KBI media

CISCO

Small Business Cyber Safety

Cybersecurity Awareness

Version 1.0.8

KBI media

CISCO

Small Business Security

In today's digital environment, Small to Medium Businesses (SMBs) in Australia and New Zealand (ANZ) are increasingly vulnerable to cyber-attacks, with cybercriminals targeting these organisations for their often-limited security measures relative to enterprise organisations. This, however, doesn't exclude them from regulatory responsibilities.

Cisco's *Cybersecurity for SMBs: Asia Pacific* Report reveals that **65% of (SMBs) in the ANZ region have experienced a cyber-attack in the past 12 months**. The report highlights phishing, ransomware, and malware as the most prevalent threats. Phishing attacks, which trick employees into revealing sensitive information, remain a leading cause of security breaches, impacting businesses across all sectors.

For small businesses, a cyber breach can have devastating financial repercussions. According to Cisco, **38% of ANZ small businesses affected by a cyber-attack faced damages exceeding $1 million AUD**, covering both direct financial losses and the cost of business disruptions. Beyond financial impacts, breaches also erode customer trust, with nearly 70% of ANZ consumers expressing concern over data privacy and preferring to do business with companies that demonstrate strong data protection measures.

While many small businesses may view cybersecurity as a secondary priority, affordable measures can significantly reduce risks. Simple steps such as regular software updates, data backups, and basic risk calculations can mitigate the most common cyber threats. As remote working continues to expand, especially since the pandemic, securing remote access is critical. In Cisco's report, **47% of ANZ businesses are now focusing on remote security**, recognising the expanded risks as employees connect from outside traditional office networks.

So many of the cybersecurity resources available SMBs often directed to are still filled with jargon, seemingly written for IT professionals. This leads to information overload, and general overwhelm, meaning the measures that *should* be within reach are neglected.

This guide provides an outline of core cybersecurity practices across three key areas;
1. Updates & Backups, 2. Risk Assessments, and 3. Remote Work Security.

By implementing these measures, SMBs can create a strong foundation to protect against cyber threats, ensuring both operational continuity and customer trust in an increasingly hostile digital landscape.

KBI media

CISCO

Small Business Security

Updates & Backups

Keeping Your Systems Current and Secure

Regular updates and backups are essential steps for any business to minimise the potential damage cyber threats can cause.

System & Software Updates

Why Update? Cybercriminals frequently exploit software vulnerabilities. Manufacturers release updates to patch these issues, typically for free. Staying up to date is your primary defence against malicious attacks.

What Should I Be Updating? Prioritise updating operating systems (like Windows and Mac OSX), antivirus software, firewall software, and commonly used applications (such as office software and web browsers) is quick and easy, and will provide huge returns in terms of security uplift.

Automate Your Updates! Where possible, set systems to update automatically. This ensures you never miss an important security patch. There might occasionally be an unintended hiccup, but the upside of automating your updates outweighs the downsides in the vast majority of circumstances.

Backups

Why Back Up Data? Regular backups can protect your business if data is lost, stolen, or compromised. Backups provide a recovery point, enabling you to resume operations quickly if issues like a ransomware attack locks-up your entire IT environment.

How Often? For most businesses, daily backups are ideal. Consider incremental backups that save only changes made since the last backup. It's a good idea to also make weekly back-ups as well, and even quarterly or annual ones. Search online for **Grandfather-Father-Son (GFS)** back-ups to understand your options better.

Where Should We Back Up? Use both on-site and off-site backups. Cloud storage offers flexible, scalable solutions, but ensure it has robust security features. Keep physical backups on secure, encrypted devices stored in a separate location.

Lastly; test your backups! Periodically test your backups and restoration systems to ensure data can be restored successfully in an emergency, and your business can continue operating with minimal impact.

KBI media

CISCO

Small Business Security

Risk Assessments

Identifying and Mitigating Cybersecurity Threats

A risk assessment identifies potential cybersecurity threats and evaluates how to manage them. By understanding your vulnerabilities, you can proactively put protections in place.

Conducting a Risk Assessment

Identify and document your critical assets, including customer data, employee information, and sensitive financial records. Imagine what impacts there would be if they disappeared or stolen.

Consider potential threats and risks such as phishing attacks, malware, ransomware, and insider threats. Cybercriminals may target weak points, such as unprotected software or untrained staff. A gap analysis on what you've not put measures against (or ones you need to update) will help you identify suitable solutions.

