DIGITAL INVESTIGATIVE GROUP

TEN STEPS TO A

MORE SECURE ORGANIZATION

THECYBERDIG.COM

CYBER CRIMINALS TARGET ORGANIZATIONS OF ALL SIZES

In the news you have seen how cyberattacks are happening every day, everywhere, and Montana is no exception.

It is no longer a matter of if an organization will undergo a cyberattack, but rather when. These occurrences and their growing frequency demonstrate the risk posed by cybercriminals to disrupt our lives.

As a leader of an organization you face the task of ensuring your employees and customers are protected, and if the risk of a cyberattack cannot be mitigated, there is a plan in place to deal with it.

In this document, we'll help you better understand more about the impacts of a cyberattack and provide 10 steps your organization should take to be better protected and prepared in case of a cyberattack.

CONTENTS

A cyberattack can impact your organization in multiple ways, a few of which you might not expect. More than half of all cyberattacks are targeted at small organizations and the average cost to deal with a data breach is $120,000. **It is no wonder 60% of small businesses fail within a year of a data breach.**

By understanding the potential consequences of a cyberattack, you can appreciate the importance of implementing recommended cybersecurity measures. Proactive steps will help you to protect your organization, safeguard customer data, maintain your reputation, and ensure the trust of your community.

Some of the impacts your organization may see from a cyberattack are included on the following pages.

SECTION 1

IMPACTS OF A CYBERATTACK

FINANCIAL LOSS

A cyberattack can result in significant financial losses. Costs are associated with data recovery, system restoration, and potential legal expenses. Additionally, the reputational damage caused by an attack could result in a loss of customers and revenue.

DOWNTIME & DISRUPTION

If your systems are compromised, they may become unavailable or operate at reduced capacity. This downtime can disrupt day-to-day operations, affect productivity, customer service, and overall business continuity. It may take considerable time and resources to restore your normal operations, leading to potential revenue loss and customer dissatisfaction.

DATA BREACH & PRIVACY

A cyberattack can result in the theft or exposure of sensitive customer and organizational data. This includes personal information, financial records, and proprietary business data. Such breaches can lead to legal and regulatory consequences, damage your reputation, and erode the trust of your customers and partners.

INTELLECTUAL PROPERTY

Your organization may possess valuable intellectual property, trade secrets, or innovative ideas. A successful cyberattack could lead to the theft of this intellectual property, compromising your competitive advantage and potentially impacting future business growth.

OPERATIONAL DISRUPTION

Cyberattacks can disrupt your day-to-day operations by compromising critical systems, causing delays, and hindering decision-making processes. This disruption can lead to missed deadlines, reduced efficiency, and decreased employee morale.

REGULATORY COMPLIANCE

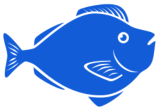
Depending on the nature of your organization and the data you handle, you may be subject to various data protection and privacy regulations. A cyberattack resulting in a data breach could lead to non-compliance with these regulations, resulting in penalties, fines, or legal actions.

REPUTATIONAL DAMAGE

The aftermath of a cyberattack can severely damage your organization's reputation and erode the trust your customers and community have placed in you. Negative publicity and word-of-mouth can deter potential customers from doing business, impacting your bottom line in the long term.

SECTION 2

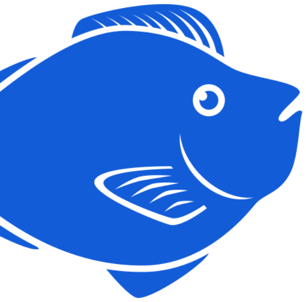
10 STEPS YOU CAN TAKE FOR A MORE SECURE ORGANIZATION



1

REQUIRE STRONG PASSWORDS

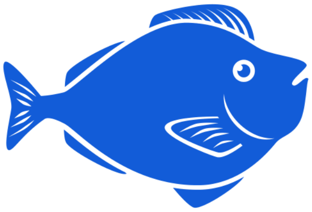
- Ensure you users are required to use unique and complex passwords for all accounts.
- Make a password manager available so creating and using complex passwords is convenient for users.



