Integrity Systems

red meat customer assurance

MEAT & LIVESTOCK AUSTRALIA

A guide to protecting your farm data and information

Edition 1: March 2021

Table of contents

MLA acknowledges the matching funds provided by the Australian Government to support the research and development detailed in this publication.

Introduction

As the world becomes increasingly dependent on technology, protecting the business information or data stored on your computer, laptop, mobile phone and other digital devices, known as cyber security, is very important.

Cyber security is vital to help prevent a cyber-attack, which is any deliberate attempt by an individual or organisation to gain unauthorised access to a computer or computer system.

A cyber-attack that impacts a small business can be devastating, however, cyber security to protect your business information or data is not difficult to implement.

This guide has been produced to help you understand and implement cyber security measures to protect your data, which is all the information stored in electronic form on your computer and digital devices.

Presented in an easy-to-read format, this guide provides clear explanations and advice.

Following the advice in this guide will significantly increase your protection of important business data and information from the most common types of cyber-attacks.

While this guide can't guarantee protection from all types of cyber-attacks, it does show how easy it is to protect your business, information, data, assets and the reputation of your business.

Measures to implement	Effort	Impact
Using passwords to protect data	Low	High
Protecting against malware and ransomware	Medium	High
Backing up data	Medium	High
Two-factor authentication (2FA)	Low	High
Keeping mobile devices safe	Low	High
Avoiding phishing attacks	High	High
Employee training	High	High
Ethical use of data – things for producers to think about	Low	Low
Terms and conditions	Low	Low
Encryption of data in transit and at rest	Medium	High
Responding to incidents	High	High

Back up your data

What is a backup?

A backup is a copy of important data that is stored in an alternative location, so it can be recovered if deleted or becomes corrupted. Depending on how often the data changes, how valuable it is, and how long it takes to back up determines how often to back up.

Why do you need to back up data?

Think about how much you rely on your business-critical data. Customer details, quotes, orders, and payment details. Now imagine how long you would be able to operate without them.

All businesses, regardless of size, should take regular backups of their important data, and make sure that these backups are recent and can be restored. By doing this, you're ensuring your business can still function following the impact of flood, fire, physical damage or theft.

Where do I keep my backups?

Whether it's on a USB stick, on a separate drive or a separate computer, access to data backups should be restricted so that they:

- are not accessible by staff
- are not permanently connected (either physically or over a local network) to the device holding the original copy

Ransomware (and other malware) can often move to attached storage automatically, which means any such backup could also be infected, leaving you with no backup to recover from. For more resilience, you should consider storing your backups in a different location, so fire or theft won't result in you losing both copies.

Identifying what you need to back up

Your first step is to identify your essential data. That is, the information that your business couldn't function without. Normally this will comprise documents, photos, emails, contacts, and calendars, most of which are kept in just a few common folders on your computer, phone, tablet or network.

You should consider the cloud

Using cloud storage (where a service provider stores your data on their infrastructure) means your data is physically separate from your location. You'll also benefit from a high level of availability. Service providers can supply your business with data storage and web services without you needing to invest in expensive hardware up front. Most providers offer a limited amount of storage space for free, and larger storage capacity for minimal costs to small businesses.

Make backing up part of your everyday business

We know that backing up isn't a very interesting thing to do (and there will always be more important tasks that you feel should take priority), but the majority of network or cloud storage solutions now allow you to make backups automatically. For instance, when new files of a certain type are saved to specified folders. Using automated backups not only saves time, but also ensures that you have the latest version of your files should you need them.

Many off-the-shelf backup solutions are easy to set up, and are affordable considering the business-critical protection they offer. When choosing a solution, you'll also have to consider how much data you need to back up, and how quickly you need to be able to access the data following any incident.

SUMMARY CHECKLIST

- ☐ **Identify what data you should back up**
- ☐ **Identify how often you should back up that data**
- ☐ **Store backups in a different location**
- ☐ **Consider cloud storage to store backups**

Protect against malware and ransomware

What is malware and ransomware?

Malicious software (also known as 'malware') is software or web content that can harm your business. Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Why should you be protected?

