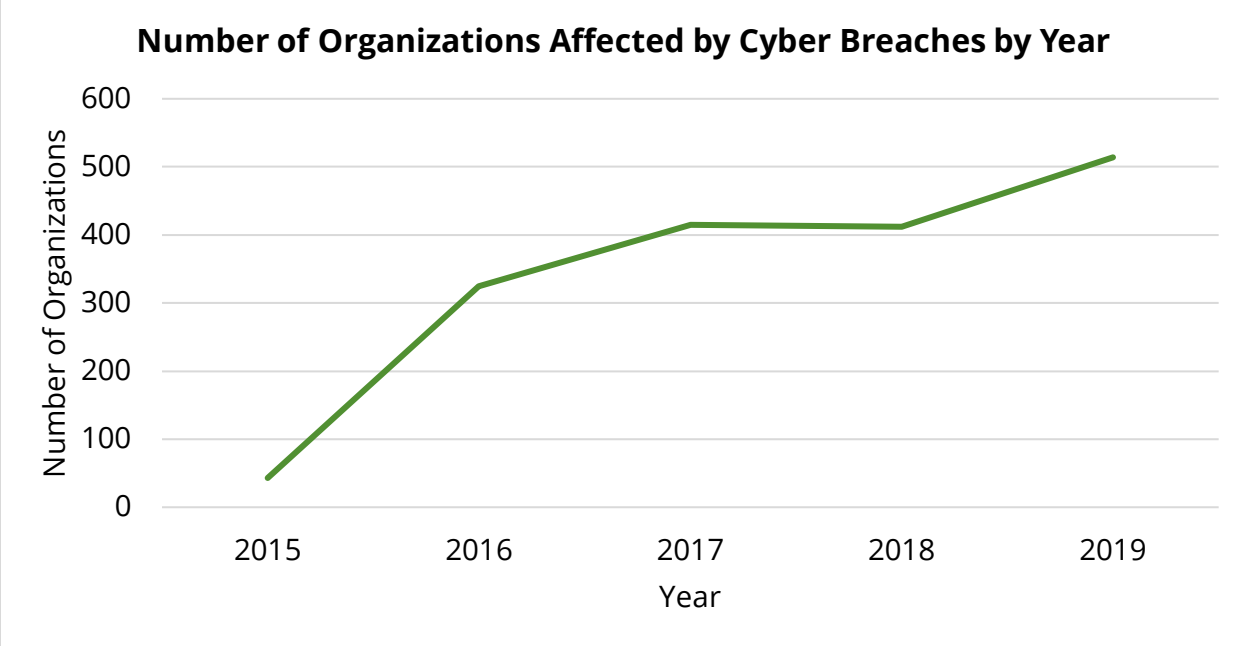
In 2019, we saw a record number of organizations get hit with cyber-attacks that affected Montanans. In fact, we saw a 24.8% increase in successful cyber-attacks in 2019 compared to 2018. **514 organizations fell victim to a cyber-attack in 2019**. These organizations ranged from large healthcare organizations to small ma-and-pa shops.

The largest breach of the year happened in Kalispell Montana which resulted in 126,805 Montanans being affected.

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 Montana in recent years. In 2019 we saw a jump from 415 organizations breached in 2017 and 412 in 2018 to a total of 514 in 2019.

As tactics for hackers continue to evolve and become more sophisticated, so must cyber-security protection. Traditional endpoint security, although still necessary, will not be the be all end all answer for the attacks of 2020. Organizations need next-generation cyber-security protection.



Looking Ahead to 2020

In 2020 we expect to see a continuation of the cyber-attacks we saw in 2019 including ransomware, mobile-based malware, cloud data breaches, Emotet, well as coordinated attacks by groups like Ryuk, and more. We expect to see more of these attacks in 2020:

1. Credential Stealing- Your security measures are only as effective as the admin credentials are. We saw several organizations fall victim to credential stealing which hackers then used to turn off cyber-security measures and penetrate the network. This type of cyber-attack will continue to grow in 2020.

