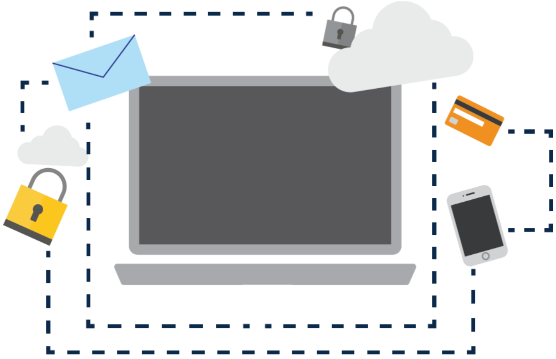
# 5 major cybersecurity threats facing your business in 2019.

BIZTECH

# Contents

The world of cybersecurity is constantly shifting, with new threats to enterprise security arising every day. This means businesses need to stay on top of the major issues facing their IT infrastructure and data.

We gathered expert views of Biztech's computing security team to determine the current lay of the land in Australian enterprise online security. We also investigated the five major cybersecurity threats that could face your business in 2019, offering crucial guidance on how you can negate these threats.



# Australian Cybersecurity in 2019

Cybersecurity defence in Australia is beginning to strengthen after years of comparative weakness on a global scale. The Office of the Australian Information Commissioner (OAIC:'s Notifiable Data Breach scheme was introduced in February 2018, with its effects now felt by enterprises nationwide. The policy has laid bare the extent of cybersecurity threats nationwide – nearly 250 breaches were reported to the OAIC between July and October 2018. Further, over half of these were identified as malicious or criminal attacks. This shows cyber threats are advancing more rapidly than cybersecurity defences.

Figures from a recent Thales Security Data Threat report shows that spending on IT security is on an upward trajectory. There was a five per cent increase in the number of organisations worldwide that raised their cybersecurity budget between December 2017–2018. However, this wasn't enough to reduce the frequency of breaches – Thales also shows more than a third of businesses saw an increase in cyber attacks in 2018.

This demonstrates how crucial it is that Australian organisations stay on top of emerging cybersecurity risks and long-standing issues that can affect you business.

# Threat 1: Cryptojacking

Since its introduction in 2009, cryptocurrency has become a key asset in online trading. Although its value has fluctuated, the appeal of a decentralised and encrypted currency for businesses online has remained high. Cryptocurrency is a key part of trading in Asian economies such as Japan and Korea – important markets for Australian enterprises.

However, as institutional capital flows into the cryptocurrency market, abuse of cryptomining resources is set to increase too. This was detailed in recent research from CYFIRMA, the cybersecurity division of global machine learning firm Antuit Analytics.

Unauthorised cryptomining, also known as cryptojacking, occurs when a hacker gains unauthorised background access to the use of someone else's computer or smart device. The cryptomining code generates cryptocurrency for the hacker while the host central processing unit deteriorates, causing slower performance. Unlike other malware, cryptojacking doesn't damage business infrastructure or target data.

However, slower computer performance can still incur significant time and expense costs as IT teams track down performance issues or replace the hardware components trying to tackle the problem.

Hackers have two primary ways to set up cryptomining software on a victim's computer. The first requires phishing emails that trick users into loading cryptomining code onto their device once they open the message and follow a malicious hyperlink. The second attaches a cyber script to a website or advertisement. Once victims visit the website or the infected ad pops up in their browsers, the script automatically executes.

This malware is becoming popular among hackers, with cybersecurity firm Symantec claiming just under 5 million cryptojacking events were blocked in July 2018 alone.

## The Solution

**1)** Incorporate cryptojacking prevention into your security awareness training, focusing on identifying phishing attempts to load scripts onto users' computers.

**2)** Regularly update your web filtering tools and track web pages that deliver cryptojacking scripts, making sure your users are blocked from access to malicious sites.

**3)** Use endpoint protection from a vendor capable of detecting crypto miner activity.

## Threat 2: Insider Threats

A staggering 37 per cent of OAIC breach notifications received last year were down to human error. Australian businesses simply cannot afford to overlook internal risks when building more resilient enterprise cybersecurity infrastructure. This sentiment is echoed in Thales' Data Threat report – more than half of respondents considered privileged user access to an organisation's data to be the most likely breach point, ranked 9 per cent ahead of aggressive cyber attacks or malware.

Privileged users are often the target of phishing emails and spam as these individuals have unfettered access to a business' sensitive data. If an executive level employee opens a link to these dangerous software threats, no amount of external cybersecurity defences can help.

## The Solution

Here are a few techniques that can reduce the risk of one of your employees opening the door to a major cybersecurity threat:

**1)** Introduce mandatory cyber safety training for all employees, especially those with privileged access. It will help to have your whole business looking out for cyber threats.

**2)** Restructure internal access systems. Rethinking what data employees need in their roles usually leads to tightened security around sensitive company information.

**3)** Develop consistent incident handling procedures. This ensures all individuals involved learn what mistakes were made and what should be done differently in the future.

