CORAGGIO
FEARLESS OBJECTIVE ADVICE

CYBER SECURITY – HOW TO ESTABLISH, PREPARE AND MITIGATE CYBER ATTACKS TO MINIMISE RISK

Ebook

coraggio.com.au

CONTENTS

Is Cyber Security a ticking time bomb

The COVID-19 pandemic significantly changed the cyber threat landscape. Work-from-anywhere has become the new norm with 92% of global organisations adopting new technologies to facilitate the switch to remote operations. While this has created plenty of new opportunities for vendors, it highlights numerous security and privacy risks associated with remote work.

We are living in a digital age and whilst this means the cost of communicating with loved ones and work teams has become almost negligible, it also means the cost of digital has escalated and cyber attack vulnerabilities are a ticking time bomb . This combined with the large profits of cyber crime, the wealth disparity between countries and continuing acts of more sophisticated cyber warfare, equates to cyber attacks are on the rise and constantly evolving.

Most businesses and services are switching primarily to online operations and those companies already online had to expand, introducing entirely new processes into their workflows. This rapid shift opened companies up to cyber threats on a larger scale than ever before.

Cyber attacks are rising and everyone is vulnerable. One in three Australians are expected to be impacted by a cyber attack. We need to take more responsibility of our employees personal phones, computers and networks – home and work to ensure all devices are up to date and secure.

As a result, cyber threats are a massive hazard and with the increase in artificial intelligence (AI) and automation, cyber attacks are easier to carry out. Effective corporate cyber security is an issue many businesses are facing today and there can be a lot of risk involved not having a comprehensive strategy for protecting customers' information. Protection has never been more critical.

In fact, in 2021, a staggering 37% of global companies were attacked by cyber criminals at least once per day and in Australia every year there are thousands of cyber breaches which mostly affect smaller businesses, however occasionally "major" cyber breaches impact larger businesses affecting a significant number of consumers.

Over 1,000 had sensitive data stolen and publicly leaked by ransomware gangs. Even if we return to offices, it seems clear that digital operations will remain far more prevalent than in previous years. With data at the core of every business with remote access and collaboration tools increasingly necessary, it's clear that information technology (IT) services are no longer optional.

Understanding the cyber threat landscape is key to staying safe online as it is not going away unless companies take the necessary steps to protect themselves against cyber attacks and will continue to force business closures.

A fake Zoom invite forced Levitas Capital, a Sydney hedge fund to close up shop, sinking their $16 million super fund investment after cyber criminals found a way into their emails. Non-law enforcement agencies have been able to ask for access to your data under an Australian law meant to thwart terrorists.

In response, Australia's telco operators are calling on the government to close a loophole in controversial metadata retention laws that have allowed non-law enforcement agencies to request data information.

"Closing this dangerous loophole – under which Australians can have their personal data exposed without their knowledge and without a warrant as part of investigations into crimes such as littering – is a vital security fix the Government must act on,"
telco peak body Communications Alliance's CEO John Stanton said.

A section in the Telecommunications Act has allowed state-based, non-law enforcement agencies to access metadata that telcos are required to retain for two years.

The most common and fastest growing global cyber crime right now – and probably the most successful tactic that is currently employed, especially for hedge funds, is called BEC. This tactic continues to be tried all around the world – especially in areas of high dollar concentration. It is when an attacker sends a fake email to the finance department or someone with account access. That email looks confusingly similar to a genuine email and the domain name may have an extra letter in it, or it may be sent from a compromised personal email account of the CEO or CFO.

Once the attackers have a foothold in the company, they can send the email as the real individual because they've compromised the email system. As in the case of Levitas, the attackers proceed to email the recipient a fake invoice to an account number where money should not go or change the account number on a legitimate invoice.

Other governmental agencies and industry experts that they are attractive targets for cyber criminals, many managers still have not devoted sufficient time and resources to building effective cybersecurity programs.

Another way to think about it - if there is a bank vault which has no lock and lots of money which can be accessed almost instantly from around the world, do you think people will try and steal the money? Businesses which don't have sufficient cyber protections are like that unlocked bank vault, waiting for a cyber attacker to test out their security.