Malware gains access to important information such as bank or credit card numbers and passwords. It can also take control or spy on a user's computer. What criminals choose to do with this access and data includes:

- theft
- pranks
- activism
- espionage
- other serious crimes.

Install antivirus software

Antivirus software – which is often included for free within popular operating systems – should be used on all computers and laptops. For your office equipment, you can pretty much click 'enable', and you're instantly safer.

Prevent staff from downloading apps from unknown sources

You should prevent staff from downloading third party apps from unknown vendors/sources, as these will not have been checked. Staff accounts should only have enough access required to perform their role, with extra permissions (i.e. for administrators) only given to those who need it. When administrative accounts are created, they should only be used for that specific task, with standard user accounts used for general work.

Keep your devices up to date and patched

For all your IT equipment (tablets, smartphones, laptops and PCs), make sure that the software and firmware is always kept up to date with the latest versions from software developers, hardware suppliers and vendors. Applying these updates (a process known as patching) is one of the most important things you can do to improve security – the IT version of eating your fruit and vegetables. Operating systems, programs, phones and apps should all be set to 'automatically update' wherever this is an option.

Control how USB drives can be used

We all know how tempting it is to use USB drives or memory cards to transfer files between organisations and people. However, it only takes a single user to inadvertently plug-in an infected stick (such as a USB drive containing malware) to devastate the whole organisation.

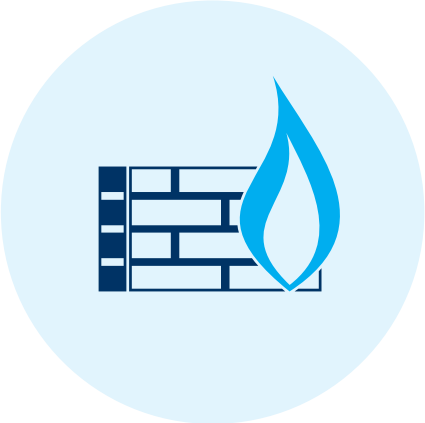
When drives and cards are openly shared, it becomes hard to track what they contain, where they've been, and who has used them. You can reduce the likelihood of infection by:

- blocking access to physical ports for most users
- using antivirus tools
- only allowing approved drives and cards to be used within your organisation – and nowhere else.

Make these directives part of your company policy, to prevent your organisation being exposed to unnecessary risks. You can also ask staff to transfer files using alternate means (such as by email or cloud storage), rather than via USB.

Switch on your firewall

Firewalls create a ‘buffer zone’ between your own network and external networks (such as the Internet). Most popular operating systems now include a firewall, so it may simply be a case of switching this on.



What should you do if you get malware on your systems?

If you suspect your systems are infected, you should disconnect the computer from your network and Internet. This way, you would be preventing the malware from spreading. In addition you should scan the system with your antivirus program. In most cases, it is recommended to reinstall the system as many attackers can use different techniques to maintain access to the compromised system.

SUMMARY CHECKLIST

- [ ] **Install antivirus on all computers and laptops**
- [ ] **Prevent staff from installing applications from suspicious sites**
- [ ] **Keep devices up to date**
- [ ] **Limit USB drives use**
- [ ] **Turn on Firewall**
- [ ] **See also the Avoid phishing attacks section of this handbook on page 14**

Use passwords to protect data

What is a password?

A password is a string of characters used to prove identity or access, which should be kept secret from those not allowed access. It allows business owners to decide who they would like to give access privileges to and enforce staff access control limits.

Why do you need a password?

Unauthorised access is a potentially major problem for anyone who uses a computer or high-tech devices such as smartphones or tablets. Your passwords are the most common way to prove your identity when using websites, email accounts and your computer itself (via user accounts). The use of strong passwords is therefore essential in order to protect your security and identity. The best security in the world is useless if a malicious person has a legitimate user name and password.

The consequences for victims of these break-ins can include the loss of valuable data. Victims may also have their bank account information, money, or even their identity stolen. Moreover, unauthorised users may use someone else's computer to break the law, which could put the victim in legal trouble.

