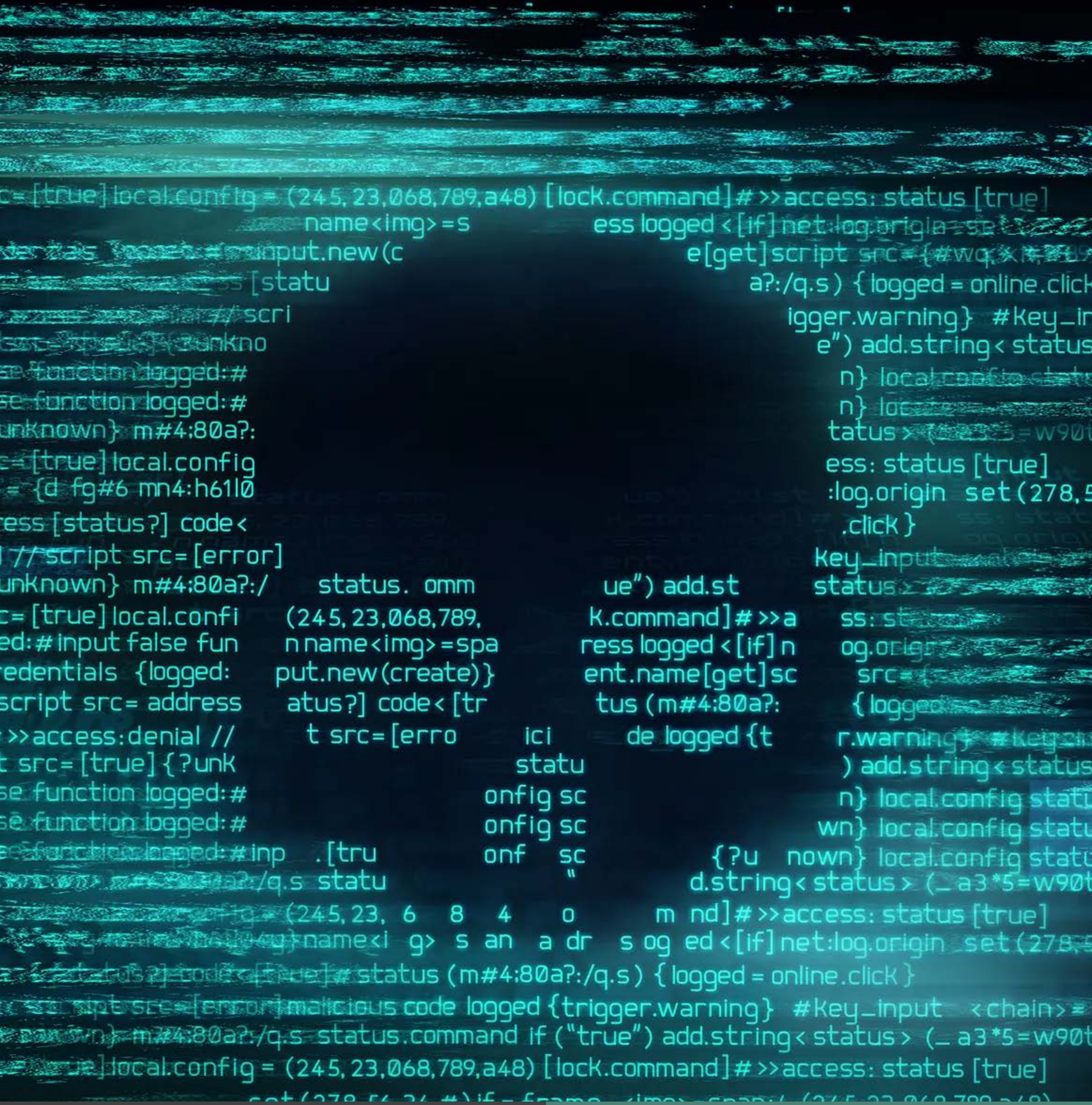


Cybersecurity Insights

VICTUAL
RETHINKING RISK AND INSURANCE

IN COLLABORATION WITH

tesserent

Staying Cyber-Safe

With cyber-crime currently believed to cost Australians more than $1 billion each year (1) and 65% of Australian businesses being interrupted due to a breach in 2020 (2), it's little wonder that businesses are becoming more alert to the risk of an attack. The Food and Beverage industry is vulnerable to exploitation through many aspects of business operations: agri-tech systems being targeted at the production stage, through to the vulnerability of systems that manage distribution, safe storage and delivery of goods, and eCommerce and email compromises at wholesale, retail or point of sale stages – any of which have the potential to significantly disrupt your business.

