2018 CYBER-SECURITY REPORT- MONTANA

www.pinecc.com

2018 Montana Cyber-Security Report

Introduction

Montana law (see below) dictates that companies report their 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))"

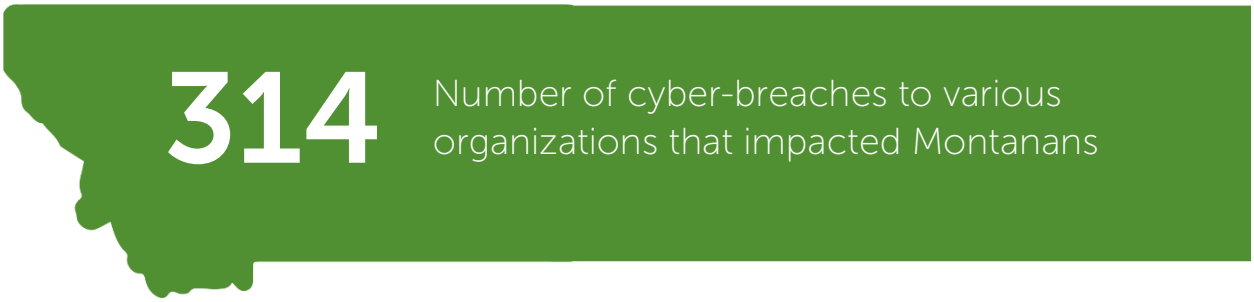
The Montana Department of Justice shares this information publicly on their website for transparency reasons. We at Pine Cove Consulting have taken the time to analyze this data and present it in a way that may help you better understand the threats and what you can do to protect yourself. In this report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

1. Overall cyber-breach statistics for Montana
2. Common types of cyber attacks
3. How you might consider preparing yourself for 2019 cyber-attacks.

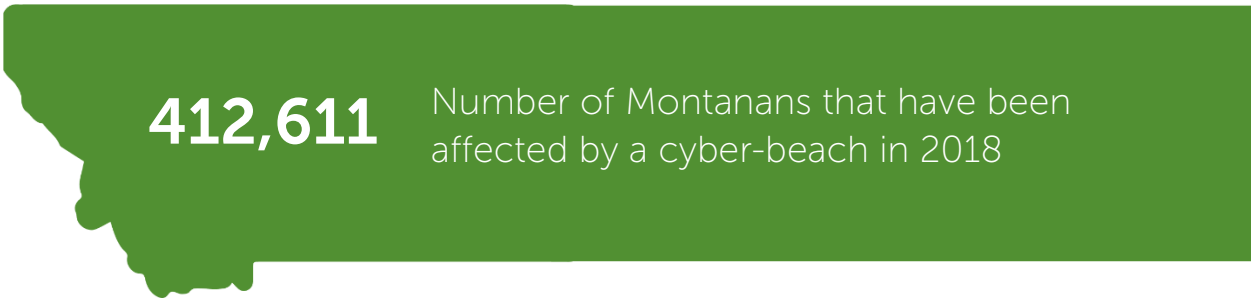
We hope you enjoy our findings and find them useful as you craft your cyber-security protection for the coming year.

2018 Montana Cyber-Breach Findings

In 2018, a significant number of Montanans saw their personal data breached. These breaches included organizations including government agencies, school districts, large nation-wide enterprises, ma and pa shops, and so much more. Montana organizations should shift their mindset from "what *if* a cyber-attack happens to me," to "how will I respond *when* a cyber-attack happens to me." Here are some statistics to give you some perspective:



The 314 reported cyber-breaches have come from organizations of all sizes spanning dozens of verticals. There is a false sense of security many small business owners choose to believe with sentiments such as "hackers won't target my business because it is small" or "I'm in Montana so the odds of a cyber-breach are lower." Hopefully this number, and the organizations behind this number, dispel that false sense of security. Organizations of all sizes are subject to cyber-attacks and should prepare accordingly. This number is also quite alarming considering that many cyber-breaches go unreported regardless of state law.