Therefore every business is effectively making the decision to either wait for a cyber attack to happen and react to it, or proactively invest in their cyber security protection to defend against it. The clock is already ticking.

Coraggio Member, Martin Boyd from Vertex Cyber Security shares,
"Now is a great time to start thinking about improving your Cyber Security but choosing who to talk to or where to start can feel daunting. We recommend having a conversation with a good Cyber company like Vertex to understand your options and figure out the most appropriate next step for your business. This is because Cyber Security can be confusing with options such as Penetration Testing (Ethical Hacking to find your vulnerabilities), ISO27001 certification, Cyber Security Audits, Cyber Security Policies, Firewalls, AntiVirus, Managed Cyber Security, Cyber Training, Cyber Security Products and the list goes on."

Impact of Cyber Security Attacks - Case Studies

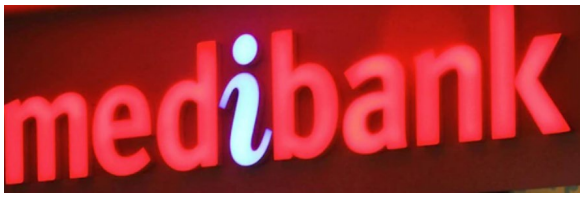
Cyber criminals do not have to win many attacks – if they try 20 and only one of them pays off, it's potentially still a couple million dollars. These criminals used to attack bank accounts and divert the money or look for large amounts of personal information they could steal. However, they are becoming more sophisticated and realised the most lucrative ways to monetize an attack by using ransomware which Wikipedia describes as *a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid*. Ransomware is responsible for 41% of all cyber insurance claims.

When a hacker gains access to your systems, they don't strike straight away, they bide their time and wait for the right moment by watching for your weaknesses, investigate your database and work out how best to maximise their profit including extortion and causing reputational damage to convert to a financial gain.

In many cases the cybercriminals are from other countries, which means we need international co-operation to track them down.

Millions of Australians have had their privacy breached in recent cyber attacks against Optus, Medibank and other companies when cybercriminals stole sensitive health and financial data that can be used for ransom, blackmail or fraud.

In September 2022, a hacker demanded that Optus pay them US$1 million ransom, or they would leak the data of all 11 million customers affected by the breach, however Optus did not respond to the ransom demand causing immense reputational company damage.



Following this cyber breach compromising customer information Optus immediately shut down the attack and commenced working with the Australian Cyber Security Centre to mitigate any risks to customers. Optus also notified the Australian Federal Police, the Office of the Australian Information Commissioner and key regulators. Optus set aside A$140m for the costs of the Cyber Attack. This does not include the reputational and loss of sales impacts.

Information which may have been exposed includes customers' names, dates of birth, phone numbers, email addresses, and, for a subset of customers, addresses, ID document numbers such as driver's licence or passport numbers. Payment details and account passwords have not been compromised.

The Department of Foreign Affairs and Trade says about 100,000 passport numbers were released in the Optus breach.

One quick way to turn these data into money is to use them to apply for credit cards. Many credit card providers, eager for new customers, have very simple and streamlined processes to check identity.

Alongside stolen data such as a name, address and driver's licence details, cybercriminals will need an email address, a phone number and payslips. Phone numbers and email addresses used for communication and authentication are easy enough to provide, and fake payslips generated.

"We are devastated to discover that we have been subject to a cyberattack that has resulted in the disclosure of our customers' personal information to someone who shouldn't see it," said Kelly Bayer Rosmarin, Optus CEO.

Another example, involves attackers with the ability to mimic the voice of an executive using deepfake audio, and machine learning or artificial intelligence will soon be able to write emails that look like they're coming from whomever the attackers want.

According to *Acronis Cyber Protect Cloud* the following are examples of high-profiled ransomware and cyber attacks in 2021.

On July 18, **Telecom Argentina** — the country's largest telecommunications provider — was hit by a ransomware attack that encrypted over 18,000 systems, including terminals with highly-sensitive data. The infamous Sodinokibi group demanded an initial ransom of $7.5 million, set to double if not paid within 48 hours.

