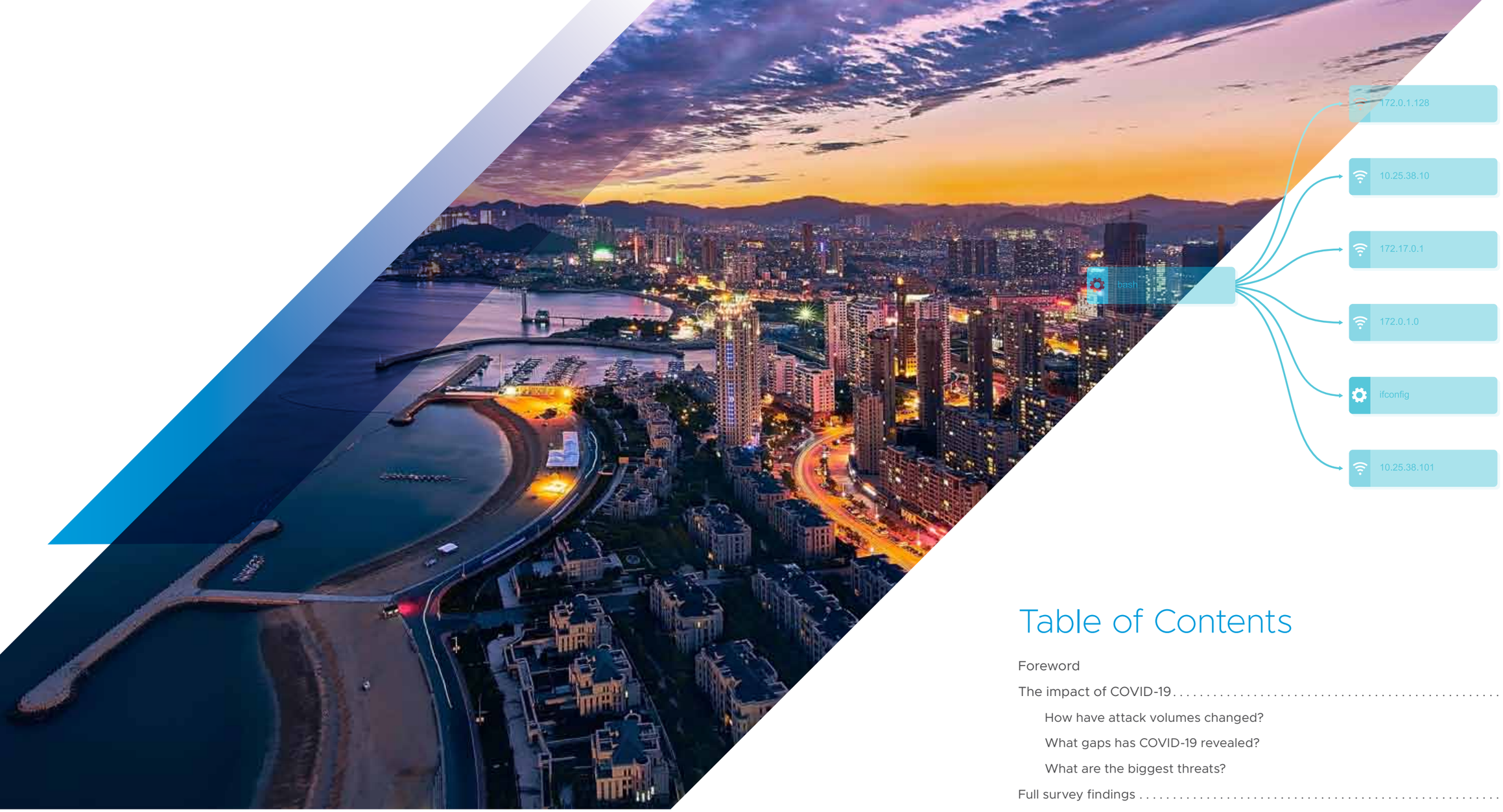
vmware Carbon Black

Australia Threat Report

Extended enterprise under threat

June 2020



Introduction

This research was conducted to understand the challenges and issues facing Australian businesses when it comes to escalating cyberattacks. It identifies trends in hacking and malicious attacks and the financial and reputational impact any breaches have had. It examines Australian organizations' plans for securing new technology, for adopting cybersecurity frameworks and the complexity of the current cybersecurity management environment.