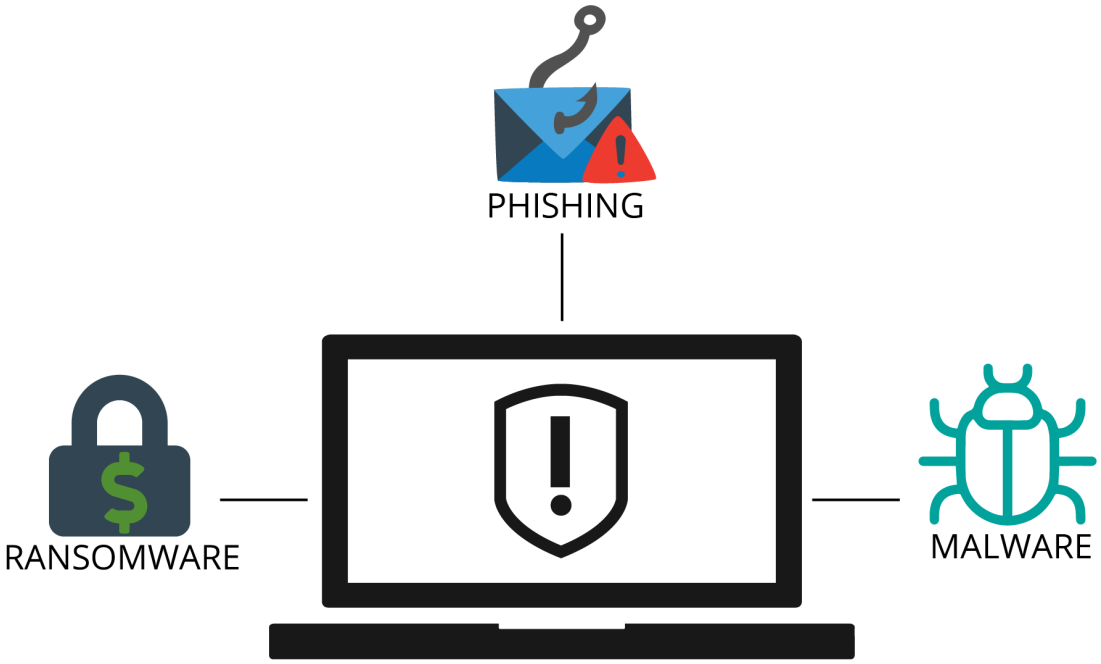
According to the most recent population estimates from the US Census, there are 1,062,305 residents in Montana. Assuming each Montanan affected by a cyber-breach is a unique individual, that would mean **38.8% of Montanans were affected by a cyber-breach in 2018**.

82 Average days between the start and end of cyber-breaches within Montana in 2018

82 days is a long time for cyber-criminals to harvest your organization's assets. In many instances, it can take organizations a long time to even realize their assets have been compromised, let alone act to remove the cyber-criminals from their systems.

Common Types of Cyber-Attacks

While Montana law doesn't dictate organizations to reveal how their data was breached, based on our observations and experience working with many of these organizations, we feel confident in listing ransomware, phishing, and malware as the most common types of cyber-attacks. These attacks are each uniquely equipped to penetrate organizations and access valuable information.



Ransomware

What is it: Ransomware is software that denies you access to your files or computer until you pay a ransom.

Ransomware Protection: Keep your system updated. That little notification in the bottom right corner of your screen can be important to protecting yourself from ransomware attacks. Cyber-criminals often target users who haven't updated their computers. Another important means of protection is backing up your documents. Make sure you have copies of all your important documents in case you ever get infected and can't retrieve them. Employees will never fail at downloading/opening suspicious content, so you should implement a more robust system of protection.

Phishing

What is it: Phishing refers to the process of deceiving recipients into sharing sensitive information with an unknown third party.

Phishing Protection: Prevention first starts with educating the members of your organization on how phishing works. Encourage employees and co-workers to be suspicious of emails from unfamiliar recipients or emails asking for sensitive information. However, education is not enough. There will always be that one employee who can't help but click on the bait in the email to see what is going on. According to statistics, 30% of recipients open phishing email links. What you really need is a comprehensive cyber-security solution that includes both educational mechanisms and security solutions.