How to pick a good password?

By following best practice with your passwords, you can significantly reduce the chance that you'll succumb to an attack from another website, regardless of how they store your information.

If you use a different password everywhere, then only the password for that service is broken. Since the attacker will likely already have all the information stored with that service, they're not going to get any additional information they didn't already have.

There are four components to a good password:

- Your password should be **long**
- Your password needs to be **random**. Don't use your name, or your date of birth
- Your password should be **unique**. Every account should get its own password, and you shouldn't follow patterns
- Your password should be **private**. Never share it with anyone.

Avoid using predictable passwords – Good vs bad passwords

Hopefully it's all clear to you why 'password' is a really bad password to use. Please don't ever use it, or any dictionary word. What about the next one though, 'P4ssw0rd'? The 'a' has been replaced with a '4' and the 'o' a '0'. This can also be trivially broken, as these are standard letter replacements and are a widely known technique. This might add a few minutes to the amount of time it takes to break.

The next one is better, 'P&sSw0~d', we've got special characters in there now, and not some standard replacements. But the password is only 8 characters long, and as we learned earlier, that's too short.

What about 'I Like Rainbows!'. This is going to be much harder to break, but there are password cracking tools specifically designed for sentence based passwords. You can treat each word here like an individual 'token', and it becomes similar to a four-character password (albeit with a much larger alphabet). This will certainly take longer than the others to break, but it can be broken much quicker than you probably realise.

Some examples of good passwords include:

- lakuSj>qP&^`H;Bk^jo]3%}&’iTH\VU*7iw”>k:WOZC:t/3A?
- -#!frWr[:pGYur=R5E:,gpr%h;]t#}#FjZpwesims(dvRw<!c
- Q2D”g(l^C34sNqFv^huED{n*ljmqZ;,3`RO$,y2(2dt7l+1z

They’re long, unique, and random. Although obviously they’re no longer private because they’re on this document and you’ve all seen them, but this gives you an idea of what your passwords should be looking like.

What is a password manager and why should you use one?

There’s no chance we can remember those types of passwords, but that’s the point. Any password that’s easy for a human to remember is going to be even easier for a computer to break.

So, how do you remember all the passwords? You don’t. You need to use a tool called a password manager. They each have their own pros and cons depending on how you prefer to operate. Most have browser plugins to automatically enter your passwords for you. But they’re all designed to do pretty much one thing. Store a directory of all your usernames and passwords, protected by a single ‘master password’, which is the one password you need to remember. The idea is that it’ll be the last password you need to remember.

Using a password manager is the single most effective thing you can do to enhance your security online. Password managers are designed to remember all of your passwords for you, in a secure way.

They can also generate completely random passwords for you, and you can typically change the criteria associated with this generation. So if a website doesn’t let you use special symbols, you can exclude those and still get a strong password. But the most important feature of password managers is that they let you use a completely different password for everything, without having to worry about remembering it yourself.

How to create a good password

While you set up your password manager and choose a completely random password, here is a guide on how to pick a good password:

- use song lyrics or a phrase
- grab one character from each word
- the result looks random
- But is easy to remember
- use 12-16 characters.

Phrase:

- You have not experienced Shakespeare until you have read him in the original Klingon

Possible strong passwords:

- YhneSuyhrhitoK (letters only)
- Yh<>e$uyhrh1t0K (alphanumeric & symbols)

Security questions

There's some things that are basically the same as your password. For example, security question answers. If they have that information, they can likely gain access to your account.

Never use real information for security questions. No matter how strong you make your password, if you use real information for your security questions, your account is going to be easier to compromise. Treat them like passwords, generate them in your password manager and store them there.

Change all default passwords

Regardless of what they are being used for, default passwords need to be changed immediately upon being introduced to a digital environment or network. Many manufacturers will provide default passwords to enable easy access to additional features, security, etc. However, these default passwords can be found in a whole host of different locations. These resources are typically meant to be used when a user forgets the default credentials – but you can be sure that hackers will use the same resources as well.

Your password has been breached – what should you do?