Table of Contents

METHODOLOGY

VMware Carbon Black commissioned a survey, undertaken by an independent research organization, Opinion Matters, in March 2020. 250 Australian CIOs, CTOs and CISOs were surveyed from companies in a range of industries including: financial, healthcare, government and local authority, retail, manufacturing and engineering, food and beverage, utilities, professional services and media and entertainment. This is the third Australian Threat Report from VMware Carbon Black, building on the previous surveys, which were undertaken in February 2019 and October 2019. This forms part of a global research project across multiple countries, including: Australia, Canada, France, Germany, Italy, Japan, Netherlands, Nordics, Singapore, Spain, the UK and the US.

THE 2020 AUSTRALIA CYBERATTACK LANDSCAPE

Rick McElroy
Cyber Security Strategist, VMware Carbon Black

Foreword

The Australian cyber threat landscape has escalated. In this, our third Australia threat report, we find that attack frequency has reached unprecedented levels; 94% of security professionals said the volume of attacks they faced has increased. Attackers are employing a more diverse range of tactics and techniques than ever before as they bid to extort, disrupt and infiltrate organizations.

As a result, breaches are inevitable. Our research found that:

96% of Australian organizations have suffered a data breach as a result of a cyberattack in the past 12 months and the average organization has experienced 2 breaches.

The increase in attack volume has jumped from 90% in October 2019 and 81% in February 2019, demonstrating a clear upward trend. At the same time, however, the number of breaches has dropped once more, down from 3.78 in October 2019.

The considerable leap in attack frequency and sustained increase in sophistication revealed in this iteration of the report shows that, however fast Australian businesses may be adapting to the intensifying environment, the cyber threat landscape is evolving faster. 88% of security professionals say attacks have become more sophisticated, 16% of those say they have become significantly more advanced. This confirms what VMware Carbon Black Threat Analysis Unit research has been finding: adversaries are adopting more advanced tactics as the commoditization of malware is making more sophisticated attack techniques available to a bigger cohort of cybercriminals. It's not surprising that custom malware is the most commonly seen attack type.

94%

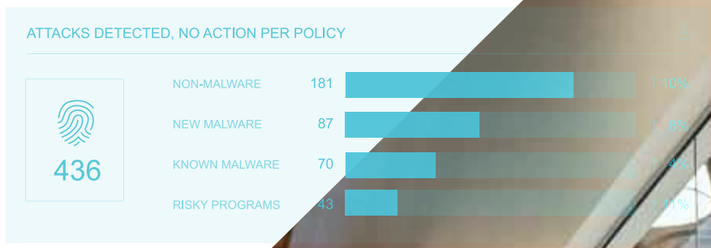
of security professionals said the volume of attacks they faced has increased

96%

of Australian organizations have suffered a data breach as a result of a cyberattack in the past 12 months

88%

of security professionals say attacks have become more sophisticated, 16% of those say they have become significantly more advanced



11%

Island hopping, despite only featuring in a small percentage of attacks experienced, was the fourth most common cause of breaches, at the root of 11%.

96%

of survey participants anticipated an increase in spend

43%

say they will need to increase security spending and controls

Third Party Breach Risk On The Rise

In addition to the general escalation in intensity, this report reveals a shift in the causes of successful breaches. OS vulnerabilities and third party application compromise were the most common cause of breaches, affecting 18% in each case. Island hopping, despite only featuring in a small percentage of attacks experienced, was the fourth most common cause of breaches, at the root of 11%. Furthermore, 6% of breached businesses had been compromised via their supply chain. Clearly, the extended enterprise ecosystem is generating considerable security concerns.

