Cyber Security & Insurance Guide

Introduction

In response to the recent increase in cyber-related insurance claims in Canada and across the globe, insurers have tightened their underwriting guidelines focusing on loss prevention and loss mitigation to control costs and now require organizations to maintain certain IT controls as a condition to offering coverage.

There are a variety of factors contributing to the increase in cyber-related claims activity with the primary being the size and quantity of ransomware losses arising from inadequate IT controls.

The IT controls listed below are intended to help reduce the risk of experiencing a ransomware attack and to help the business quickly restore operations if the controls fail. It is important to note that businesses of any size without Multifactor Authentication (MFA) and Offline/ Cloud Back-ups are in most cases deemed uninsurable and are therefore considered critical security controls.

Depending on the business operations, medium and large sized enterprises may be deemed uninsurable for failing to implement some, or all, of the key controls marked as highly important outlined below.

Critical security controls

1

Multifactor Authentication (MFA) privileged accounts/remote access

MFA helps you protect sensitive data and/or access to your network by adding an extra layer of security by making it considerably more difficult for malicious actors to log in as if they were a legitimate user. Any remote access to the network or access to privileged accounts, must be protected in this way.

2

Offline/cloud backups

A backup of critical data and applications must be stored offline or in the cloud and inaccessible from the main network.

Have questions? We have the answers.

Clive Bird 604 817 8072 · clive.bird@axisinsurance.ca
Stacey Copeland 604 619 7775 · stacey.copeland@axisinsurance.ca

Highly important security controls

3

End point detection and response (EDR)

An endpoint is a remote computing device that communicates back and forth with a network to which it is connected. EDR offers continuous monitoring and more advanced detection and automated response capabilities.

4

Privileged access management

Users should be required to use higher security login credentials to access administrator or privileged accounts. These login credentials should be different to the credentials used for day-to-day activities.

5

Email filtering and web security

Technical controls around email accounts and web applications protect internal end users from unintentionally giving access to cyber criminals. This can occur innocently by clicking on the wrong link or opening malicious attachments.

6

Patch management and vulnerability management

A patch management system or policy is designed to highlight, classify and prioritize any missing patches on an asset. Vulnerability management is a process that discovers assets on the network, categorizes the OS and applications on the assets and reports on security vulnerabilities on target systems.

7

Logging and monitoring/network protections

Logging every action of every device within a network is essential for providing a digital record of movements. These logs can then be analyzed pre or post event for abnormalities.

8

End-of-life (EoL) systems replaced and protected

Windows XP and Windows Server 2003 are good examples of systems that have reached their end of life. When updates and patches have stopped being provided, those systems effectively become more vulnerable to security threats. It is vital these EOL systems are removed, or where they can't be, they must be surrounded by enhanced security measures.

9

Wire transfer fraud and phishing attacks: Call-Back Procedures

Wire transfer fraud is a serious threat to individuals and organizations, and it is essential to understand the methods used and the best ways to protect against them. Call-back procedures are an effective way to reduce the risk of falling victim to this type of phishing attack, and by following best practices, individuals and organizations can better protect themselves against these attacks and reduce the risk of sensitive information and funds being lost.

Highly important security controls

10

Network hardening techniques

Hardening techniques, such as disabling certain network protocols and unused or unnecessary network ports, is an area being increasingly examined by underwriters. Particularly, in relation to Microsoft's vulnerable Remote Desktop Protocol (RDP) and whether it is disabled or protected.

11

Cyber incident response planning and testing

Organizations need to develop and implement an Incident Response Plan which includes defined roles, training, management oversight and other measures that will help discover attacks, contain damage, and restore operations more effectively. All senior staff must know what to do, if and when an incident occurs.

1 Multifactor Authentication (MFA)

With MFA implemented, even if a malicious actor had your password, they would still need your second and maybe third "factor" of authentication, such as a security token, your mobile phone, your fingerprint, or your voice to gain access to your network.

As an added benefit, MFA also allows you to clearly distinguish among users of shared accounts, improving your access control.

Why is this critical?