Examine areas where your business might have vulnerabilities., and thus be exposed to risk. Your first stop should be looking for outdated software, weak passwords or password policies, or unencrypted data that you won't like to lose or share with the world.

Develop a Strategy

As an SMB you need to work with other businesses, both suppliers and customers. There should be a mutual expectation that critical security measures are in place to protect from supply chain attacks too. So, as well as taking care of your own fundamental security, work with your aligned businesses to ensure that your door to them isn't also a door to hackers, and nor are you unwittingly providing access to their systems.

Focus on high-priority risks first. For example, phishing attacks are common and often target businesses indiscriminately. Invest in a secure email filter and educate staff on recognising phishing attempts.

Implement Safeguards to limit access to sensitive data to just those employees that specifically need it, and enforce strong password policies, ideally along with M/2FA.

Risk management is an ongoing process. Regularly review your risk assessment and adapt to new threats or operational changes. Aim to conduct full assessments annually or following major changes in your business.

KBI media

CISCO

Small Business Security

Remote Work Security

Off the corporate network but still on your radar

Remote working is a part of the modern workscape, but presents unique security challenges. Protecting your business requires a combination of technology, policies, and employee training.

Secure Remote Access

A VPN (Virtual Private Network) encrypts data transmitted between your network and remote devices, providing a secure connection. Set up a reliable VPN for all employees working off-site. They're inexpensive, particularly for small businesses, and very effective in uplifting your security.

Implementing Multi-Factor (including Two-Factor) Authentication (MFA or 2FA) on all systems to add a second layer of security. This makes it *significantly* harder for unauthorised individuals to gain access, even if a password is compromised. Most software platforms you use will offer this function, which typically include an SMS or email of a single use pin to enter as an additional later of protection. There are several enterprise-grade versions of software available for free.

Device Management

Company-issued devices should have endpoint protection software, which monitors and blocks potential threats like malware, ransomware, and unwarranted remote access installations.

Device Encryption protects sensitive data if they are lost or stolen on any devices levering it. This is especially important when handling any sensitive information like customer data, banking & financial details, and any intellectual property your organisation may have.

Set devices - whether a phone or computer - to lock after a short period of inactivity to prevent unauthorised access when the user is away from their keyboard for any period of time.

Policies & Training

Establish a remote working policy outlining security requirements for remote work, including guidance on using only secure, personal Wi-Fi networks, and *never* public ones.

Train employees to recognise social engineering tactics, secure their home networks, and practice good cyber hygiene, such as regularly changing passwords.

Encourage employees to report suspicious activity or incidents immediately. A swift response can prevent potential damage. And let them know they won't be in trouble for coming clean!

KBI media

CISCO

Small Business Security

Additional Tips

Cybersecurity is an ever-evolving field.

By taking even the basic steps inside this document you're already making your business much more secure. So, once you've completed these measures, what should you look at next?

Password Management

Encourage use of a password manager to create & store complex passwords. Remind employees to avoid reusing passwords across different accounts. A breach can lead to lists of passwords being made available to hackers, and they can use those same passwords on your business.

Network Security

Install a firewall on your network to prevent unauthorised access. You can also use firewall software for remote employees as well to block many nefarious attempts.

Email Filtering

Implement email filtering to detect and block phishing emails, spam, and malicious attachments before they reach inboxes.

KBI media

CISCO

Small Business Security

Additional Tips

Security Awareness

Regularly update your team on evolving threats. Awareness is one of the most effective defences against cybercrime. It doesn't have to be onerous. There are paid and free security and threat intelligence feeds available online. (See the Additional Resources section of this document).

Spot The Difference

It can be very hard to spot a phishing email, particularly in the era of AI where the messaging and designs can be honed automatically to be even more convincing.

See if you can identify the telltale signs in the phishing email example below:

From: support@microsoft.help.dd
Sent: 09/11/2024 11:11
To: Jane Smyth jane.smyth@acmesecurity.co
Subject: Urgent! Action Required!

Outlook.com

Microsoft Account

Verify your Account

Dear Valued Customer,

We recently noticed suspicious activity in your account and require immediate verification to ensure your security.

Action Required:
Please click on the link below to verify your account information within the next 24 hours to avoid service disruption.

If you do not verify your account by the deadline, your access to online accounts will be temporarily restricted.