Only a week later, **Garmin** — one of the world's largest wearable device companies — began experiencing a major outage of services and production. Garmin later confirmed this was the result of a WastedLocker ransomware attack. The cyber criminals are believed to have demanded a $10 million ransom, which Garmin reportedly paid — although the company has not publicly verified this.

Canon, the multinational firm specializing in optical and imaging products, fell victim to the Maze ransomware in August. Many of the company's internal systems were impacted, as was their U.S. website. The Maze operators appear to have stolen over 10 TB of data, including the Social Security numbers and financial account details of thousands of current and former Canon employees.

Cyber criminals have taken tried-and-true cyber threats, such as phishing campaigns and malicious email attachments and themed them during the pandemic. By exploiting anxieties and a general sense of urgency, such attacks often succeed in getting victims seeking answers and assistance. Data recovery is worth millions of dollars to many companies.

Coraggio, CEO, Richard Skarzynski cites,

"Regardless of the industry sector, data is increasingly at the forefront of business operations. Decisions made regarding taking proactive measures, may directly impact financial and reputational damage if companies do not mitigate their risk."

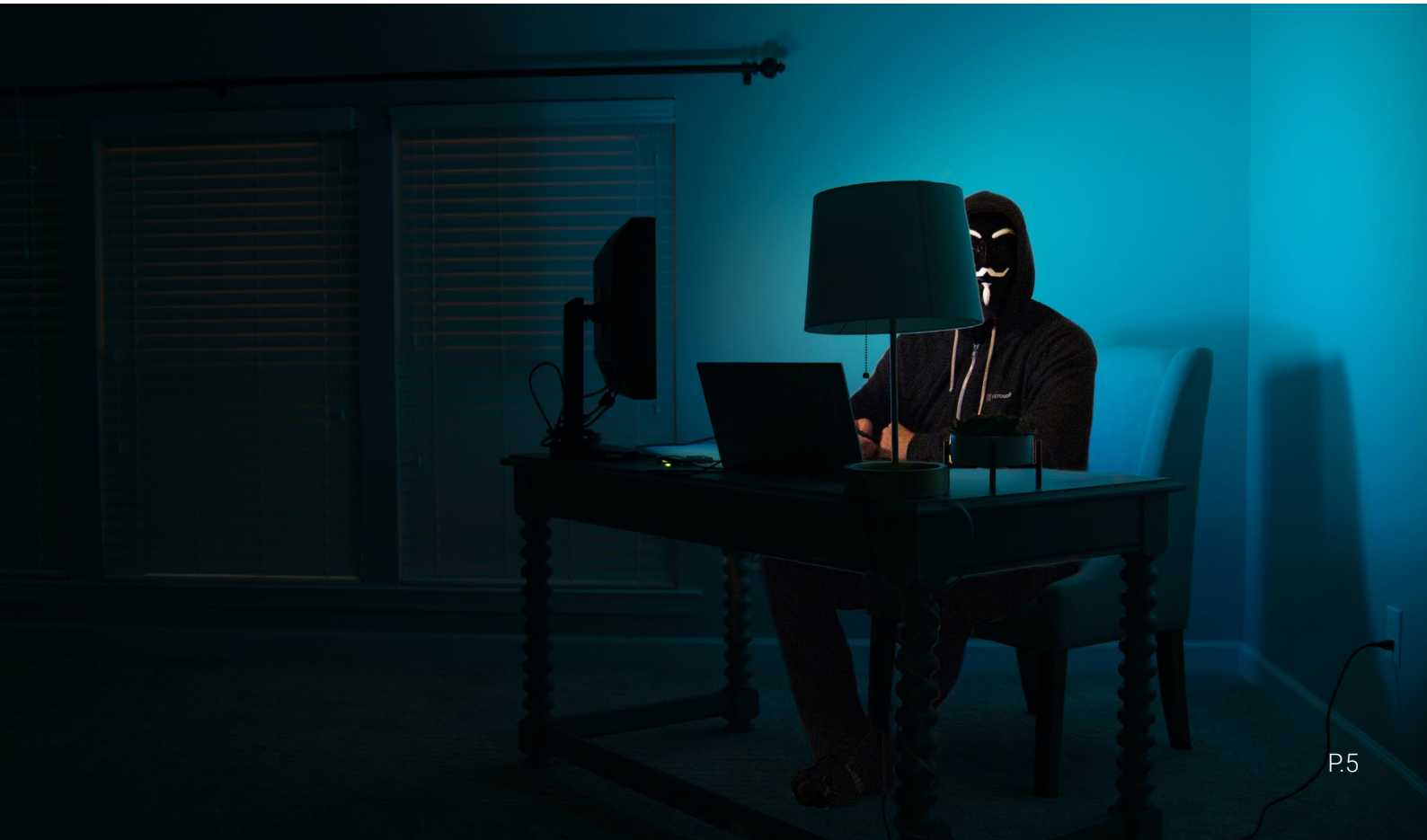
Steps to protect your business and mitigate risk