If you suspect or know that your account has been compromised, you must change the password immediately. If you have reused your password on other accounts, which is a habit you definitely should get rid of, you should change passwords for those accounts as well.

SUMMARY CHECKLIST

- ☐ **Use strong passwords and keep them safe**
- ☐ **Do not use the same passwords across multiple sites**
- ☐ **Use a password manager to keep stock of all your passwords and log-in details**
- ☐ **Change all default passwords**

Two-factor authentication (2FA)

What is two-factor authentication?

You may have heard the term 'multi-factor authentication', or 'two-factor authentication' a lot. But what exactly is it?

In the field of authentication, there are three main types of evidence (or 'factors') you can provide. These are called 'knowledge', 'possession', and 'inherence'. In plain English, that's something you know, something you have, and something you are. So, something you know would be a password. Something you have would be your phone, or a physical object. And something you are would be a fingerprint, or some other form of biometrics.

The idea of two-factor authentication is that you pick two of these factors, and require them in order to authenticate a user. It significantly decreases the risk of a hacker accessing your online accounts by combining your password (something you know) with a second factor, like your mobile phone (something you have).

Why should you use it?

The vulnerability of passwords is the main reason for requiring and using 2FA. While an attacker might be able to remotely steal your password, it's pretty unlikely they'd also be able to physically steal your phone or get a fingerprint. Likewise, if an attacker can physically steal your phone, it's unlikely they'd also be able to get your password.

While it does require one extra step to a log-in process, it provides a much stronger defence for your account. If your password is hacked (accessed by someone else without your permission) and you have 2FA activated on your account—the hacker cannot gain access. They need both levels of authentication.

Having 2FA is not going to remove all risk, but you are much harder to hack than accounts with only single-factor authentication. This means you are a much less attractive target and you are dramatically reducing your risk of being hacked.

How do you configure your account for 2FA?

Some online services will automatically prompt you for a second factor when you log in. However many don't, so you will need to activate it yourself. You'll find the option to switch on 2FA in the security or privacy settings of your online accounts (it may also be called 'two-step verification'). The Turn It On website (***https://www.telesign.com/turnon2fa/***) details which websites and apps offer the option to use 2FA and gives instructions on how to set it up.

SUMMARY CHECKLIST

- ☐ **Wherever possible, activate two-factor authentication (2FA)**
- ☐ **Activate two-factor authentication in all work systems**
- ☐ **You should use it for all your personal stuff too**

Keep mobile devices safe

Switch on password protection

A suitably complex PIN or password (opposed to a simple one that can be easily guessed) will prevent the average criminal from accessing your phone. Many devices now include fingerprint recognition to unlock your device, without the need for a password. However, these features are not always enabled 'out of the box', so you should always check they have been switched on.

Keep your device up to date

No matter what phones or tablets you are using, it is important that they are kept up to date at all times. All manufacturers (for example Windows, Android, iOS) release regular updates that contain critical security updates to keep the device protected. This process is quick, easy, and free. Devices should be set to automatically update, wherever possible. Make sure your staff know how important these updates are, and explain how to do it, if necessary. At some point, these updates will no longer be available (as the device reaches the end of its supported life), at which point you should consider replacing it with a modern alternative.

Keep your apps up to date

Just like the operating systems on your business's devices, all the applications that you have installed should also be updated regularly with patches from the software developers. These updates will not only add new features, but they will also patch any security holes that have been discovered. Make sure you know when updates are ready, how to install them, and that it's important to do so straight away.

Don't connect to unknown Wi-Fi hotspots without a VPN

When you use public Wi-Fi hotspots (for example in hotels or coffee shops), there is no way to easily find out who controls the hotspot, or to prove that it belongs to who you think it does. If you connect to these hotspots, somebody else could access:

- what you're working on while connected
- your private login details that many apps and web services maintain while you're logged on.

The simplest precaution is to not connect to the Internet using unknown hotspots, and instead use your mobile 3G or 4G mobile network, which will have built-in security. You can also use Virtual Private Networks (VPNs), a technique that encrypts your data before it is sent across the Internet. If you're using third party VPNs, you'll need the technical ability to configure it yourself, and should only use VPNs provided by reputable service providers.