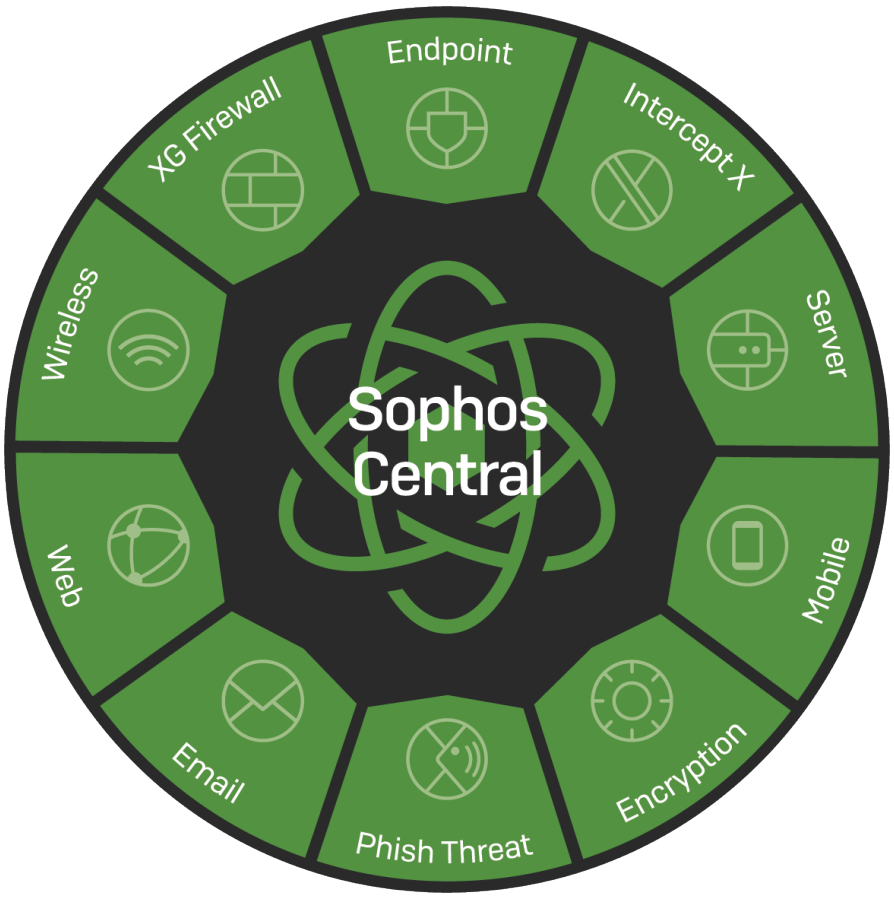
Malware

What is it: Malware is a general term for malicious software. Malware includes viruses, worms, Trojans and spyware. Many people use the terms malware and virus interchangeably. Malware is more of an umbrella term used to describe a lot of different cyber-attacks.

Malware Protection: Due to the expansiveness and diversity of malware attacks it's hard to pinpoint one specific way to protect against all malware attacks. Often companies find themselves having to go to multiple security providers to protect from all the different malware attacks. It is rare to find all the protection in one place, but with Sophos' Synchronized Security you can be protected from it all. Synchronized Security protects you from your firewall to your endpoint and everything in between.

How to Protect your Assets in 2019

Cyber-attacks are increasing and are projected to continue increasing in 2019. It is no longer a matter of *if* you will be affected by a cyber-attack, but *when* will you be affected. Our mindset is that your organization has either; **BEEN** attacked, is currently **BEING** attacked or **WILL BE** attacked by cyber criminals. Our mission at Pine Cove Consulting is to provide you the knowledge, the vision, and the solutions to secure your assets.



Synchronized Security

Synchronized security combines the products listed above to give you unparalleled protection by combining an intuitive security platform with next-gen products that actively work together to block advanced threats. To learn more about our cyber-security solutions, visit www.pinecc.com/cyber-security.