Thank you for choosing Microsoft Services. We are committed to keeping your information safe.

http://account.liive.com/resetpassword.aspx

Sincerely,
Microsoftr Services Support Team
www.microsoft.com
Customer Support: 1-800-555-1234

From: support@microsoft.com
Sent: 09/11/2024 11:11
To: Jane Smyth jane.smyth@acmesecurity.co
Subject: Unusual Sign In Activity

Outlook.com

Microsoft Account

Verify your Account

We recently detected unusual activity about a recent sign in from your Microsoft account ja*****@acmesecurity.co signalling that you might be signing on from a new location or device.

To help keep your account safe, we've restricted access to your inbox, contact lists, and calendar for that session.

Please review your recent activity and we'll help you ensure your account is secure. To regain access you'll need to confirm that the recent activity was yours:

Review recent activity

Thanks,

The Microsoft Support Team

KBI media

CISCO

Small Business Security

1. From: support@microsoft.help.dd
Sent: 09/11/2024 11:11
To: Jane Smyth jane.smyth@acmesecurity.co
2. Subject: Urgent! Action Required!

Outlook.com

Microsoft Account

Verify your Account

3. Dear Valued Customer,

We recently noticed suspicious activity in your account and require immediate verification to ensure your security.

4. **Action Required:**
Please click on the link below to verify your account information within
5. the next 24 hours to avoid service disruption.

6. If you do not verify your account by the deadline, your access to online accounts will be temporarily restricted.

Thank you for choosing Microsoft Services. We are committed to keeping your information safe.

7. http://account.liive.com/resetpassword.aspx

Sincerely,
8. Microsoftr Services Support Team
www.microsoft.com
Customer Support: 1-800-555-1234

1. A non-authoritive domain. It may look similar, but it likely won't be the same as the primary domain for the organisation.

2. There will often be a false sense of urgency to lead towards immediate action. The user will feel compeled to act now, rather than spend time taking a closer look.

3. The opening greeting may seem overly formal or strange. Terms like "Dear", "Sir/Madaam" or similar may be used.

4/5. A sense of urgency is being deliberately manufactured.

6. Loaded language is used to again compel the user to immeaite action.

7/8. There will often be typographical errors or unusual combinations of letters in links or surrounding text.

---

1. From: support@microsoft.com
Sent: 09/11/2024 11:11
To: Jane Smyth jane.smyth@acmesecurity.co
2. Subject: Unusual Sign In Activity

Outlook.com

Microsoft Account

Verify your Account

3. We recently detected unusual activity about a recent sign in from your Microsoft account ja*****@acmesecurity.co signalling that you might be signing on from a new location or device.

To help keep your account safe, we've restricted access to your inbox, contact lists, and calendar for that session.

Please review your recent activity and we'll help you ensure your account is secure. To regain access you'll need to confirm that the recent activity was yours:

4. Review recent activity

Thanks,

The Microsoft Support Team

1. Use of the primary domain of the sending organisation. Look for similarly styled choices like **nn**icrosoft.com

2. Factual statements as to the reason and nature of the email being sent to you.

3. Specific details being encapsulated - usually redacted - in the text to demonstrate account voracity.

4. A call to action that links to the correct top level domain, and the relevant page or section of your account when you hover over the link.

KBI media

CISCO

Small Business Security

Additional Resources

Cybersecurity is an ever-evolving field.

For more on staying safer, visit the KBI.Media site helping people and small businesses improve their cyber safety.

Learning Resources

https://www.cisco.com/c/en_au/products/security/what-is-cybersecurity.html
https://www.cisco.com/c/en/us/products/security/cybersecurity-awareness-month.html
https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html
https://www.netacad.com/home

Threat Intelligence & Security Awareness News

https://talosintelligence.com/

More Resources

https://www.cosboa.org.au/cyber-security
https://www.cyber.gov.au/resources-business-and-government

KBI media

CISCO

Small Business Security

About Cisco

Cisco is the worldwide technology leader that securely connects everything to make anything possible. Our purpose is to power an inclusive future for all by helping our customers reimagine their applications, power hybrid work, secure their enterprise, transform their infrastructure, and meet their sustainability goals.

About KBI.Media

KBI.Media is the independent and agnostic voice of cyber. No paywalls. No sponsored content. We share opinion pieces, news and thoughts about the cyber security space. We're focused on delivering information within the cyber security community, and the broader business market.

You can download this PDF too and get access to additional links inside the digital version:

Scan Me

kbi.media/smb