In regards to ransomware, data exfiltration is poised to become bigger than encryption, as cyber criminals strive to maximise success rates and monetize every attack. Strikes against cloud services will only grow alongside the services' own popularity, taking advantage of improper configurations and weaknesses in the supply chain.

It's likely we will continue to see huge increases in the volume and variety of more traditional cyber threats. Advances in automation and data mining allow cyber criminals to rapidly create and iterate new malware variants, using data from corporate websites and social media profiles to personalise each attack.

What should business owners prioritise in the absence of a specific need?
We recommend these steps to protect against the leading cyber risk, phishing.

Five steps to protect your business from a Phishing Attack
1. Teach your employees to be Cyber Safe and prepared for phishing attacks by performing regular **refresher training**
2. Setup browser **phishing protection** such as XSurfLog, to detect and protect against phishing links
3. Setup a password manager to ensure only **secure passwords** are used
4. Setup advanced **email filtering** to reduce the amount of phishing emails and
5. Setup **Two-Factor Authentication** across your organisation.



Other measures to protect your business

Check for open RDP links (Remote Desktop Protocol)

It's Microsoft technology that allows a local computer to connect to and control a remote PC over a network or the internet. RDP links left open to the internet are a very common route for cyber criminals to enter your network. Scan for open RDP ports regularly and utilise multi-factor authentication for your links (multi-factor authentication is where you generate a code on a separate device to prove it's really you). Or have them behind a VPN (Virtual Private Network), which gives you a private network from a public internet connection.

Keep an eye out for unexpected software

Often, cyber criminals will take control of just one PC first, perhaps using a phishing email to persuade someone to click on a bad link without realising it. Once they have control of one PC, they can then target the entire network.

Monitor your admin

What's the best way for hackers to download the applications they need? They create a new administrator account for themselves. Then they can download whichever tools they need to compromise your network. You need to be aware of software such as Process Hacker, IOBit Uninstaller, GMER and PCHunter. These are all legitimate tools which could be used by any IT specialist.

Check out any disabled tools and software

You can tell that an attack is close to being launched if Active Directory and your domain controllers are disabled. Next, any backup data the criminals have found will be corrupted. And any systems that automatically deploy software will also be disabled, to stop your attempts to update your computers after an attack. Something called PowerShell will then be used to spread everything across your network.