Cybersecurity is in simple terms, the application of technologies, processes and controls to help protect data, systems, networks and programs from unauthorised access and cyber-crime.

Typically, these attacks are aimed at accessing, changing or destroying data or extorting money from businesses. Criminals are increasingly finding innovative ways to penetrate through even the most guarded of businesses. Whilst it seems absurd now, the solution to some of the earliest cyber-crime was to shut down the entire internet. Evidently, this is no longer a solution, but it does serve to highlight the impact cyber-crime can have on a business, even more so in our sophisticated digital age.

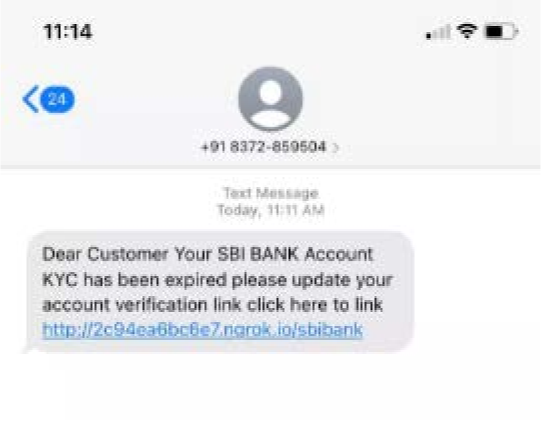
Over the past ten years, large, well organised cyber-attacks have presented a new challenge and businesses need to be vigilant about getting the basics right. Businesses should be proactively looking to prevent attacks and minimise their risk – it's not a case of if, it's a case of when an attack occurs.

A key reason why Food and Beverage companies have a greater cyber risk today, is largely due to their systems becoming more connected to traditional IT infrastructure. They're using data in smarter ways to track quality, make commercial decisions and operationally optimise their businesses.

In a recent ransomware attack JBS, one of the world's largest meat manufacturers was targeted, forcing it to temporarily shut operations and pay a ransom of $14.2 million, to end the five-day attack. The impact of this attack on the business was huge, not just financially but operationally and from a brand reputational perspective. This is not just an exposure for global giants this is equally relevant to small to medium businesses.

Whilst many businesses see cybersecurity solely as the domain and problem of the IT team, or their IT provider, the reality is that it’s the responsibility of management to ensure the right questions are being asked and they understand the key areas of risk, and whether these are being addressed.

Cybersecurity is everyone’s business; it only takes one weak link to allow criminals to penetrate through even the most innovative protections. It happens as quickly and easily as a team member clicking on an external, unverified link.



11:14

24

+91 8372-859504

Text Message
Today, 11:11 AM

Dear Customer Your SBI BANK Account KYC has been expired please update your account verification link click here to link http://2c94ea6bc6e7.ngrok.io/sbibank

Every organisation should ensure that the people, processes and technology all link seamlessly to create an effective defence against cyber-attacks and that preventative measures and risk management strategies are deployed, prior to an attack. There’s little to be gained from scrambling to react once systems have been breached.

CEO of cybersecurity provider Tesserent, Kurt Hansen says “The Food and Beverage and Grocery industries are no different from every other Australian business – cyber criminals are looking for entry points in the largest, and in the smallest operators. Every management team needs to work from the assumption that they will get attacked and review their controls accordingly. Third parties can be helpful in providing independent assessment and assistance.”

Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE CENTRE

Security Legislation Amendment (Critical Infrastructure) Bill 2020

Explanatory Document

Such is the extent of growth of cyber-crimes, The Security Legislation Amendment (Critical Infrastructure Bill) 2020 is currently making its way through parliament. It has the potential, if passed, to dramatically change the scope of security expectations for a range of industries, by uplifting the security and resilience of critical infrastructure. It aims to introduce greater checks and balances and provide greater protection for those industries deemed critical to our nation.

The Food and Grocery industry is one of the proposed sectors for inclusion, given the essential nature of the service they provide and the huge workforce they employ to keep the supply chain running smoothly. The proposed bill acknowledges that cyber warfare is an unfolding growth area, and is a proactive measure, representative of the evolving situation with cyber-attacks and crime.

What might inclusion of Food and Grocery on the list of critical infrastructure industries mean for your business? There may be greater reporting requirements to assure the government that you have cybersecurity measures in place, an obligation to report any security incidents and, in the event of major disruptions, the government may step in to assist.

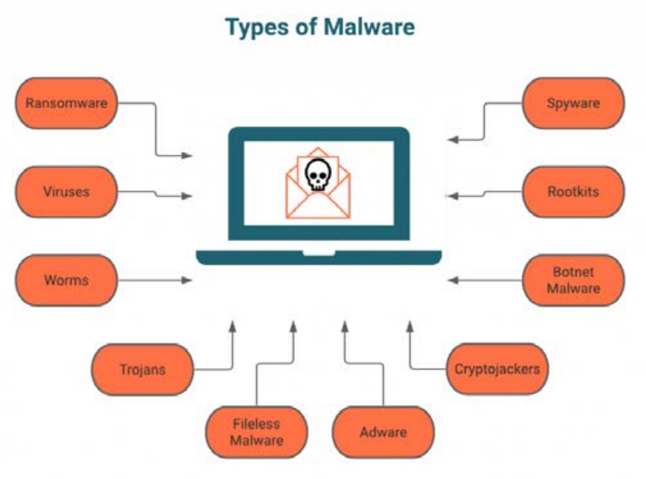
In short, being proactive about your cybersecurity is imperative.

Identifying key cyber threats

The impact of a cybersecurity attack can be devastating – it can shut down production, compromise customer data, force a business to stop trading and can ruin years of building a strong brand reputation. An Enterprise Risk Plan or Register will help identify the unique cybersecurity risks to individual businesses, but there are several ways criminals are commonly able to penetrate businesses. Some of the most common ways cyber-attacks take place (3) are:

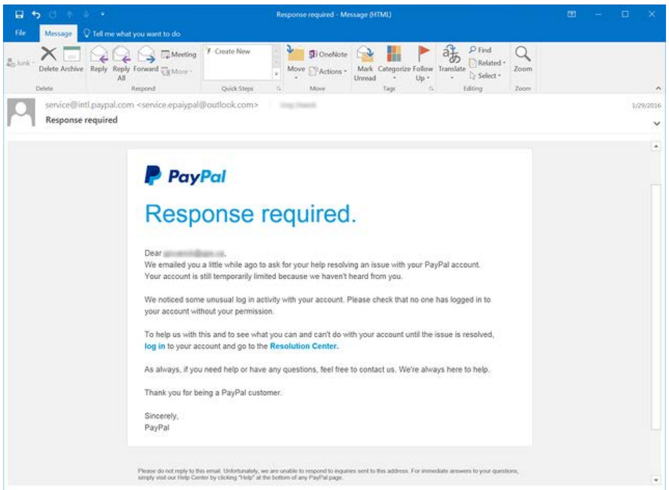
1 Malware

Malicious software (Malware) is software designed to cause harm. It typically gains access to important information such as passwords and can spy on a user's computer to help achieve the goal of theft or espionage. Criminals can be quietly in your network watching activity, waiting for an opportunity to execute fraud – for example through diverting invoices or payroll to a third party account.



2 Phishing

Scam e-mails (phishing) are trick e-mails designed to extract recipients out of money or data. As they often appear real, recipients in businesses frequently fall victim to clicking on links or verifying confidential data. They can have malware attachments, which when opened, infect the computer. It's easy to be tricked, especially with busy inboxes and external stakeholders.



service@intl.paypal.com <service.epaiypal@outlook.com> [redacted]

1/29/2016

Response required

PayPal

Response required.