Hackers today have access to technology enabling them to break user passwords of all strength. Users are particularly vulnerable when they reuse passwords across multiple sites, which occurs frequently.

Organisations should bolster their security through MFA which requires at least two pieces of evidence (factors) to prove the user's identity. Usually, the two factors are something you know and something you have. For example, a time-sensitive pin code delivered either through an application or via text message is often the second factor after inputting the user's password. Although no cybersecurity tools are perfect, MFA provides a substantial barrier to entry.

It is essential that businesses protect any remote access to their network with MFA, both for their own employees and vendors. Without it, malicious actor can access the network by simply finding one employee's credentials. Remind users that passwords should be unique to your business systems and should never be shared across other personal accounts.

Privileged/Administrative accounts are also highly valuable. They give the user control of the network and the ability to make changes across the whole business. As such, privileged accounts should be protected with MFA.

2 Offline/cloud backups

Backup intervals will depend on how often the data changes, but most organizations run periodic full backups weekly or multiple times per month, with more regular incremental backups daily or every few days.

It is essential to logically separate backups from the main network to ensure they're not accessible to any threat actors – often underwriters ask that copies are therefore stored offline or in cloud storage.

Immutable backups, which lock up previous versions of your backup to prevent it from being altered or deleted, offer a similar layer of security.

The IT/IS department should also establish a data restoration testing schedule during which backups are restored to accounts, improving your access control.

Why is this critical?

Increased ransomware activity underscores the need for organisations to have a robust backup strategy for their critical data and applications. Backing up data is one of the best practices for information security that has gained increased relevance in recent years. With the advent of ransomware, having a full and current backup of all your data can be a lifesaver.

Without a back up, organisations are often left with no option but to pay demands to attackers that can hold all their data and applications for ransom. The process of backing up data is pivotal to a successful disaster recovery plan.

Check are you following the 3-2-1 rule – 3 copies, on 2 separate systems, with 1 being 'offline'

3 Endpoint detection and response (EDR)

EDR offers continuous monitoring and more advanced detection and automated response capabilities. The monitoring software will watch for any suspicious or irregular activities on any endpoints. EDR also facilitates rapid incident response across an organization's environment which often stops suspicious activity until it can be inspected. Examples of endpoints include, desktops, laptops, smartphones, tablets, servers, workstations, Internet-of-things (IoT) devices. Ensure that you have anti-virus installed and signatures are kept up to date .

Why is this important?

Endpoints represent key vulnerable points of entry for cybercriminals. Endpoints are where attackers execute code and exploit vulnerabilities, as well as where there are assets to be encrypted, exfiltrated or leveraged.

With organizational workforces becoming more mobile and users connecting to internal resources from off-premises endpoints all over the world, endpoints are increasingly susceptible to cyberattacks.

4 Privileged access management (PAM)

Special users such as IT, network, or database administrators — should only be allowed to carry out specific tasks through their privileged access. Users with privileged or administrator accounts should be required to log out of their privileged accounts to conduct any nonprivileged, day-to-day tasks. That means that a system administrator that logged in through their privileged account to change security settings should log out after that task is completed and be required to use 'standard user' credentials to check email or browse the web, even if these are work-related tasks.

Many organizations implement privileged access management solutions to automate privileged credential management and session management.

A much better solution is to use the principle of least privilege. In other words, assign each new account the fewest privileges possible and escalate privileges if necessary. And when access to sensitive data is no longer needed, all corresponding privileges should be immediately revoked.

Check that old accounts have been disabled, particularly privileged account. Constant privilege management can be difficult and time-consuming, especially for large companies, but there are a lot of access management solutions on the market that can make it easier.

The zero trust practice says to grant access only to those users and devices that have already been authenticated and verified in the system.

Why is this important?

The misuse of administrative privileges is a primary method for attackers to spread inside an enterprise. To gain administrative credentials, they can use phishing techniques, crack or guess the password for an administrative user, or elevate the privileges of a normal user account into an administrative account. If organizations do not have resources to monitor what's going on in their IT environments, it is easier for attackers to gain full control of their systems. Granting new employees all privileges by default allows them to access sensitive data even if they don't necessarily need to. Such an approach increases the risk of insider threats and allows hackers to get access to sensitive data as soon as any of your employee accounts are compromised.