Reputations Are In The Firing Line

As public awareness of data protection rights has grown, and regulatory fines have hit the headlines, so the impact of breaches has continued to rise, with an increasing proportion of respondents reporting severe reputational damage.

Budgets Rise Again But Will Spending Be Strategic Or Tactical?

Australian security professionals are responding to the uptick in cyber threats by boosting cyber defense spending. 96% plan to increase budgets, which is the same as our last report in October 2019 and an increase on the February 2019 survey which was 90%.

Where that spend will be directed is an interesting question. Respondents told us unequivocally that threat hunting is paying dividends and increasingly being recognised for its value in identifying malicious actors already in the system, so it seems likely this investment will continue, but what of emerging risks?

In our October 2019 survey, 98% of respondents said they had security concerns around the implementation and management of digital transformation and 5G. But, when it comes to the crunch, opinion is split on the need for security spending. 43% say they will need to increase security spending and controls, while 55% won't be focusing their budgetary increases on securing 5G.

A Complex, Crowded, Multi-Technology Environment

Perhaps this is because they're already supporting multiple security technologies. Respondents are already operating an average of more than seven different consoles or agents to manage their security program. This indicates a security environment that has evolved reactively as security tools have been bolted on to tackle emerging threats, not built-in. This has resulted in siloed, hard-to-manage environments that hand the advantage to attackers from the start; evidence shows that attackers have the upper hand when security is not an intrinsic feature of the environment. As the cyber threat landscape reaches saturation, it is time for rationalization, strategic thinking and clarity over security deployment.

Split Over The Value Of Security Frameworks

Visibility and validation of security posture can be significantly enhanced by the application of the MITRE ATT&CK® framework, but it seems the jury is still split on the relevance and value of this approach. 87% are aware of it, but only 58% plan to use it to validate security posture, demonstrating that there is still work do to establish this framework as the gold standard among enterprises.

7

Respondents are using an average of more than seven different consoles or agents to manage their security program.

87% vs 58%

87% are aware of the MITRE ATT&CK® framework but only 58% plan to use it

The Impact Of COVID-19

When we conducted our primary research for this edition of the VMware Carbon Black threat report, the impact of COVID-19 was only just beginning to reverberate across the globe. In the interim period, as we analysed the results, it became clear that the rapid escalation of the situation meant it would be disingenuous to present the research without attempting to include a measure of its effect on cybersecurity and the cyber threat environment. Therefore, we went back to our CISOs with supplementary questions to understand the immediate impact and what cybersecurity professionals are seeing on the ground as they work to adapt to a fast-changing scenario. We are grateful to all those who took time to respond during this critical period and believe that the information obtained will prove valuable in informing the cybersecurity response going forward.

We hope you find our third Australian Threat Report useful and informative.

COVID-19 Supplemental Research Findings

1002 global respondents from March to April 2020 including UK, USA, Singapore and Italy

The sudden global shift to homeworking due to COVID-19 has both increased cyberattack activity and exposed some key areas for security teams to address and learn from going forward. Our COVID-19 research has found that the vast majority are facing an uptick in cyberattack volumes due to employees working from home, and COVID-19 related malware is making its malicious presence felt.

The predominant gaps identified in disaster recovery planning revolve around communication with external parties such as customers, prospects and suppliers, as well as in IT operations themselves and challenges around enabling the remote workforce and communicating with employees.

Those who had delayed implementing multi-factor authentication face challenges, as inability to institute it is now the biggest threat faced by more than a quarter of our respondents worldwide. As we adjust to a new normal of increased remote working and its associated threats, IT teams will face the challenge of extending security protection into employees' homes.

"Attackers are employing a more diverse range of tactics and techniques than ever before as they bid to extort, disrupt and infiltrate organizations."

Has The Overall Number Of Typical Cyberattacks On Your System Changed As A Result Of More Employees Working From Home?

A staggering 91% of all global respondents stated that they had seen an increase in overall cyberattacks as a result of employees working from home.

7% of respondents reported that these had increased by between 50 and 100%. Just under a quarter (24%) recounted that attack volumes had gone up by between 25 and 49%.