2

MULTI-FACTOR AUTHENTICATION

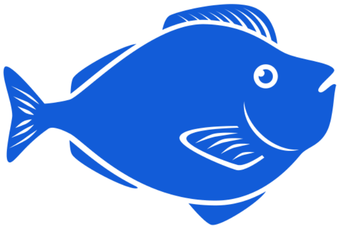
- Across your organization's IT environment, enable MFA wherever possible to provide an extra layer of security.
- Provide fobs or mobile devices to make this additional verification step easy for users.



3

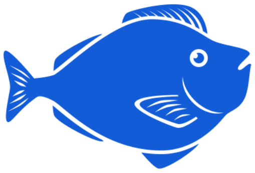
REGULAR SOFTWARE UPDATES

- Keep your operating systems, applications, and software up to date because updates often include important security patches that fix vulnerabilities.



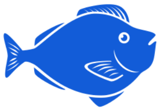
4 EMPLOYEE EDUCATION

- Train employees on cybersecurity best practices regularly.
- Provide training on how to identify phishing emails, avoid suspicious downloads, and practice safe browsing habits.



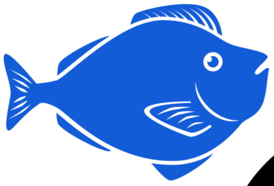
5 SECURE NETWORK

- Ensure your network is properly secured with firewalls, intrusion detection systems, and strong encryption because these measures protect your data from unauthorized access.



6 DATA BACKUPS

- Set up regular back ups for critical data.
- Backup locations should be offsite or in the cloud to ensure data can be recovered in case of a disaster or cyberattack.



7 INCIDENT RESPONSE PLAN

- Develop a detailed plan for the the organization to respond to cyber incidents.
- Assign roles and responsibilities to establish communication channels for quick response and recovery.

8 ACCESS CONTROLS

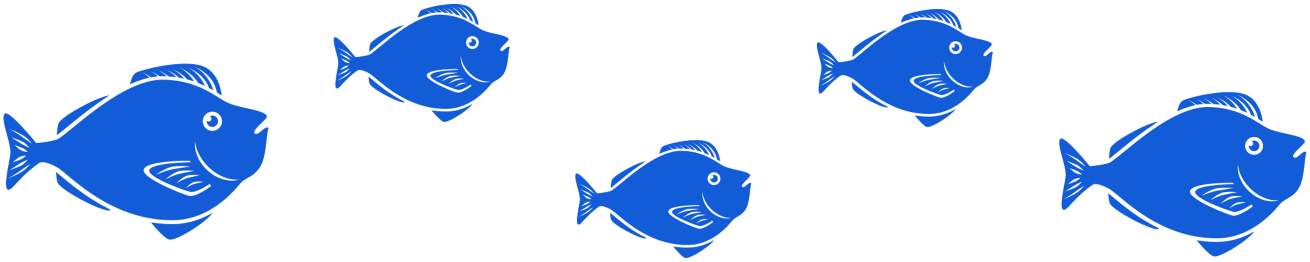
- Limit access to sensitive data and systems to authorized individuals only.
- Create user permissions and role-based access controls prevent unauthorized access.

9 REGULAR SECURITY ASSESSMENTS

- Conduct periodic security assessments and audits to identify vulnerabilities.
- The organization should address weaknesses proactively before attackers exploit them.

10 PARTNER WITH AN EXPERT IT PROVIDER

- If you don't have experienced cybersecurity staff within your organization, partner with a knowledgeable, experienced cybersecurity provider, such as the Digital Investigative group.



THE DIGITAL INVESTIGATIVE GROUP

The **DIGITAL INVESTIGATIVE GROUP**, the DIG, is a Montana-based Managed Cybersecurity Services team. We are experienced, certified, and have access to state-of-the-art security tools. With the DIG, securing your organization is affordable and easy to manage with all your security tools in one place.

We provide cybersecurity services and solutions designed to meet your needs and protect your business

To learn more about the DIG's services, contact us.