SUMMARY CHECKLIST

- ☐ **Turn on password protection across all your mobile devices**
- ☐ **Turn on automatic updates**
- ☐ **Turn on automatic app updates**
- ☐ **Be careful when using a public Wi-Fi. Use your 3G/4G or a VPN**


Username
Password
LOGIN

Avoid phishing attacks

What is social engineering?

For those who've not heard the term before, here's a quick definition of what social engineering is. Basically it's a type of confidence trickery. Convincing people to give up information either without them realising it, or by making them believe you're someone else.

Social engineering is mostly about building trust. If a hacker wanted to social engineer the CEO of a company, the CEO would not be their first phone call. They'd start by calling a low-level employee claiming to be a new employee needing help, or they'd call a new employee and claim to be an established employee asking for help. They'd learn some little bits of information, maybe a bit of internal lingo that's being used. Then the next person they'd call would be slightly higher up the chain, they'd use the information they learned on the first call to sound more credible. And so on and so forth. By the time they call the CEO, they'd have so much internal knowledge and language for the company that it would sound like the hacker was an employee.

This is hard to defend against, since human nature is to want to help others. So if someone contacts you claiming to be an employee, and you've never heard of them before, verify they are who they say they are via another channel. If they email you, call them or message them to check if they have actually emailed you.

What is a phishing attack?

Phishing (with a 'ph') is a particular type of social engineering attack that people get exposed to. The term comes from "fishing for information", and generally involves receiving an email designed to trick you into giving up information. As a company gets larger, it becomes more of a target for these types of attacks.

Some phishing attacks can be pretty easy to spot. You've likely heard of the Nigerian Prince Scam. This is where an email claiming to be someone who can give you lots of money is sent to lots of people. This is a 'spray and pray' approach to scamming. Maybe one or two people will bite, but that makes it worthwhile enough for the scammer. These are pretty easy to spot, and not something to really worry about.

What is spear-phishing?

These much more targeted attacks are called 'spear-fishing'. An attacker spent a lot of time learning about our internal organisation's structure and crafting a legitimate looking email in order to try and get lots of money from us. These are the types of attacks we care the most about protecting against.

Protecting yourself

Unfortunately, there's no golden rule. It's up to everyone to remain vigilant and watch for signs of suspicious emails. Some things to take care with, the 'from' address of an email can easily be spoofed. There are technologies that can help to prevent this, but they're not implemented everywhere. So while a misspelled domain is a strong indicator of phishing, a real domain isn't a 100% indicator that it's genuine.

- Many phishing scams originate overseas and often the spelling, grammar and punctuation are poor. Others will try and create official looking emails by including logos and graphics. Is the design (and quality) what would you'd expect from a large organisation?
- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look out for emails that appear to come from a high-ranking person within your organisation, requesting a payment is made to a particular bank account. Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- If it sounds too good to be true, it probably is. It's unlikely that someone will want to give you money, or give you access to some secret part of the Internet.

Report all attacks

Make sure your staff are encouraged to ask for help if they think they might have been a victim of phishing, especially if they've not raised it before. It's important to take steps to scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred.

Do not punish staff if they get caught out. It discourages people from reporting in future, and can make them so fearful that they spend excessive time and energy scrutinising every email they receive. Both these things cause more harm to your business in the long run.

SUMMARY CHECKLIST

- [ ] **Watch out for suspicious emails**
- [ ] **'From' addresses can be spoofed**
- [ ] **To verify if it's from an employee, ask them via IM or in person**
- [ ] **Never click on any links in an email you think may be phishing**
- [ ] **You are your greatest asset in the fight against phishing**

Employee training

Why should employees be trained?

Humans are the weakest link in information security. If the human factor is not taken care of, the levels of exposure to threats, and subsequent impact, is way higher than what most would call acceptable. That is where security awareness training plays a major role. Awareness requires having knowledge, being conscious of why the rules exist. Your users will understand why information security is a vital aspect of your business, what are the consequences of incidents, and what is expected of them.

What does security training involve?