Three people out of 1002 stated that they did not have more of their employees working from home than usual because of COVID-19.

Out of the four countries surveyed **Singapore** respondents were most likely to report increases in attacks, with 93% saying this, followed by the **UK** with 92%, then **Italy** 90.5% and lastly the **USA** with 88%. That said Italy witnessed the highest percentage of attack increases (14%) in the between 50 and 100% scale, compared to the **UK** which experienced the lowest in this category (50 to 100%) with 2%. The US was the highest in the 25-49% category, with 28% of respondents saying they had seen attack increases on this scale.

14.5% of **media and entertainment** companies witnessed attack increases of between 50 and 100%. **Retail** was also high at 13% for this category. 45% of those in retail also reported increases between 25 and 49%. This was followed by **manufacturing and engineering** with 33%.

41% of companies with **501-1000** employees reported high attack increases of between 25 to 100%.

Just over a quarter (26%) of those with IT team sizes of **more than 100** witnessed increases between 50 and 100%.

18% of those with IT team sizes between **41-50** conveyed increases of between 50 and 100%.

91%

of all global respondents stated that they had seen an increase in overall cyberattacks as a result of employees working from home

NEARLY HALF

(48%) of global respondents surveyed reported very significant gaps around communication with their external parties

What Gaps If Any Did COVID-19 Reveal In Your Company Disaster Recovery Planning And How Significant Were Those Gaps In Terms Of The Effectiveness Of Your Disaster Recovery Plan For The Situation?

Nearly half (48%) of global respondents surveyed reported very significant gaps around communication with their external parties including customers, prospects and partners. Overall, 84% reported gaps ranging from severe to slight in **communication with external parties.**

Over a third (35%) reported very significant gaps in disaster recovering planning in **IT operations** including hardware and software roll outs. Overall, 87% reported gaps, be that severe or slight, in **IT operations.**

Just under a third (32%) of global respondents found very significant gaps in their **visibility into cybersecurity threats** with an additional 38% stating that there were slight gaps.

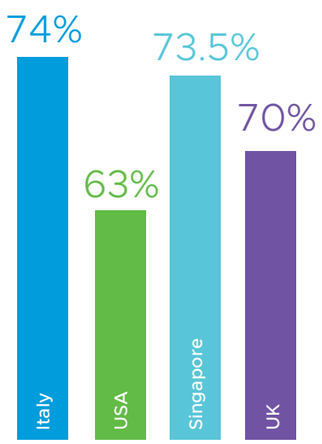
In terms of **enabling a remote work force,** severe and significant gaps were felt by over a quarter (28%) of survey respondents, and overall, 85% of respondents felt that there were gaps.

Over a quarter (27.5%) admitted to severe cracks in dealing with the situation in terms of **communication with employees** and overall, 78.2% of respondents stated that these were either slight or very significant.

In terms of **recovery planning** one third (33%) of respondents identified very significant gaps and 88% highlighted disparities of some kind.

Five respondents out of 1002 opted out from answering this question stating that COVID-19 had not revealed any gaps in their company's disaster recovery planning.

Italy figures were higher than the other three countries in identifying very significant gaps in IT operations (41%), enabling visibility into cybersecurity threats (38%) and remote workforce (37%). The **USA** had the highest very significant gap impact (30%) in communication with employees, whereas **Singapore** scored highest (52%) in communicating with external parties. Both Italy and the **UK** reported the highest very significant gaps in recovery planning with 36% respectively.



Had COVID-19 revealed gaps in visibility into cyber threats?

29%

Over a quarter of global respondents (29%) recounted the inability to institute multi-factor authentication as the biggest threat to their company

Which Of The Following Threats Associated With COVID-19 Have Been The Biggest Threat To Your Company So Far?

Over a quarter of global respondents (29%) recounted the **inability to institute multi-factor authentication** as the biggest threat to their company. Second to this was **COVID-19 related malware** with 15.5% and third was the **inability to roll out timely software patches** (13%). 10% cited **phishing,** 6% stated **spear phishing, IoT exposure** and **remote access inefficiencies.** Other notable threats were **masquerading** (4.5%), **ransomware** (4%) and **social engineering** (4%).