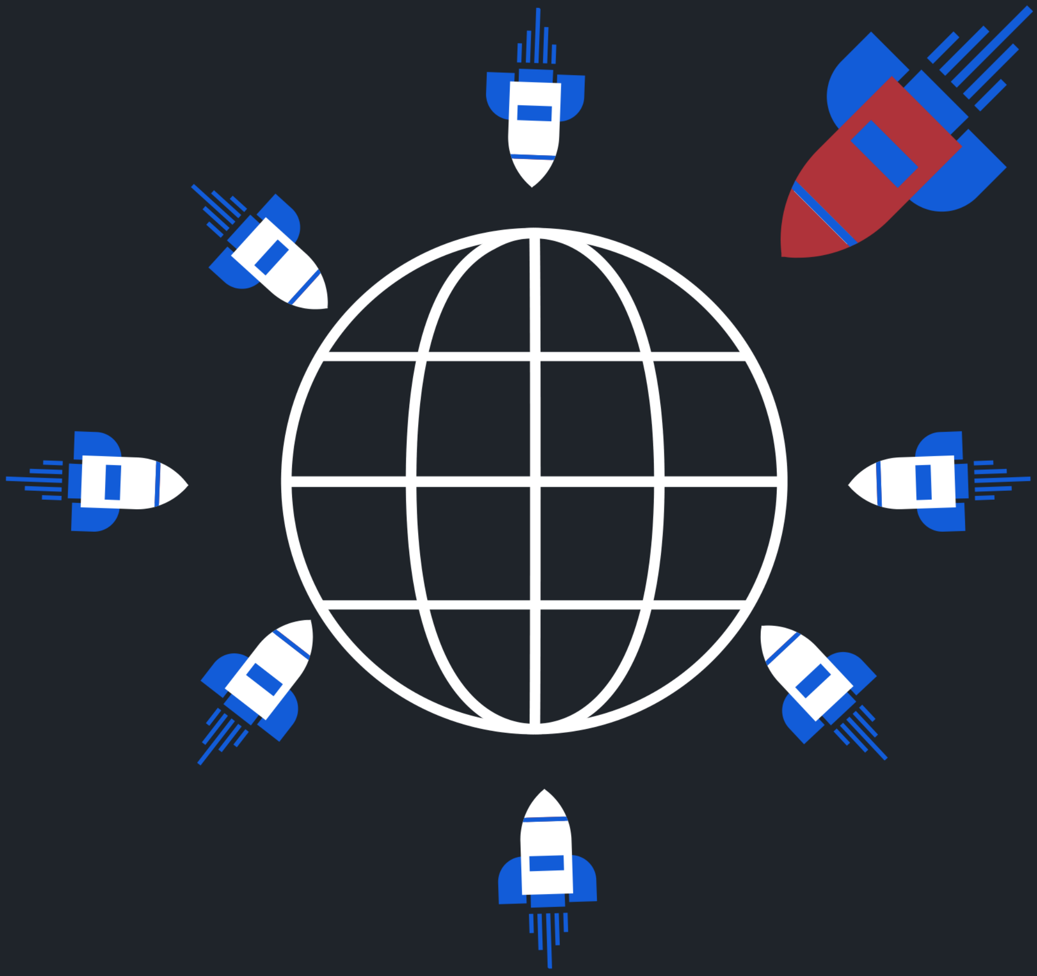
- (866) 293-2344
- ContactUs@thecyberdig.com
- Offices in Helena and Billings

For security tips and information specialized for the Montana IT community, subscribe at thecyberdig.com/blog

SECTION 3!

Remember, cybersecurity is an ongoing battle. To be prepared, you need to regularly review and update your security measures as new threats emerge. By implementing these practices and engaging with a our expert services, you can significantly enhance your organization's resilience against cyberattacks and protect your valuable assets.

To learn more about the DIG and our services, contact us.
Thank you!



ARE YOU READY TO DIG DEEPER?

SCAN ME!

To learn more about our services, scan this QR code.

thecyberdig.com