Security awareness training can be performed in a variety of ways that can be utilised alone or in conjunction with each other. Those mediums can consist of a more thorough classroom-style training, creation of a security-awareness website, pushing helpful hints onto computers when they start up and/or e-mailing helpful hints on a weekly or monthly basis, and using visual aids like posters.

In addition, topics addressed by the security awareness training can range from phishing to passwords, two-factor authentications and malware.

Remember to make your content as familiar as possible. You can use pictures as well. Finally, the proof of the pudding is in the eating. Before the training, phishing simulation is a great way to measure your organisation's exposure to phishing attacks.

When should you train your employees?

The security awareness training sessions should be repeated on a regular basis as the positive effects fade away over time. Also, phishing simulation campaigns should be a routine exercise to:

- keep a general level of security awareness and vigilance
- identify new employees (e.g. new hires, contractors, vendors) with challenges to withstand social engineering attempts
- identify existing members of staff who may require further education
- raise staff awareness of new types of phishing emails they are likely to receive.

SUMMARY CHECKLIST

- ☐ **Face-to-face training where possible**
- ☐ **Make the content relatable and use examples of actual phishing emails your organisation has received**
- ☐ **Encourage positive security practices at home as well as the office**
- ☐ **Validate the effectiveness with phishing simulation before and after training**

Terms and conditions

What are terms and conditions?

The terms of service is a legal document that protects the company and explains to consumers what the rules are when using the service. The terms and conditions are nothing other than a contract in which the owner clarifies the conditions of use of its service. Some quick examples are the use of the content (copyright), the rules that users must follow while interacting with one another on the website/ app and, finally, rules related to the cancellation or suspension of a user's account.

Understanding terms and conditions

Terms of service are often too long to read, but it's important to understand what's in them. Your online rights depend on them. If you do not understand the implications of what you are signing up to, you may not be aware how much control the service provider is asserting over their content or the extent to which their information is being mined and traded.

However, who has the time to wade through page after page of dense legal jargon to spot the worrisome bits? For that reason, you should search for keywords or phrases in the document that will tell you what information the app or website collects, how long it keeps it and with whom it shares it. 'Third parties' is a key phrase, as are 'advertising partners' and 'affiliates'. 'Retain' or 'retention' can indicate how long the company keeps your personal information. 'Opt out' may indicate how to turn off the sale or collection of your personal information.

"Terms of Service; Didn't Read" (short: ToS;DR) is a project started in 2012 to help fix the 'biggest lie on the web': almost no one really reads the terms of service we agree to all the time. This site summarises key points of the most common terms and condition services. The project offers a free browser extension that labels and rates these agreements from very good (Class A) to very bad (Class E) on the websites you visit. When installed in your browser, it scans terms of service to unearth the worrisome stuff. ***https://tosdr.org/***

Common issues with T&C

People are often surprised to find out they're obliged to pay to return unwanted items purchased online, as it is commonly stated in the terms and conditions – and these fees can be expensive.

It is really important you understand everything before you sign on the dotted line, as you could find yourself landed with extra fees or charges.

In addition, your personal information and identity can be used in ads or shown to other users. Your activity on other websites can also be tracked.

SUMMARY CHECKLIST

- ☐ **Make sure you understand what you are agreeing to**
- ☐ **Search for keywords**
- ☐ **Check 'Terms of Service; Didn't Read' site to see if they summarised the service you are signing up to. *https://tosdr.org/***

Encryption of data in transit and at rest

What is encryption?

Encryption is the process of altering a piece of information so that only the intended receivers can understand it. In other words, encryption is a way of scrambling data so that only authorised parties can understand the information.

Data in transit vs data at rest

Data in transit is actively traveling from one location to another across the digital channels of the Internet or a private network. A big concern with data of this sort is protection while it is moving, as it may be lost or intercepted in various ways.

Data at rest is not traveling from network or device to another in any way. Think of data stored on hard drives and flash drives, or sometimes inside of laptops or computers. When it comes to data at rest, protection aims to preserve inactive data stored on devices or networks. This data is less susceptible to interception and is often considered more valuable to attackers than data in motion. However, in case a laptop or hard drive is stolen, if the data is encrypted, the criminal would not be able to read the information from it.