Martin Boyd offers his expertise

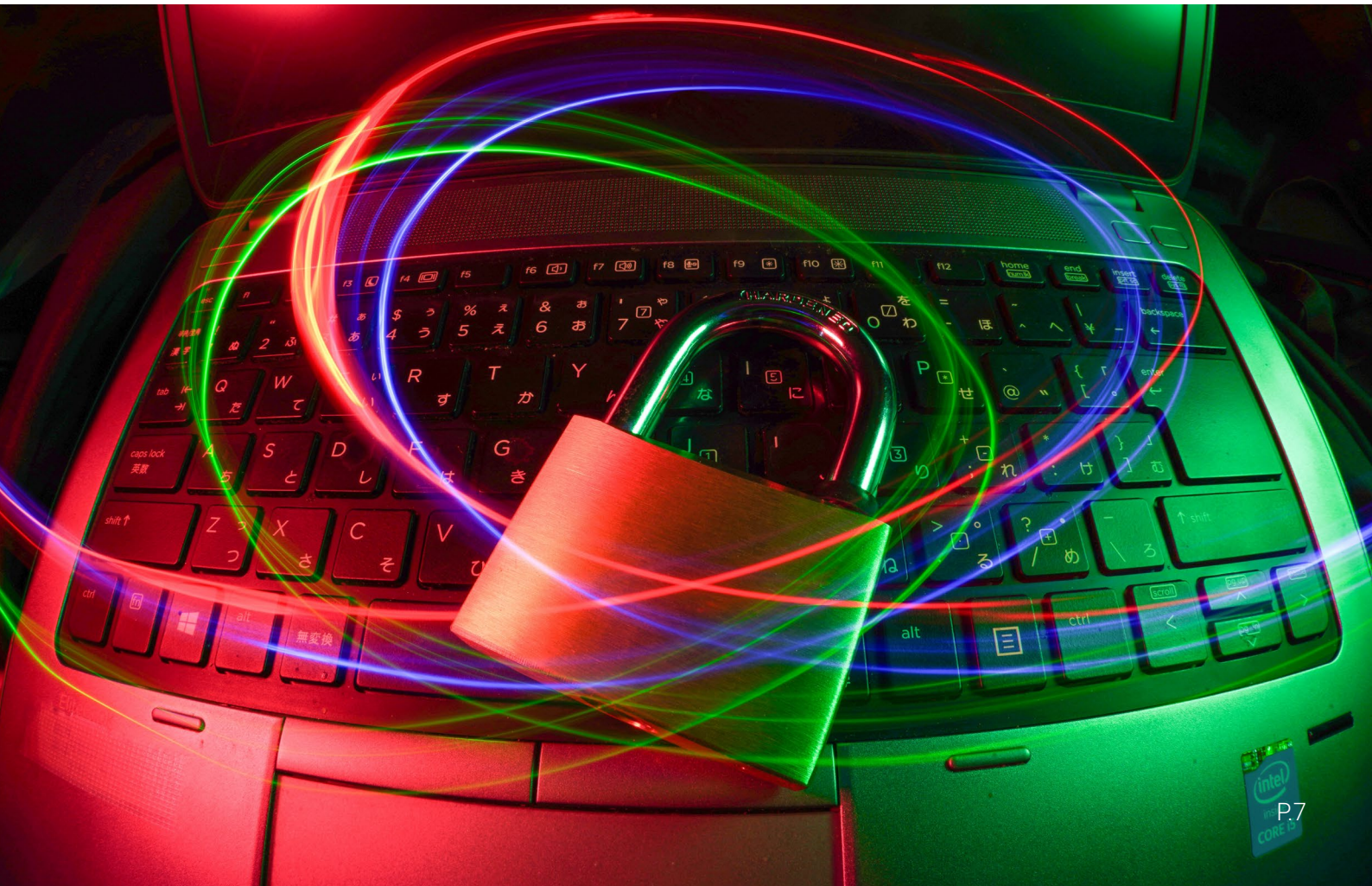
"Vertex can assist you to determine where to start and what to prioritise and in the absence of a specific immediate need, we would suggest taking steps to protect against the number one cyber risk, phishing. If you want an easy way to implement these then feel free to contact Vertex which have built a platform specifically for this purpose which can be quickly and seamlessly set up, easily managed and very affordable.""

Vertex are providing 3 months free using the coupon "**CORAGGIOCYBER**" at https://auth.vertexcybersecurity.com.au/signup/

Vertex Cyber Security
If we can penetrate your systems and data...
Imagine who else can.

Martin adds,

"Cyber Insurance is also worth discussing, however it is a reimbursement and not a protection. We still strongly recommend every business should invest in cyber insurance with their cyber protection. In the event of a cyber incident insurance may help reduce the financial impact, however ultimately it cannot undo the consequences of a cyber incident, such as company reputational fall out."