The **inability to institute multi-factor authentication** was most keenly felt by **Singapore** and the **USA** with 32% respectively. **COVID-19 related malware** was highest in **Italy** (21%) closely followed by the **UK** (20%). While **phishing** emails were highest in **Singapore** (12%).

The **inability to institute multi-factor authentication** was the biggest threat for financial services organizations with 50% claiming this to be the case. **COVID-19 related malware** impacted heavily on **food and beverage** (49%), and **professional services** (30%). **Media and entertainment** were most susceptible to **phishing** emails (29%).

COVID-19 related malware impacted more on small sized organizations, particularly those with 50-250 employees (43%). For company sizes of 251-500 the biggest impact was the **inability to institute multi-factor authentication** (46%).

92%

The highest increase in threat changes during COVID-19 was with COVID-19 related malware, which saw overall threat change increases of 92%

How Have Any Of The Threats Changed During COVID-19 And To What Extent?

The highest increase in threat changes during COVID-19 was with **COVID-19 related malware,** which saw overall threat change increases of 92%, and 53% of these increases were in the 51 to over 100% categories. Second was **IoT exposure,** with 89% reported threat change increases and 21% of these were in the 51 to over 100% categories. In third place was **phishing emails** with 89% and 24.5% of these were in the 51 to over 100% categories. **Spear phishing** was also significantly high with 88% overall increases in threat changes and just under a quarter (23%) of these were also in the 51 to over 100% category.

Out of the four countries Italy had the highest overall **COVID-19 related malware** increase of 96% with a staggering 70% reporting increases in the 51% to over 100% categories. This was followed by the UK with 93% overall and 54% in the 51% to over 100% categories.

A new family of ransomware known as Coronavirus has recently been found and there has been an upward trend in ransomware. Sadly, there has never been a better time for the threat actors to create and distribute **ransomware.** However, **ransomware** was lower than other categories with respondents reporting 67% in overall threat change increases.

29% of global respondents recounted the **inability to institute multi-factor authentication** as the biggest threat to their company so far. In terms of how threats have changed during COVID-19, this was relatively high with 87% reporting overall threat change increases and 24% of the respondents reporting increases between 51 and more than 100%.

Full Survey Findings

Have You Seen An Increase In Cyberattacks On Your Company In The Last 12 Months? If So, By How Much?

A staggering 94% of Australian organizations have seen an increase in the number of cyberattacks on their company in the last twelve months. This is a considerable increase from 90% in the October 2019 report and 81% in the previous February, making it the highest increase in attack frequency we have ever witnessed.

Respondents reported an average increase in frequency of 72%, and 55% overall said there had been an increase in attack volumes of between 51% and 300% - this is a jump from the last report where only 24% reported increases of this magnitude.

40% of respondents in the **healthcare** sector and 53% of respondents in **manufacturing and engineering** had seen a 51-100% increase.

Companies in the **2001-5000 employee** category saw an above average increase in attack volumes, reporting increases of 81%.

Have Cyberattacks On Your Company Become More Or Less Sophisticated In The Last 12 Months?

88% of respondents say attacks have grown more sophisticated over the last twelve months – a figure that has held steady from October and February 2019. Of these, 16% said they had become **significantly** more sophisticated, and 43% said they were **moderately** more sophisticated.

Respondents from the **financial services** sector are facing an above average increase in attack sophistication – 40% say attacks have grown **significantly** more sophisticated.

94%

of Australian organizations have seen an increase in the number of cyberattacks on their company in the last twelve months.

88%

of respondents say attacks have grown more sophisticated

16%

of respondents say attacks have grown significantly more sophisticated

96% of the CISO/CIOs that took part in our research said they had suffered a breach following a cyber attack in the past 12 months.

Custom malware tops the table again, with a 19% of respondents seeing it as the most frequent attack type, the same percentage as last time.

What Has Been The Most Prolific (i.e. Most Frequent) Type Of Cyberattack Your Company Has Experienced In The Last 12 Months?