2. Adware- Adware is software that installs itself on your device (commonly seen on mobile devices) and automatically pushes advertisements to users while generating money for the developer. These ads can be tricky to find and remove from your devices.

3. Automated-Enhanced Active Attacks- Hackers are now automating machines to do their dirty work. These machines are patient and wait for an opening to present itself in your network. Once it exploits that opening, it hands over controls back to the hacker which will then complete their objective.

These three different highlighted attacks represent a small portion of the attacks we expect to see in 2020. To read more about 2020 cyber-threats click the button below to read Sophos' 2020 threat Report

Read More

Security Measures for 2020

As companies grapple with cyber-security in 2020, we would like to offer a few security suggestions that can help guide your strategy in 2020 and give you a greater peace of mind:

1. You can't defend against what you don't understand. When analyzing cyber-attacks and weighing them against your cyber-security protection it can be easy to get lost in the complexity of it all. As cyber-security practitioners, we owe it to our end-users and consumers to protect their information and be aware of the threat landscape. Educate yourself on current threats and make sure security is a top priority for your organization. If you don't have the capacity to properly educate yourself, consider working with a vendor who has your best interests in mind.

2. Proactive protection is better than reactive regret. If your organization is proactively embracing security measures to combat these next-generation cyber-threats, you will not regret it. If your security lacks, you will regret not protecting the organization. The cost of cleaning up and securing your organization after an attack is significantly more than investing in proactive protection.

3. Build a threat response team. If you have a threat response team (also referred to as cyber-security operations or SOC) in place, in conjunction with necessary cyber-security measures, you will be able to mitigate threats as they attempt to penetrate your network. You will be able to trace their path taken in the attempt to hack you. If they do bypass your security measures, you can see where the threat resides and quickly remediate those threats. In the past this was tough for small organizations, however, you can now outsource this service for an affordable rate.

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

About Us

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

- Assess Current Technology
- Identify Improvements
- Review Technology Possibilities
- Implement Personalized Solution

Our Solutions

Cyber-Security **Communication** **Infrastructure**

Technical Background

- 30,056 Cyber-Attacks Stopped Daily
- 20,103 Users Currently Supported
- 2,527 WAPs Installed
- 2,008 Server Installs/Configs
- 35 Technical Certifications
- 26 Years of Experience

SOPHOS SECURITY AWARDS 2016 WINNER Complete Security Partner of the Year Pine Cove Consulting

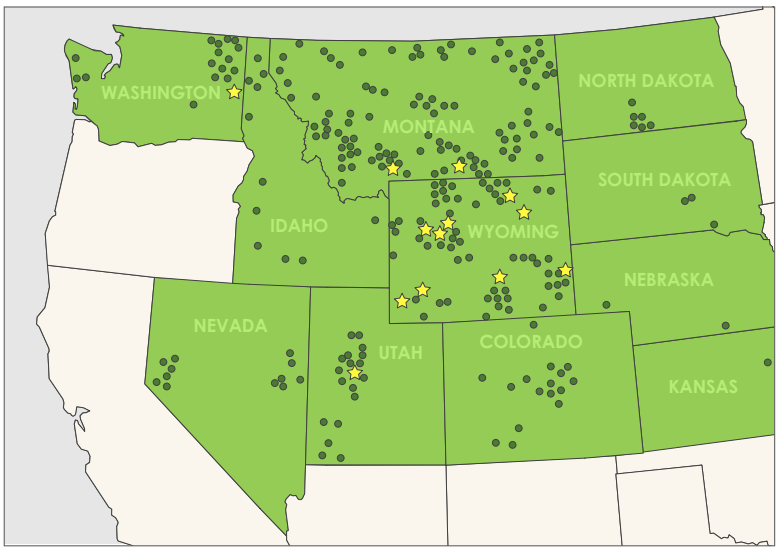
SOPHOS SECURITY AWARDS 2017 WINNER Q2 Partner of Quarter Pine Cove Consulting

SOPHOS SECURITY AWARDS 2018 WINNER Rising Security Star Award Pine Cove Consulting

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



Contact

Sales@pinecc.com
pinecc.com/contact

www.pinecc.com