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account.
Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

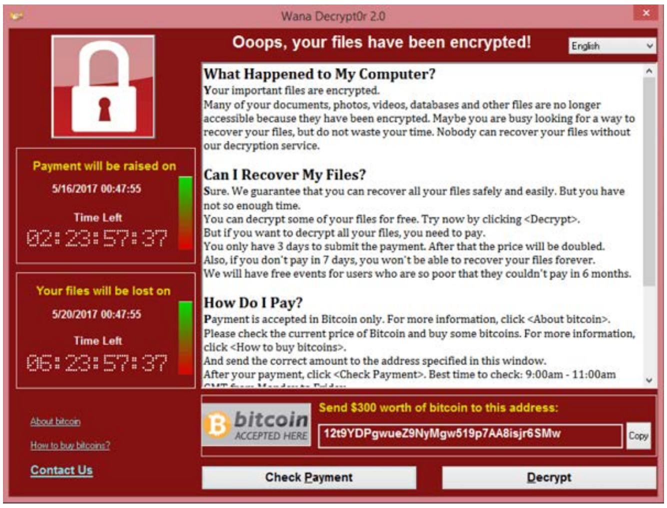
Thank you for being a PayPal customer.

Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

3 Ransomware

Ransomware is unfortunately a threat organisations of all sizes face. Normally carried out via a malicious e-mail link, the malware locks down the computer and files until a ransom is paid to restore access. Even then access may not be restored.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

No business is immune to an attack, but steps can be taken to mitigate the risk. Risk by its nature incorporates facing uncertainty in order to meet business objectives. In an online world with evolving technologies, this means that every business needs to take action to mitigate those risks which could impact upon performance, output or reputation. Even the largest businesses aren't immune to cyber-attack; Cadbury, based in Tasmania, recently got hacked, resulting in the production facility being shut for a few days, while they brought operations back online.

Setting up defenses against cyber-attack

As in many industries, the technology available in the food and beverage industry is quickly developing, most of which requires greater connectivity and use of the internet. Whilst fantastic for efficiency and productivity, this can present greater risks for cyber-attacks. Whether it's sophisticated technology to run production lines, or gathering private data about customers to stay connected to them, organisations have a responsibility to ensure they are protecting their customers, their staff and their business to the greatest extent they can.

There are a few key areas businesses should consider in their risk management plan, to proactively take steps to stay one step ahead of cyber-crime.

1 Multi-Factor Authentication

A security measure which requires two or more proofs of identity before allowing access. Whilst it can be frustrating to doubly authenticate when quick access is required, the multiple layers make it far more challenging for criminals to access your systems. It's a simple, effective way to verify that users are who they say they are. Typically, 2FA (Two factor Authentication) uses a username and password, combined with, for example, a code texted to a smartphone.

2 Cybersecurity awareness and training

Businesses, however large or small, should be alert to the unavoidable fact that one of the most common entry points into a business, is through their staff. It's the responsibility of everyone in the organisation to help protect the business. Setting up strong internal processes and training, will help provide another layer of defence with shared accountability. It's only too easy for a team member who hasn't had the benefit of security training, to inadvertently click on a link or open an unsolicited attachment. Seek expert help, to firstly understand your unique risks and only then can training modules or courses be devised to educate the team as to how to play their part in protecting the business – how to recognise an attack, avoid it and report it. Creating a positive culture around the risk of cybersecurity requires a deep understanding of the risks and how to manage them effectively.

3 Update Software

It sounds obvious, but maintaining the latest, safest version of software is critical to your cybersecurity defence. Sofware updates provide security protection and often enhanced features and efficiencies. Whilst larger organisations likely have systems and teams in place to review and update software versions, smaller organisations can be left vulnerable. Every Management team should be asking the right questions of their IT team, administrator or IT service provider to ensure the business is protected with updates and is not left vulnerable to attack via out of date software.