Types of cyber security solutions

It takes a long time to build trust and to have clients think about your brand positively. A breach in security can cause issues with both your customers and people within your company. By looking into which measures you can take, you can help to protect your business' files and data, including:

AntiVirus / AntiMalware

Detects and blocks some (30%) virus/malware/ransomware before it executes. It is recommended to get it with monitoring to review new software to detect new malware not typically detected immediately.

Firewalls

Every computer should have a firewall. Many devices come with one already installed however it may not be enough to protect you from hacking your corporate accounts. It's worth investing a bit more than you would for your personal account, for example, because you are responsible of others' data.

There are a number of firewall options created for businesses. These can help destroy viruses or malware that could compromise your security.

The network is used for Cyber Attacks, so the firewall can block some of the connections. Ensuring it is enabled on all computers is essential. Some office firewalls can reviewing incoming network connections and sometimes dynamically block cyber attacks and malware.

Password Manager

Users are not password storage devices so to ensure secure passwords can be used a password Manager like Bitwarden must be provided for all employees.

Cyber Training

People need training to know how to avoid being a victim of a Cyber attack. Vertex are providing 3 months free using the coupon "**CORAGGIOCYBER**" at https://auth.vertexcybersecurity.com.au/signup/

VPNs

A VPN can also be a great way to throw off hackers looking to track your online trail. A corporate VPN scrambles your IP address and makes it more challenging for those looking to acquire login information or your company's files.

Personal VPNs offer the most basic protection, so it's important to find one that will also monitor the traffic on your business's server. This allows you to see if there is any suspicious behaviour and if there are any gaps where a hacker might be able to access.

These VPNs can also be used to encrypt data itself, so even if hackers do manage to find a way to download your information, they won't be able to open it.

Using unknown wifi like hotel or Cafe Wifi can be dangerous and using a VPN can provide protection while using it. VPNs can also be useful to hide tracking information of from advertisers, social media and other trackers.

Maintain backups

Just as you would make sure to back up a personal computer, you'll also want to make sure there are copies of your important business files on another server. Many hackers not only hold data for ransom and sell it to other companies, but they can also threaten to not give it back.

Backups can keep you from having to pay large amounts of money to get it back because you can download it again from another source.

There are plenty of types of backup software available, and it's recommended your files have security measures in place. Whether you choose to place them on a USB drive or CD, or you would like to have it on a cloud storage service. Backups can save your company a lot of resources, time and stress preventing hackers ransoming your files.

Having a backup plan that is isolated from a Cyber attack provides an important plan b, as long as the backups are encrypted and protected otherwise they could also be the cause of a cyber breach.

Phishing Browser Protection

Phishing attacks can come from multiple locations but typically load in the browser, placing leading cyber protections like XSurfLog can provide the last layer of protection even when someone click a phishing link.

Incident Response Plan

Like being prepared for a fire, being prepared for a cyber attack is important to reduce time, decisions and impacts. Regularly practicing the Incident response plan is also important to make sure the team is prepared to move quickly.

Cyber Audits

An external Cyber Company like Vertex sees many cyber attacks across many companies and knows what best protections should be applied to protect against a Cyber attack. Having an external Cyber Security audit can help a business understand the risks and protections required for their business from a Cyber experts perspective.

Introduce a contingency plan

Cyber security becomes a common problem when you may find yourself dealing with an attack. To mitigate this risk, it's recommended you have a "action plan". Time is of the essence when you are facing a security breach.

How quickly you and your employees respond can make a big difference in how much of your data is stolen and how to swiftly deal with the situation.

First responders

The first thing you should consider is which staff members will be involved and who you should immediately contact in order to resolve the problem. Including an IT expert, may be your first step to shut down the attack and control how much company and consumer data is stolen.

Do you need a system-wide shutdown?

While this should be seen as a last resort, if the attack is bad enough it may be necessary to shut down your entire system. This can stop an already-occurring attack and lock out any additional hackers.