Why data encryption is important?

With encryption, we can achieve three main objectives.

- Confidentiality (or privacy). It means that only the intended readers can understand the message, and no one else.
- Authenticity is an important guarantee for the receiver. Authenticity means that you can validate the original sender, and be sure that they are who they claim to be.
- Integrity is another guarantee for the receiver. With it, the receiver is sure that what they received is the same as the data sent, and no one altered it along the path.

SUMMARY CHECKLIST

- ☐ **Familiarise yourself with encryption**
- ☐ **Make sure data in transit is protected between your end user device and the service**
- ☐ **You should have sufficient confidence that storage media containing your data are protected from unauthorised access**

Responding to incidents

What is an incident?

A cyber security incident can be defined as:

- **A breach of a system's security policy in order to affect its integrity or availability**
- **The unauthorised access or attempted access to a system.**

Cyber incidents can take many forms, such as denial of service, malware, ransomware or phishing attacks.

What actions do you need to take?

Planning your incident response (IR) ahead of time is essential. This will be a major determining factor in the final outcome of any real world incident. You should produce IR plans, exercise your response and review your capabilities (including those of any third party service providers). This will give you the best chance of minimising the impact of any attack and recovering quickly.

You should also determine what type of incident you are facing. Some examples include:

- Malicious code: Malware infection on the network, including ransomware.
- Denial of Service: Typically a flood of traffic taking down a website, can apply to phone lines, other web facing systems, and in some cases, internal systems.
- Phishing: Emails attempting to convince someone to trust a link/attachment.
- Unauthorised access: Access to systems, accounts, data by an unauthorised person (internal or external) – for example, access to someone's emails or account.
- Insider: Malicious or accidental action by an employee causing a security incident.
- Data breach: Lost/stolen devices or hard copy documents, unauthorised access or extraction of data from the network (usually linked with some of the above).
- Targeted attack: An attack specifically targeted at the business – usually by a sophisticated attacker (often encompassing several of the above categories).

Who should you report an incident to?

The people it is escalated to must have the authority to make critical decisions. For example, when a decision may result in a major business impact, such as taking a critical service or system offline.

Identify the people who are empowered (or who hold delegated authority) to make such decisions and ensure the escalation process includes these key personnel.

SUMMARY CHECKLIST

- ☐ **Identify what kind of incidents can affect your organisation**
- ☐ **Create a plan to respond to incidents**
- ☐ **Identify who should be contacted when an incident occurs. These people should have the authority to make critical decisions**

Ethical use of data

What is personal data?

Personal data is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual. This includes:

- **biographical information (e.g. your name, address, date of birth, passport number, gender, family members and nationality)**
- **contact details (e.g. postal address, email address and phone number)**
- **information collected when you contact ISC online (e.g. email address, password, location and IP address)**
- **payment information (e.g. credit card and bank account details)**
- **photos of you, your home, etc.**

Data classification – general data, business data, customer data

- General data is anything that is intentionally available to the public. The key being intentionally. If something gets leaked, it doesn't automatically become general data.
- Business data is anything used to operate our business. Examples would be an employee list, payroll information, etc.
- Customer data is any data provided to ISC by the customer.

How to handle sensitive data

How you handle data depends on what type of data it is. For example, general data does not need to be encrypted, as it's considered public. All other types of data should always be encrypted in transit and at rest, however.

- Public data can be shared with anyone.
- Restricted data is only to be shared with customers who are under a non-disclosure agreement.
- Internal data only is not to be shared with anyone outside of the organisation.

Compliance laws – GDPR and NDB

The General Data Protection Regulation (GDPR) is a legal framework that came into effect in 2018, that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). Since the Regulation applies regardless of where websites are based, it must be heeded by all sites that attract European visitors, even if they don't specifically market goods or services to EU residents.

The GDPR mandates that EU visitors be given a number of data disclosures. The site must also take steps to facilitate such EU consumer rights as a timely notification in the event of personal data being breached.