4 Data Backup

How many times have you worked on a document and panicked when you lost it, or your computer died? There are potentially hours wasted trying to recover it, or worse still rewrite it. Imagine if this happened to your entire business as a result of a ransomware attack and you lost access every bit of data ever saved or programmed. A backup is a digital copy of your business's most important information and enables a business to get back on its feet quicker if a cyber-attack occurs and information is lost or stolen. It also helps to manage the risk of meeting privacy and security obligations to customers and to any regulators. Best practice also dictates that these backups are stored in a way that is not connected to your systems – avoiding your backup also becoming corrupted.

5 Insuring for what might happen

Insurance can be complex at the best of times, particularly when taking out a cybersecurity policy, given the progressive nature of the industry and its technologies. Insurance companies prefer to insure businesses who understand their risks, and who can proactively show that they're taking steps to mitigate risks as much as possible, before taking out cyber insurance. They're a safer bet and less likely to claim, thanks to the due diligence they've put into their risk management and action plan. Businesses are vulnerable to not taking out the cover they require and instead settle for a blanket policy, which may not even cover major risk areas. Understanding insurance policies alone can be time consuming and ambiguous to the untrained eye. Purchasing insurance should be the final part of a thorough risk management approach, rather than a quick fix solution, which seeks to offset obvious cyber risks through insurance.

Taking proactive steps to prevent a cyber-attack, alongside creating a framework to help recovery if one does occur, are both critical business measures in today's world.

Whilst an IT team may take on the bulk of responsibility for many of the preventative measures listed above, it's the role of management to be the challengers over deficiencies in processes or policies, to ensure the business remains protected.

Managing risk, through the creation of an Enterprise Risk Register, helps to identify areas of the business most at risk of cyber-attack. Updating this should take place on a cyclical basis to help identify areas where expert help is required. Throughout this identification and assessment process, Management teams should keep returning focus to the potential of cyber-attacks as one of the risks in their business.

> **"Cyber is consistently in most risk mature Food and Beverage Organisations top 5 risks. Boards expect to see it there and will ask questions if it isn't. We know it's a risk, but the key question is what are you doing to manage the risk? "**
> **- Peter McGee**

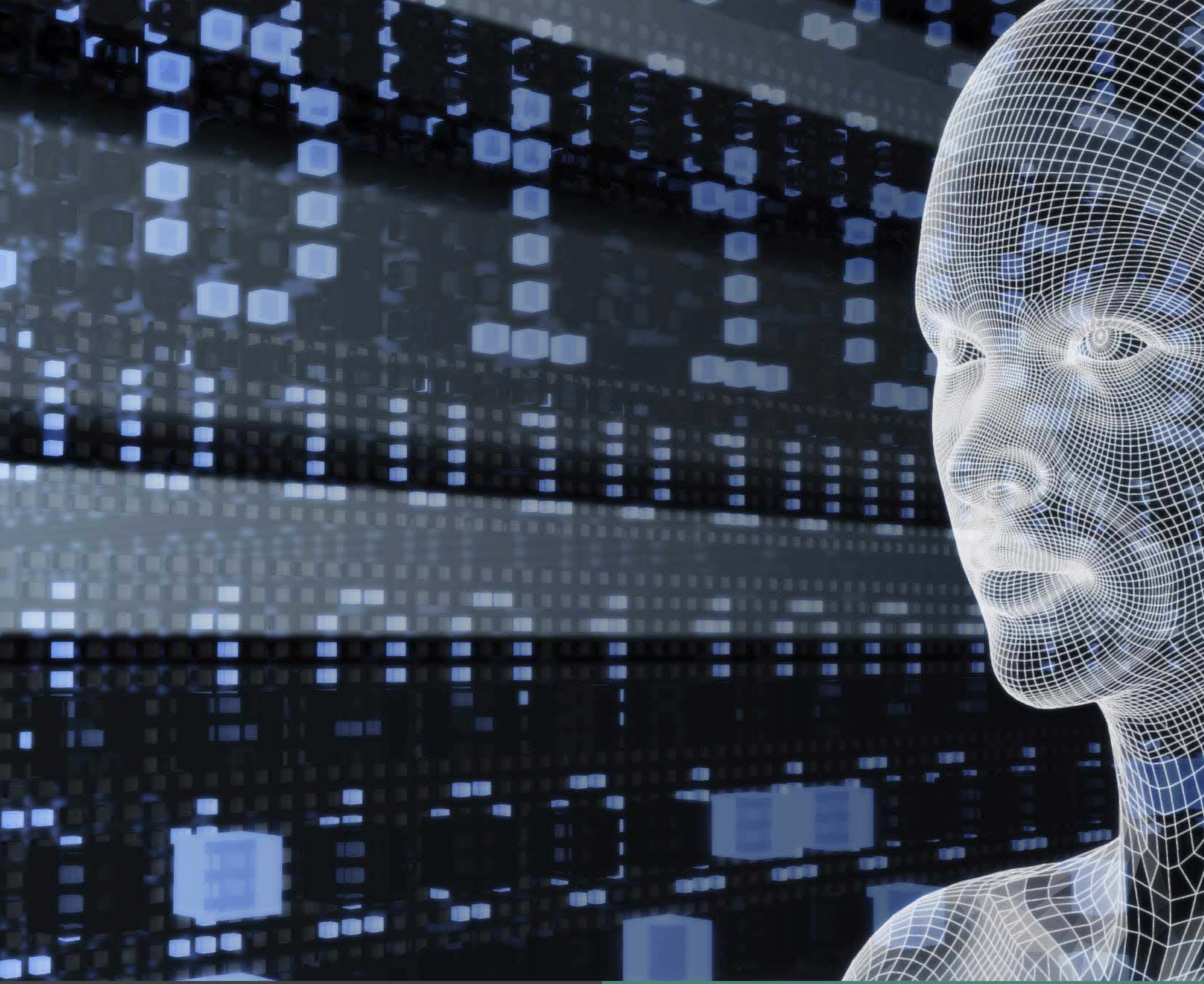
There are some key questions, to lead the conversation with IT teams or outsourced providers:

- **How long could we stay operational without access to our core systems?**
- **What damage would a major cyber incident have on our clients and suppliers?**
- **How do we backup our data, how often and where is it stored?**
- **Are all our core systems protected by multi-factor authentication? If not, why not?**
- **Have we tested our team in a phishing exercise? Do we know how they'd perform?**
- **How often are we patching our software?**

Whilst no fail-safe process exists to stop a cyber-attack, the key is to be prepared. By understanding the unique risks the business faces and then taking preventative action, leadership teams are avoiding a potentially devasting impact on business continuity. Cybersecurity attacks can be embarrassing and expensive, a fate every organisation seeks to avoid. Technical advances mean we're collecting data at an increasing rate and aggregating information in ways we never thought of before, meaning new opportunistic forms of attack are on the rise and every business, including in the Food and Beverage industry, should be ready for when, not if they arrive.

References

(1) KPMG/au/en/home/service – Cyber Solutions for the mid-market
(2) Telstra security Report 2019, Telstra
(3) Cyber.gov.au – Small Business Security Guide



Get In Touch

Victual are risk and insurance experts in the Food and Beverage industries. Risk is the effect of uncertainty on objectives and our purpose it to creating value and opportunity by rethinking and better managing risk.

Victual:
Address: Level 5, 77 Pacific Hwy, North Sydney NSW 2060
Phone: +61 (0) 2 9929 5052.
Email: enquiries@victual.com.au
Website: victual.com.au

Tesserent is the region's largest ASX-listed cybersecurity provider, Tesserent's Cyber 360 strategy simplifies cybersecurity for our clients, helping them achieve full end-to-end protection for their digital assets.

Tesserent Limited:
Address: Level 5, 990 Whitehorse Road Box Hill, VIC, 3128
Phone: +61 3 9880 5555
Email: info@tesserent.com
Website: tesserent.com

VICTUAL
RETHINKING RISK AND INSURANCE

tesserent

Victual proudly collaborating with Tesserent to produce this Cybersecurity Insight Paper.

RAI Commercial Pty Ltd, trading as Victual is a Corporate Authorised Representative (No 1254696) of RAIGLIS Pty Ltd AFSL 510066.