A Leader's Framework for Cloud Security

DATAHIVE
Proactive SECURE Protection

DATAHIVE
Proactive **SECURE** Protection

The corporate issue is
cloud data security.

DataHiveSecure.ca

Read on for critical information on steps to protect corporate data...

DataHiveSecure.ca

Efficiently Reduce Cloud Attacks

Within three years, close to 100% of all business data will be stored in a public cloud.

Here’s what is happening right now:

- Corporate data is uploaded to a public cloud in various locations
- Your data is connected to apps located in other clouds
- Your apps then connect to other apps in other clouds not known to you
- Now unknown access to corporate data has increased
- Now some apps are connected to your cloud without your knowledge
- Now hackers have unlimited access to any information in the cloud
- Your access to corporate data is 100% insecure

There is wisdom in the development of a Cyber Security Plan

Cyber Security Planning

To become secure, consider establishing an on-going security framework consisting of five steps: identify, protect, detect, respond and recover. This process helps achieve corporate cybersecurity defense, free of gaps and holes from hackers.

A systematic security framework with consistent checks and balances, increases business data security.

DataHiveSecure.ca

The Tough Questions

WHO is the guardian of corporate data?

WHAT is the impact of illegal data intrusion?

WHY is corporate data at risk on the cloud?

WHEN there is no one else to blame - who?

WHERE does the buck stop?

IS IT YOU?

DataHiveSecure.ca

Sixty Percent of World Data is on the Cloud...

...and it is 100% vulnerable. Attackers are now able to find poorly protected assets and access them illegally - bypassing authentication.

The Public Cloud creates challenges due to open connectivity. Security is jeopardized as computing and data management connections are linked to multiple cloud sources.

DataHiveSecure.ca

Where are you in this Security Framework?

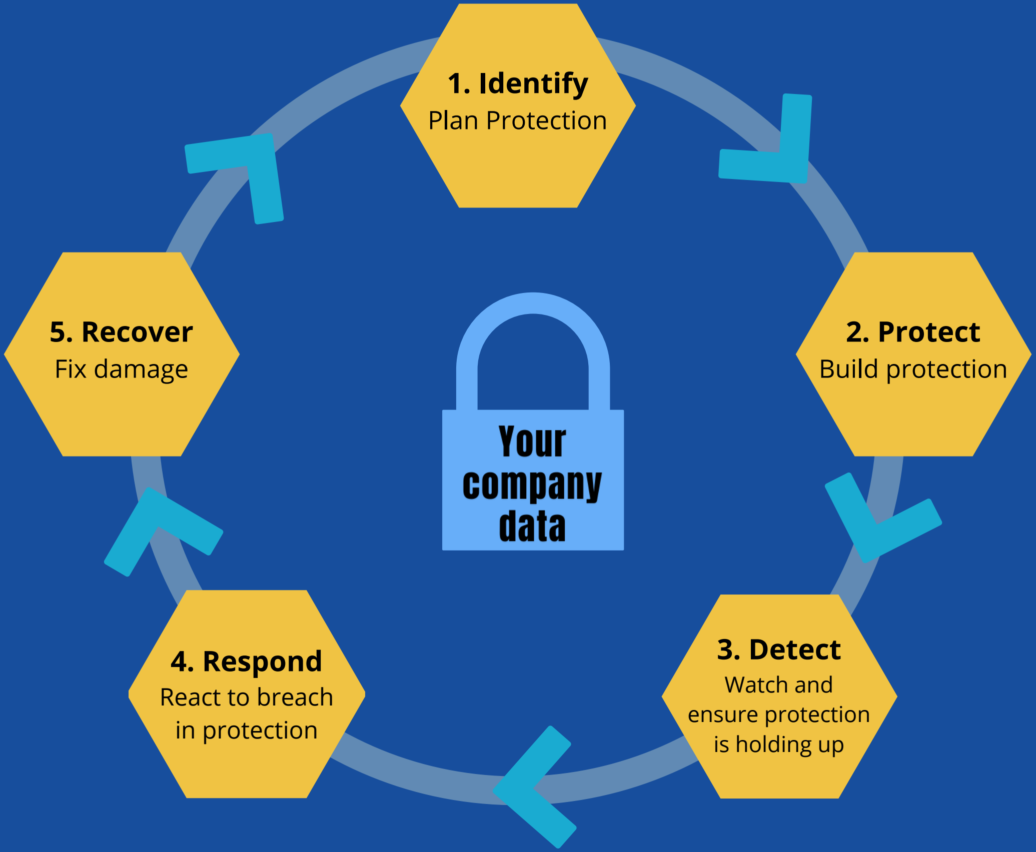
A hacker looks for weaknesses or gaps in every layer of software.

The public cloud increases vulnerability to data breaches.