Physical controls should also be employed wherever important information resides. A company laptop or a smartphone, for instance, should not be left unattended in a vehicle. Enable auto-lock function on any devised used for business purposes.

5 Email filtering and web security

Security tools can screen links and attachments to identify any potential malware or other malicious content. Flagged attachments can be opened in a "sandbox" to be thoroughly checked for malware.

Organizations should block access to any web pages that are deemed inappropriate and those that may contain malware. It is also essential to ensure that your company website is configured and maintained in a secure manner so that any personal data is appropriately protected.

Why is this important?

Malicious actors can create content and spoof users into taking actions that can introduce malicious code and lead to loss of valuable data or access to the network. Phishing attacks are becoming more complex. Even with security awareness training, employees can still be fooled into clicking a malicious link or downloading a virus.

Content filtering can help combat this by blocking access to content that is deemed risky. Web filtering means that employees won't be able to download restricted, offensive, or illegal content. This can reduce the threat of an outside data breach. It also means organizations can be protected against regulatory violations, associated fines, and embarrassment.

6 Patch management and vulnerability management

Patch management tools or policies can be used to manage the update of software, operating systems and applications on an asset in a logical manner. Organizations need to continuously acquire, assess and take action on new information (e.g. software updates, patches, security advisories and threat bulletins) to identify and remediate vulnerabilities attackers could otherwise use to penetrate their networks.

Why is this important?

As soon as researchers report new vulnerabilities, a race starts among all relevant parties: Culprits strive to use the vulnerability for an attack, vendors deploy patches or updates, and defenders start performing risk assessments or regression testing. Attackers have access to the same information as everyone else and can take advantage of gaps between the appearance of new knowledge and remediation.

Check that your business has a comprehensive inventory of assets, particularly of internet facing applications. Turn on automatic updates whenever possible and Identify software and hardware that requires manual updates taking into account mobile and IoT Devices

7 Logging and monitoring/network protections

Log monitoring is the action of categorising actions and searching the data for abnormalities that might cause problems with the system. Abnormalities could include error codes, login difficulties, or potential threats from outside parties. Organizations need to collect, manage and analyze event logs to detect aberrant activities and investigate security incidents.

An effective monitoring system collects the data from logs and categorizes them into easily digestible information. This information is translated into the preferred format of the IT team responsible for overseeing the logs. It is becoming increasingly essential to have a 24/7 Security Operations Centre, whether internal or external, to monitor and respond to these abnormalities/threats.

Why is this important?

A lack of security logging and analysis enables attackers to hide their location and activities in the network. Even if the victim organization knows which systems have been compromised, without complete logging records, it will be difficult for them to understand what an attacker has done so far and respond effectively to the security incident. Log or infosec monitoring categorizes all actions that occur within the system. As the system learns which activities are normal, it's able to weed out the data that reveals potential threats within an organization's network.

Real-time identification of these threats combined with an effective alert system provides you with a way to detect and interrupt potential threats more quickly. Events occur and you can count on them to disrupt files and cause downtime. It's no secret that prolonged downtime is the enemy of good business. Log event files can help clarify what happened and recover essential files and reconstruction of corrupted files can be completed more quickly by reversing the changes noted in the logs.

Have questions? We have the answers.

Clive Bird 604 817 8072 · clive.bird@axisinsurance.ca
Stacey Copeland 604 619 7775 · stacey.copeland@axisinsurance.ca

8 End-of-life (EoL) systems - replace or protect

Software developers continuously release patches to offer bug fixes, improvements and patch recently discovered security vulnerabilities. This practice cannot continue indefinitely as each new version of their software has its own security challenges.

Microsoft, for example, no longer provides patches for Windows 7 or older versions of their operating system– even some versions of Windows 10 are already not being supported. Once manufacturers cease providing patches for software they are considered “End-of-life” systems.

Why is this important?

Over time, the number of discovered vulnerabilities in these EoL systems will grow, but no patch or solution will be provided to defend them.