## Threat 3: AI Security

The long-awaited promise of commercially available Artificial Intelligence (AI) that can aid business' data collation and automation may present a double-edged sword when it comes to cybersecurity. Hackers and cyber criminals can now access AI and machine learning solutions to automate bot or malware delivery to multiple servers simultaneously.

AI can also help malicious online attacks on data security, allowing hackers to probe a business' security infrastructure with coordinated attacks. Concern around AI-powered cyber attacks is acute in businesses nationwide and globally. Thales claims 43 per cent of cybersecurity report respondents felt misuse of AI will lead to an increase in the frequency of data breaches in the future.

But what is equally worrying for Australian businesses is over reliance on AI security infrastructure as a comprehensive solution for addressing commercial cybersecurity attacks. Cisco's Security Capabilities Benchmark Study shows more than 70 per cent of mid-sized businesses worldwide are reliant on AI for their operations – including security.

Not only are AI security features exposed to misuse by sophisticated cyber hacks, the online software also lacks the nuanced understanding of human behaviour that other humans do. In other words, an expert IT professional can often identify and respond to hacker behaviour more effectively than a cybersecurity infrastructure based solely on AI.

## The Solution

AI security is certainly a useful asset for Australian businesses – but expert IT security providers should remain a valuable part of an overall cybersecurity defence strategy. This can be done through a periodic security architecture review or firewall audit.

## Threat 4: Outdated Processes

Less than half of global businesses agreed that they regularly and strategically review and improve security practices, according to Cisco's security benchmark study. This shows apathy and adherence to outdated security processes has as much to do with costly data breaches as any criminal activity. Passivity in reviewing outdated security protocols even extends to expert computing workers. Research from security software company Cyberark shows nearly half of IT security professionals worldwide rarely change their security strategy substantially – even after experiencing a cyber attack.

Cyber threats are constantly evolving as new applications and technologies become commercially available. This means any security infrastructure that is proverbially standing still is in fact falling behind, and is unlikely to be adaptive enough to protect your business from the cybersecurity issues potentially awaiting in 2019.

## The Solution

It isn’t difficult to internally review your enterprise’s security processes through:

Firewall Auditing

Penetration Testing

Web Application Analaysis

Analysing these crucial factors can lead to surprising revelations about what your business is or isn’t prepared for. This process can be managed by an external security provider should you want an expert outside opinion on your essential cybersecurity.

```
<head>
  <!--meta-->
  <title></title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0,
  <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">
  <link rel="icon" href="/favicon.ico" type="image/x-icon">
  <!--css-->
  <link type="text/css" rel="stylesheet" href="css/materialize.min.css"
  <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/font-awesome/
  <link rel="stylesheet" href="/css/animate.css">
  <link rel="stylesheet" href="css/theme.css">
</head>
<body>
  <!-- banner-->
  <div class="banner">
  <nav class="nav">
    <div class="nav-wrapper">
      <div class="container">
        <a href="#" class="brand-logo hide-on-med-and-up"><b><span style="font-weight
      </div>
    </div>
  </nav>
```

## Threat 5: Lack of Cyber Expertise

A final major issue facing Australian enterprises is the ongoing lack of cybersecurity experts to meet the increasing demand. This affects businesses of all sizes and spanning multiple industries, and also isn't isolated to the national market. Cisco's 2018 security benchmark report shows 41 per cent of global respondents claimed they lacked the internal expertise to deal with cybersecurity threats. This means organisations are inherently on the back foot in dealing with online risks that can compromise operations.

This issue is emphasised by Cyberark research showing one in two IT security professionals admit customers' privacy is at risk because their data is not secured beyond legal requirements. The data protection obligations in the federal Privacy Act 1988, while covering the basics, doesn't go far enough to guarantee the safety of consumer and operational information.

## The Solution

Sourcing the expertise to deal with the cybersecurity threats facing Australian businesses poses two options; in-house recruitment or partnering with external services. Competition for cybersecurity personnel remains tough , with expanding firms and new businesses all competing for a limited pool of professional. External cybersecurity providers can provide a suite of services, offering your business the exact support it needs.

# What Biztech offers

We provide a range of managed IT security services to clients across NSW and ACT, ensuring all systems and enterprise data are secure. We work with your IT team to review your current infrastructure and identify areas that may be exposed to major cyber threats.

**We offer the following solutions to help reinforce your business' online defence:**

- Firewall Audit
- Web Application and Email Threat Analysis
- Penetration Testing
- Security Architecture Review
- Comprehensive Internal and External Vulnerability Assessment

Our skillful team of computing professionals and cybersecurity experts implement custom IT security solutions to address ever-changing online threats. To get the process of securing your business's proprietary data underway, **reach out to Biztech today.**

# Contact Us

☎ (02) 6176 3380

✉ sales@biztech.com.au

🌐 biztech.com.au

## Canberra Office

☎ (02)  61763380

📍 Unit 14, 41–45, Tennant St, Fyswick, ACT 2609

## Sydney Office

☎ (02) 8355 4300

📍 2/1C Grand Ave, Rosehill, NSW 2142

BIZTECH