DataHiveSecure.ca

DataHiveSecure.ca

DataHiveSecure identifies, documents, and recommends solutions for your cybersecurity framework



1. Identify
Plan Protection

2. Protect
Build protection

3. Detect
Watch and ensure protection is holding up

4. Respond
React to breach in protection

5. Recover
Fix damage

Your company data

DataHiveSecure.ca

1. IDENTIFY

Through the identification process of applying industry best practices, we identify vulnerabilities before hackers do.

Learn More

2. PROTECT

One of the smartest ways to protect company data is incorporating a WAF, Endpoint protection, Email filtering, Micro segmentation, and Vulnerability patching.

When your data is moving through the insecure internet - plan ahead.

This helps keeps online traffic safe from prying eyes and tampering.

Learn More

3. DETECT

An emergency breach response plan is essential for every corporation. Rapid detection minimizes damage.

Understanding network traffic patterns and recording details of breaches is crucial in cleaning up, hardening, and preparing for potential future attacks.

DataHiveSecure's remote logging and analysis service will help protect vital data from tampering, during an attack.

Learn More

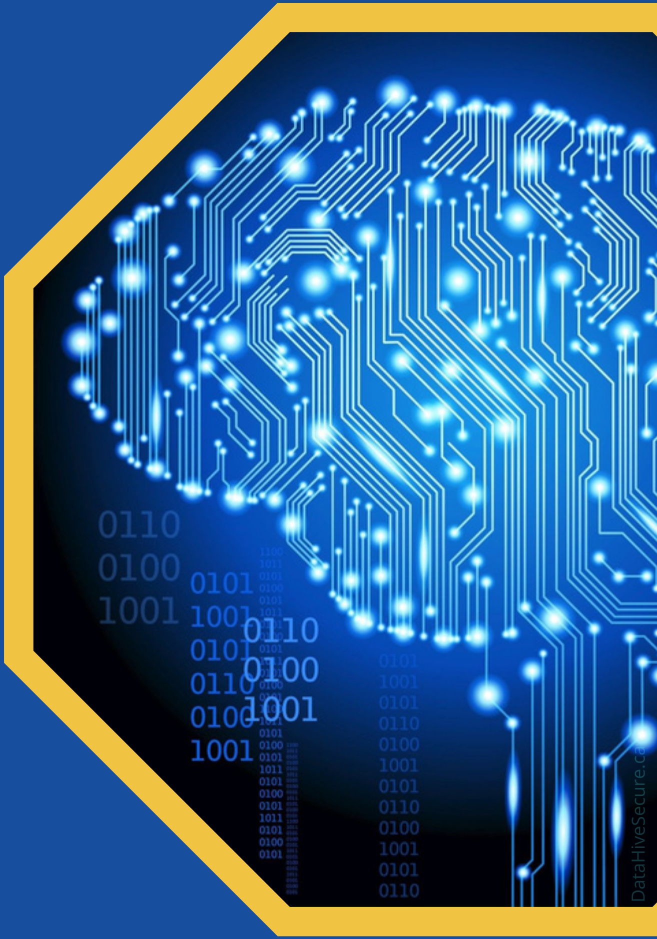
4. RESPOND

An emergency breach response plan is essential.

IT security experts provide an exact understanding of the system's vulnerability status and business needs.

An established mitigation framework facilitates a quick reaction if a breach occurs.

Learn More



5. RECOVER

An up-to-date disaster recovery plan is the first line of defence.

A backup plan is the last and most important layer. By storing duplicate files in a separate location in case of loss, theft, destruction, or ransomware interference, business can continue.

Ask us about our unrelenting secure private cloud storage.

Learn More

DATAHIVE
Proactive **SECURE** Protection

DataHiveSecure, a Calgary company, is approaching its 20th year in the data security business. Its reputation has been built into national and international prominence. Our story is one of highly intense security by employing the best possible staff, including Certified Ethical Hackers who ensure the on-going security of client data.

Security is the company’s day-to-day focus. By working with corporations to identify vulnerabilities, DataHiveSecure helps clients to defend their business against the threats of data compromise and loss.

DataHiveSecure.ca

Visit our Website to get exclusive VIP information to upcoming events:

- Tradeshows
- Speakers
- Demonstrations

DataHiveSecure.ca

Next Steps

You may be particularly interested in how DataHiveSecure would approach your specific data security concern. Some issues may need to be confidential in nature.

DataHiveSecure employs two Certified Ethical Hackers with whom you can meet personally. Their goal is to effectively address potential risk to help secure data before a breach attempt. In this way costly staff time, payouts and business interruptions can be avoided.

Best of all DataHiveSecure is nearby. You will know us personally and can meet with us any time to discuss your specific wishes or concerns.

Contact us

Email: info@datahivesecure.ca
Phone: (403) 313-1106

DataHiveSecure.ca

DATAHIVE
Proactive SECURE Protection

Mailing address:
PO Box 21062 Dominion RPO
665 – 8 Street SW
Calgary, AB T2P 4H5

Company address:
340, 840 – 7th Avenue SW,
Calgary, AB T2P 3G2

Proactive security out performs *reactive*...every time

Thank you for your time