- The right to be informed about what data is being collected and how it is being processed
- The right to access the data an organisation holds about them
- The right to correct any errors or omissions in the data
- The right to erasure, also known as the right to be forgotten, of any data that is out of date, was processed without legal basis, or is no longer relevant
- The right to restrict processing of data the organisation holds about them
- The right to data portability between competing companies to ensure a fair market.

Finally, it introduces substantial maximum penalties for non-compliance, including up to €20 million or 4% of the organisation's global revenue from the previous year, whichever is higher.

On the other hand, Australia introduced a Notifiable Data Breach scheme in 2018. Under the Notifiable Data Breaches (NDB) scheme any organisation or agency the Privacy Act 1988 covers must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved.

A data breach occurs when personal information an organisation or agency holds is lost or subjected to unauthorised access or disclosure. For example, when:

- a device with a customer's personal information is lost or stolen
- a database with personal information is hacked
- personal information is mistakenly given to the wrong person.

The notification to individuals must include recommendations about the steps they should take in response to the data breach.

SUMMARY CHECKLIST

- [ ] **Don't discuss company information in public**
- [ ] **Don't look at information you shouldn't**
- [ ] **Identify what kind of data you need for business purposes**
- [ ] **Identify sensitive data and handle it accordingly**
- [ ] **Familiarise yourself with new regulation laws like GDPR (EU) and NDB (AU)**

Quick guide

SUMMARY

A cyber security incident that impacts a small business can be devastating. This handbook has been specifically designed for small businesses and producers to understand, take action, and increase their cyber security resilience against ever-evolving cyber security threats. If you are learning about cyber security for the first time, or are keeping yourself up to date, this guide is an excellent place to start.

Backing up your data

- Identify what data you should back up
- Identify how often you should back up that data
- Store backups in a different location
- Consider cloud storage to store backups.

Protect against malware and ransomware

- Install antivirus on all computers and laptops
- Prevent staff from installing applications from suspicious sites
- Keep devices up to date
- Limit the use of USB drives
- Turn on firewall.

Use passwords to protect data

- Use strong passwords and keep them safe
- Do not use the same passwords across multiple sites
- Use a password manager to keep stock of all your passwords and log-in details.
- Change all default passwords.

Two-factor authentication (2FA)

- Wherever possible, activate two-factor authentication (2FA)
- Activate two-factor authentication in all work and personal systems.

Keep mobile devices safe

- Turn on password protection across all your mobile devices
- Turn on automatic updates
- Turn on automatic app updates
- Be careful when using a public Wi-Fi – use your 3G/4G or a VPN.

Avoid phishing attacks

- Watch out for suspicious emails
- 'From' addrsses can be spoofed
- To verify if it's from an employee, ask them via IM or in person
- Never click on any links in a mail you think may be phishing
- You are your greatest asset in the fight against phishing.

Employee training

- Face-to-face training where possible
- Make the content relatable and use examples of actual phishing emails your organisation has received
- Encourage positive security practices at home as well as the office
- Validate the effectiveness with phishing simulation before and after training.

Terms and conditions

- Make sure you understand what you are agreeing to
- Search for key words
- Check 'Terms of Service; Didn't Read' site to see if they summarised the service you are signing up to.

Encryption of data in transit and at rest

- Familiarise yourself with encryption
- Make sure data in transit is protected between your end user device and the service
- You should have sufficient confidence that storage media containing your data are protected from unauthorised access.

Responding to incidents

- Identify what kind of incidents can affect your organisation
- Create a plan to respond to incidents
- Identify who should be contacted when an incident occurs. These people should have the authority to make critical decisions.

Ethical use of data

- Don't discuss company information in public
- Don't look at information you shouldn't
- Identify what kind of data you need for business purposes
- Identify sensitive data and handle it accordingly
- Familiarise yourself with new regulation laws like GDPR (EU) and NDB (AU).

For further information visit
the ISC and MLA websites:
www.integritysystems.com.au
www.mla.com.au

Integrity Systems

red meat customer assurance

MEAT & LIVESTOCK AUSTRALIA