Custom malware tops the table again, with a 19% of respondents seeing it as the most frequent attack type, the same percentage as last time. **Google drive™ attacks** were again the second most commonly experienced attack type, at 12%, and SSH attacks were third, with 10% of respondents finding them the most frequent attack type.

The frequency of **process hollowing** attacks has more than doubled from 4% to 10% since October 2019, indicating a growing attacker focus on gaining undetected access to networks. Also appearing on the attack radar is **island hopping,** with 4% saying this is the most common attack type they have faced. While this figure may seem low, these types of attacks are proving effective, as later analysis shows.

Financial services are at the mercy of custom malware with 43% saying this was the most frequently experienced attack type (compared with an average of 19%).

Healthcare sector company respondents were proportionally more affected by process hollowing attacks, with 19% experiencing it most frequently compared with an average of 10%.

How Often Has Your Company Been Breached By A Cyberattack In The Last 12 Months?

96% of the CISO/CIOs that took part in our research said they had suffered a breach following a cyberattack in the past 12 months. This figure has dropped marginally from 97% who said they had been breached in October 2019 but remains up on the 89% who said the same in February 2019.

The average number of breaches suffered by organizations is 2.05, which is a drop from 3.78 in October 2019 and 4.28 in February 2019, showing that Australian organizations are heading in the right direction. The largest group of respondents (50%) said they had suffered one breach, while just over a quarter (26%) said they had suffered two.

Government and local authority organizations reported the highest average number of breaches at 2.54.

Almost one third (30%) of **media and entertainment** companies had suffered three or more breaches.

OS Vulnerabilities

The top cause of breaches was identified as OS Vulnerabilities (18%)

11%

despite only being cited by 4% of respondents as the most common attack type experienced, island hopping was the cause of 11% of breaches

43%

of respondents said they had suffered negative reputational impact as a result of a breach,

What Was The Prime Cause Of These Breaches?

The joint top cause of breaches was identified as OS vulnerabilities (18%) as hackers take advantage of poor patching hygiene. Sharing the top spot was third party application breaches (18%), with web application attacks next, causing 13% of breaches.

Travel and Transport (30%), **financial services** (26%), **healthcare** (22%) and **food and beverage** (22%) companies are most affected by OS vulnerability breaches.

Interestingly, despite only being cited by 4% of respondents as the most common attack type experienced, **island hopping** was the cause of 11% of breaches. This indicates the vulnerability of extended enterprises to attacks originating in vendor organizations. Separate VMware Carbon Black research among incident response professionals found that island hopping was a feature in 41% of the breach attempts they encountered. Island hopping is more of an issue in sectors with large supplier ecosystems, such as the **government and local authority** sector (15%), **food and beverage** industry (15%) and **manufacturing and engineering** (14%).

Third party application breaches have also jumped, to 18% of successful breaches compared with 9% in the previous report, underlining the importance of monitoring third party risk.

Surprisingly, **phishing attacks** dropped dramatically as a cause of successful breaches. In October 2019 phishing was the cause of 27% of successful breaches, but this has dropped to just 7%. The same was true of **ransomware,** which dropped from 17% to 7%.

What Were The Consequences Of These Breaches From Financial And Reputational Perspectives To Your Company?

The percentage of respondents reporting financial impact following a breach has dropped from 56.5% to 41% stating that there had been a negative effect. However, a far higher proportion than previously said that they had suffered reputational impact following a breach – nine in ten had seen damage to their corporate image, up from threequarters last time. One fifth said the reputational impact had been severe.

61.5% of **Government and local authority** respondents said they had suffered financial impact due to a breach and 8% said it had been severe. **Food and beverage** companies were also more likely to have suffered financial damage, with 11% saying it was severe.

Financial services companies saw the most reputation effect from breaches, with 43% reporting severe reputational damage.

In The Last 12 Months Did Your Company's Threat Hunting Achieve A Goal Of Strengthening Its Defenses Against Cyberattack And Did The Threat Hunting Find Malicious Cyberattack Activity You Would Not Have Ordinarily Found?