End-of-life systems therefore create a weak point in an organization’s network which can be exploited. For this reason, an organization should replace their systems as soon as possible and should aim not to run any EoL systems. If EoL systems cannot be replaced, then additional protection is required to mitigate the risk.

A firewall and anti-virus are not sufficient protection against unpatched vulnerabilities, which hackers are quick to exploit. EoL systems should be segregated from the rest of the network and should not handle critical or sensitive information.

9 Wire transfer fraud and phishing attacks: Call-Back Procedures

Wire transfer fraud is a type of phishing attack that involves tricking individuals or organizations into sending money to a false account. This type of attack is becoming increasingly prevalent as attackers become more sophisticated in their tactics, making it essential to understand the methods used and the best ways to protect against them.

Types of Phishing Attacks Related to Wire Transfer Fraud:

1. **Business Email Compromise (BEC):** In this form of phishing, the attacker hacks into a company's email account or creates a fake email account that closely resembles a legitimate one, and sends an email that appears to be from a trusted source, such as a CEO or a vendor, requesting a wire transfer to a false account.
2. **Invoice Phishing:** In this type of phishing, the attacker sends an invoice that appears to be from a trusted vendor or supplier, asking the recipient to wire transfer payment to a false account.

Call-back procedures are an important component of protecting against wire transfer fraud. By verifying the identity of the person requesting the wire transfer and checking the information provided, individuals and organizations can reduce the risk of falling victim to this type of phishing attack. Some best practices for call-back procedures include:

1. **Verify the Requestor's Identity:** Before making any wire transfers, the individual or organization should verify the identity of the requestor and check that the request is legitimate.
1. **Check the Account Information:** The individual or organization should verify that the account information provided is accurate and corresponds to the legitimate account of the vendor or supplier.
1. **Call the Requestor:** If there is any doubt about the legitimacy of the request, the individual or organization should call the requestor using a known phone number to confirm the details of the wire transfer.
1. **Do Not Provide Sensitive Information:** The individual or organization should never provide sensitive information, such as account numbers or passwords, over the phone unless they have verified the identity of the requestor.

Why is this important?

Wire transfer fraud is a serious threat to individuals and organizations, and it is essential to understand the methods used and the best ways to protect against them.

Call-back procedures are an effective way to reduce the risk of falling victim to this type of phishing attack, and by following best practices, individuals and organizations can better protect themselves against these attacks and reduce the risk of sensitive information and funds being lost.

10 Network Hardening techniques, including remote desktop protocol (RDP) mitigation

Network Hardening refers to techniques such as properly configuring and securing network firewalls, auditing network rules and network access privileges, disabling certain network protocols and unused or unnecessary network ports, encrypting network traffic and disabling network services or devices that are not in use.

These techniques can sometimes be an afterthought for businesses, but regularly reviewing and amending these settings and controls can reduce the network's overall attack surface and limit the number of things that can go wrong.

Businesses can follow recognized industry standards and guidelines, such as the National Institute of Standards and Technology (NIST) framework, which provides best practice guides for network and system hardening.

Why is this important?

Poorly configured firewalls and network settings can either affect an organization's business operations, by being too strict, or give malicious actors more opportunity to successfully attack a network, by being too lenient.

It is essential these settings are reviewed and amended to get the best protection from these controls.

Not disabling certain network protocols that are unused or unnecessary is a particularly bad practice that cyber underwriters examine closely. The Microsoft Remote Desktop Protocol (RDP) is often asked about specifically as it is susceptible to a variety of security breaches – most notably BlueKeep which can allow an attacker to remotely access Windows systems without having to provide a username or password.

First consider whether or not remote access capabilities are actually needed for various machines on a network, if not, the RDP port can be disabled and all associated security threats can be eliminated.

If it is needed, then additional authentication methods can be used to identify a user before they can start an RDP session.

Have questions? We have the answers.