On the other hand, staff and clients will immediately know that there is a problem. You'll want to have an expert on hand to help you get things back up and running again with enhanced security in place, and you'll want to alert management to what has occurred.

Ongoing Audits

Finally, the best way to avoid dealing with a problem with security is to have regular security audits and pay attention to potential threats and be aware of any cause for concerns, ensuring employees highlight any suspicious activity.

When you have created a company culture where cyber security is a priority, your staff is more likely to recognise anything that could be a company threat.

In conclusion, with the pandemic still underway driving business operational decisions, expect more cyber threats in 2022. Work-from-anywhere is here to stay and it's unclear whether we'll ever make a full return to traditional office setups, therefore staying cyber safe is the "next normal".

Anti-malware agents may stop a cyber threat in progress, however won't be able to restore any compromised data. Backup agents won't automatically know about a cyber threat and data will be recovered slowly — assuming that it hasn't been compromised. Security patches to fix vulnerabilities in popular software are released frequently, however these are inconsequential if not enabled across your workloads in a timely manner.

With these challenges ahead, it's important businesses invest in **solutions** that can address the top cyber threats head-on and provide comprehensive cyber protection mitigating risk for your business.

Practice safe computing and stay cyber safe!

What is Coraggio?

Being a business owner is even more challenging during a crisis and may include facing unchartered territory, including the rise in cyber security. Making the right decisions to future proof your business deserves more than the occasional conversation with a mate. It deserves to aggregate the experience and a shared knowledge of collective awareness from fellow executives to stay ahead of the curve and…. it doesn't have to be lonely at the top.

Operating a company typically presents complex issues, sometimes on a daily basis. Imagine if you could leverage the experience from an extensive group of industry peers to improve your decision making and social proof as well as future proof a sustainable business, whilst being held accountable?

Also imagine if you gained the peace of mind to seamlessly access these answers and navigate business challenges, simply by connecting with entrepreneurs and gaining knowledge from business leaders? This is the strength of peer to peer leadership mentoring and impactful, meaningful relations.

Coraggio offers a mutual exchange of expertise, ideas and a support system enabling you to capitalise on a give-and-take dynamic amongst advisors who have walked the path before, mitigating risk to your business.

Leading business owners and entrepreneurs join Coraggio to become part of a highly effective business community facilitating leadership, guaranteeing accountability and sharing innovative ideas within a cohesive and confidential national network.

This mutual exchange of Member's expertise tangibly results in sustainable revenue streams, increased cash reserves and productive outcomes to future proof your business.

Coraggio Chairs are industry leaders, Members are forward-thinking advisors and all Advisory Boards are dedicated to the ongoing success of their fellow Member's businesses, offering *Fearless Objective Advice* – that's the Coraggion Spirit!

Afterall, in the words of Henry Ford

"If everyone is moving forward together,
then success takes care of itself".

CoraggioLeadershipCommunity | @coraggioleaders | /company/coraggio-pty-ltd

CORAGGIO

FEARLESS OBJECTIVE ADVICE

Being a business owner typically presents complex issues and may include facing unchartered territory. However, it doesn't have to be lonely at the top. Discover how Coraggio's proven methods can assist you build a better business and become a more effective leader.

JOIN BUSINESS LEADERS **TO GAIN A COMPETITIVE EDGE**

Contact **info@coraggio.com.au** or call **1300 899 006** to touch base with our Advisory Board Team.

Visit **coraggio.com.au** for an in-depth understanding of our Member's success stories applying the Coraggio competitive edge.

AUSTRALIAN HEAD OFFICE
Level 1, 24 Young Street, Neutral Bay, Sydney NSW 2089

Advisory Board Meetings held at:
Level 31, 1 Eagle Street, Brisbane QLD 4000
94 Seaworld Drive, Main Beach, Gold Coast QLD 4217
Level 5, 1 Margaret Street, Sydney NSW 2000
Level 14, 385 Bourke Street, Melbourne VIC 3000

QUEENSLAND | VICTORIA | NEW SOUTH WALES
1300 899 006 | coraggio.com.au | ABN 27 130 780 488