Threat hunting is becoming ubiquitous, with 92% of respondents using it as part of their cybersecurity strategy. It is also proving effective; overall 91% said it had strengthened their company's defenses, with one third saying it significantly strengthened them.

46% of respondents said they had found **significant** evidence of malicious activity thanks to their threat hunting program.

Media and entertainment and **food and beverage** companies have been particularly successful at uncovering malicious activity, with more than half finding significant evidence of attackers in their network.

46%
The percentage finding significant evidence of malicious activity was 46%

92%
of respondents are using threat hunting as part of their cybersecurity strategy

90%
of CISO/CIOs surveyed said they plan to increase budget spend

How Much Are You Planning To Increase Your Budget Spend On Cyber Defense In The Next 12 Months?

Threat hunting is becoming ubiquitous, with 92% of respondents using it as part of their cybersecurity strategy. It is also proving effective; overall 91% said it had strengthened their company's defenses, with one third saying it significantly strengthened them.

46% of respondents said they had found **significant** evidence of malicious activity thanks to their threat hunting program.

Media and entertainment and **food and beverage** companies have been particularly successful at uncovering malicious activity, with more than half finding significant evidence of attackers in their network.

98%
CISO/CIO we surveyed said they were planning to adopt 5G over the coming 12 months

7.59
is average number of technologies deployed

87%
were familiar with the MITRE ATT&CK® framework

In The Next 6 To 12 Months Are You Adopting 5G And Do You Have To Increase Security Spend And Controls To Adopt It (i.e. Are You Making Net New Investment Based On This New Risk)?

98% of the CISO/CIOs we surveyed said they were planning to adopt 5G over the coming 12 months, with 75% expecting to do so in the next six months. They are divided on the security implications. 43% say they will need to increase security spend to manage adoption, while 55% don't believe they will need to invest.

Financial services organizations are most likely to say they are adopting 5G in next six months and will be investing in related security and controls (65%). 81% of **government and local authority** organizations believe they will not need to increase spend due to 5G adoption.

How Many Different Security Technologies Do You Have In Place To Manage Your Security Program (i.e. Multiple Consoles, Multiple Agents, Multiple Tools)?

69% of companies have between 5 and 10 different technologies deployed to manage their security program. 11% have 11-25 different technologies.

The average number of technologies deployed is 7.59 – this rises to 8.84 in **financial services.** IT teams of more than 100 people are using more tools on average – 10.13 compared with an average of 7.59.

Are You Aware Of And Do You Plan To Use The MITRE ATT&CK® Framework To Validate Your Security Posture?

Awareness of the MITRE ATT&CK® framework is high in Australia – 87% know what it is - but respondents are split over whether to adopt it. 28% are aware of it but have no plans to implement it, while 58% are aware and plan to use it.

The **food and beverage** sector is the most positive about the framework, with 75% aware of it and planning to use it, closely followed by **healthcare** organizations (72.5%). The most sceptical are respondents from the **financial services** sector, where 51% say they are aware of it but don't plan to use it.

Over The Past 12 Months Which, If Any, Of The Categories Below Have Required Either An Upward Or Downward Investment (I.E. Re-Prioritization Of Budget) (Tick All That Apply)

Workload/applications lead the field at 56%, followed by **networks** at 54%, **then endpoints** and **mobiles,** both at 44%.

Workload/applications have caused more reprioritization in **media and entertainment** and **government and local authority** organizations, with 74% and 65% having to take action respectively.

Which Of The Following, If Any, Is The Biggest Breach Risk In Your Security Program?

Workload/applications is seen as the biggest risk, cited by 40% of respondents, followed by **network,** identified by almost a quarter (24%) and **mobile devices,** also at 24% of respondents. **Endpoints** such as laptops and desktops co**me in at 9%.**

Manufacturing and engineering respondents see higher than average risk from workload/applications (53%), as does **professional services (53%)**.

54% of **financial services** organizations see the biggest breach risk as the network, as do companies of between 501-1000 employees (41.5%)