Clive Bird 604 817 8072 · clive.bird@axisinsurance.ca
Stacey Copeland 604 619 7775 · stacey.copeland@axisinsurance.ca

11 Cyber incident response planning and testing

Cyber Incident Response Planning is the process of creating and implementing a plan to manage the response following a cyber event. The plan should identify threats and controls that can be implemented to minimize the probability of experiencing a cyber event. In addition, the plan should include steps to restore business operations as quickly as possible to minimize downtime in the event the controls fail. To respond quickly to security threats, investigate tools that could monitor and create alerts when suspicious activity or security breaches are occurring.

Why is this important?

Planning is important because it helps to protect the business from the potentially devastating effects of a cyber-attack or other IT disruption, such as lost revenue, damage to the company's reputation, and loss of customer trust.

By having a plan in place, businesses can minimize the impact of a disruption and quickly resume normal operations, which can help to protect the company's bottom line and maintain customer confidence.

How Axis Can Help You

When developing an application for underwriting consideration, a professional insurance broker will assess your IT security posture and make recommendations on which controls will improve your risk profile. This will enable your broker to negotiate the most favorable coverage terms and the best pricing.

We consult with you to understand your needs and can recommend vendors within our network of cyber security service providers to help you implement controls tailored to your requirements.

Have questions? We have the answers.

Clive Bird 604 817 8072 · clive.bird@axisinsurance.ca
Stacey Copeland 604 619 7775 · stacey.copeland@axisinsurance.ca

This material is for general information only and should not be considered as a substitute for legal, medical, tax and/or actuarial advice. Contact the appropriate professional counsel for such matters. These materials are not exhaustive and are subject to possible changes in applicable laws, rules, and regulations and their interpretations.

This paper was written in collaboration with
BMS Group Ltd

Next Step?

Let's engage in dynamic discussion around the factors and variables that are unique to your business so we can obtain the best product, from reliable and stable insurers to meet your needs.

Axis Insurance Managers
#400 - 555 Burrard Street Box 275
Vancouver, British Columbia
Canada V7X 1M8

Clive Bird 604 817 8072 · clive.bird@axisinsurance.ca
Stacey Copeland 604 619 7775 · stacey.copeland@axisinsurance.ca

Mining Team

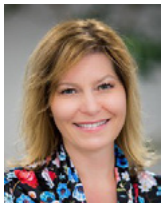
Clive Bird

Clive is an insurance risk specialist, investor, entrepreneur, and product developer for bespoke insurance risks. For over 15 years Axis Insurance enjoyed a reputation for quality, innovation, creativity and relationship building.

Clive began his Insurance career at Lloyd's of London, renowned for its technical underwriting expertise and a creative approach to risk, providing him with opportunities to push the boundaries of product innovation. Moving to the West Coast of Canada, he has expanded his broad Insurance knowledge and London market relationships to produce products for Canadian clients working across the globe.

Clive has worked extensively with public companies with a strong focus on mining and mineral exploration industry, addressing the broad range of risk exposures they face worldwide. Dynamic business enterprises are starved for the innovation and market relationships Clive can deliver. As an entrepreneurially-minded investor himself, he is embracing new technology and the shifting business landscape to stimulate new market capacity and technically efficient insurance products for the new business era.

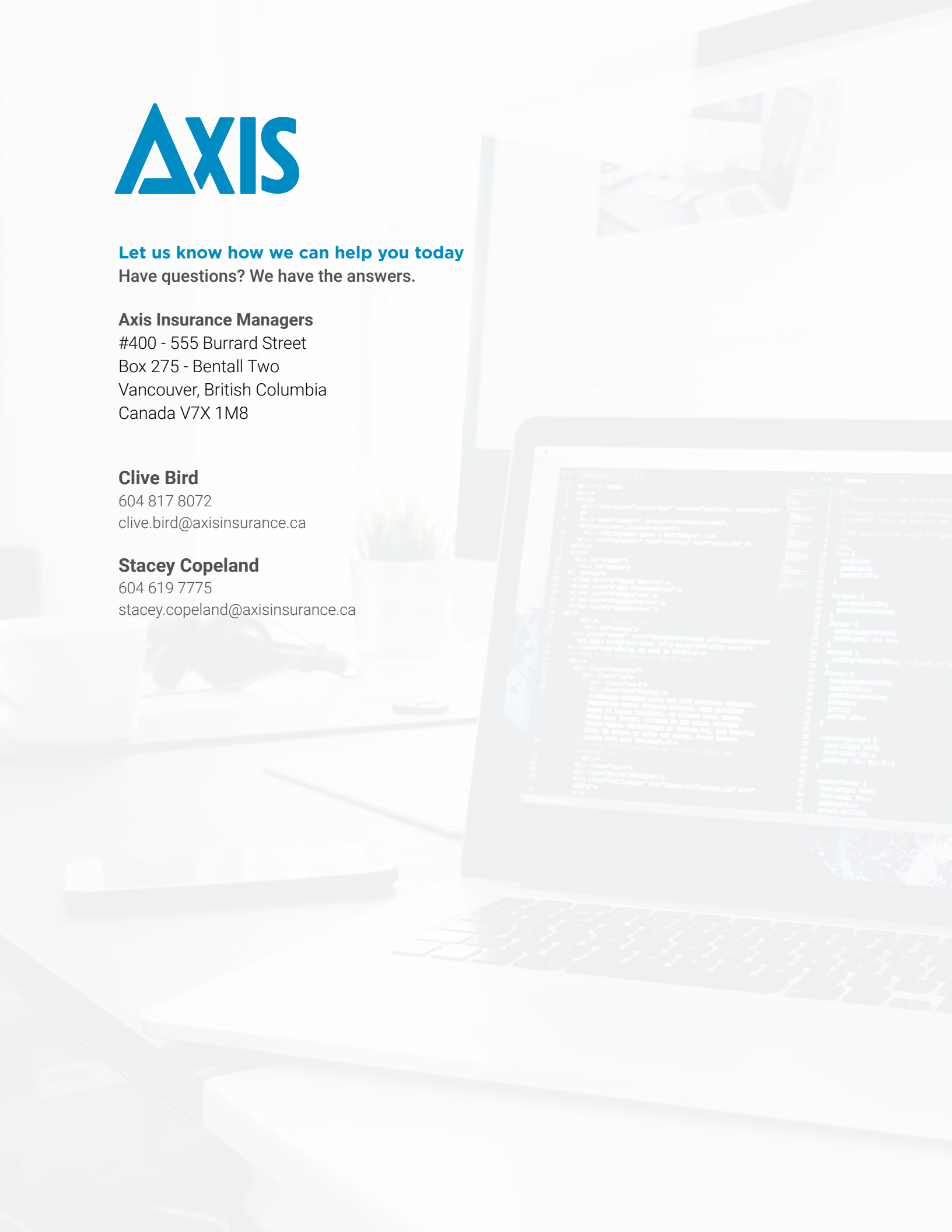
Stacey Copeland



Stacey is an account executive with 30 years of experience focused in the resource-based industry in Western Canada. Stacey joined Finning International in 1997 after 7 years at AON, and was quickly promoted to a management position with a mandate to build a highly competitive insurance facility for Finning customers. A combination of high service excellence, successful claims management, and expanded insurance offering meant a fivefold increase in net profitability.

Stacey joined Axis Insurance in 2005 as a senior shareholder and partner, immediately helping the company grow through a series of strategic acquisitions and partnerships and was instrumental in the sale of the company in 2016 to the Vertical Group, now renamed the Axis Group. Although specializing in mining, mineral exploration, forestry and energy sectors, Stacey has expanded her knowledge to include construction, transportation, cryptocurrencies, blockchain and other emerging markets and technology risks.

She aligns herself with clients that are best in class and embraces their technical challenges, meets their high service expectations and considers it the ultimate success to place the broadest coverage, at competitive pricing with A+ rated insurers.



Let us know how we can help you today

Have questions? We have the answers.

Axis Insurance Managers
#400 - 555 Burrard Street
Box 275 - Bentall Two
Vancouver, British Columbia
Canada V7X 1M8

Clive Bird
604 817 8072
clive.bird@axisinsurance.ca

Stacey Copeland
604 619 7775
stacey.copeland@axisinsurance.ca