Carbon Black. AUSTRALIA

GLOBAL THREAT REPORT SERIES

DEFENDER POWER ON THE RISE

This research was conducted to understand the challenges and issues facing businesses in Australia when it comes to escalating cyberattacks. Its purpose is to identify trends in hacking and malicious attacks and the financial and reputational impact any breaches have had on organisations. It examines Australian organisations' approach to strengthening defences, ensuring confidence in their abilities to repel attacks and addressing concerns over the skills gap.

OCTOBER 2019

Report Survey Methodology

Carbon Black commissioned a survey, undertaken by an independent research organisation, Opinion Matters in August 2019. 251 Australian CIOs, CTOs and CISOs were surveyed from companies in a range of vertical industries including: financial, healthcare, government, retail, manufacturing, food and beverage, oil and gas, professional services, and media/entertainment. This is the second Australian Threat Report from Carbon Black, building on the first survey, which was undertaken in January 2019. This forms part of a global research program with other countries being surveyed including: UK, Germany, Italy, France, Canada, Singapore and Japan.

FOREWORD

THE 2019 CYBERATTACK LANDSCAPE IN AUSTRALIA

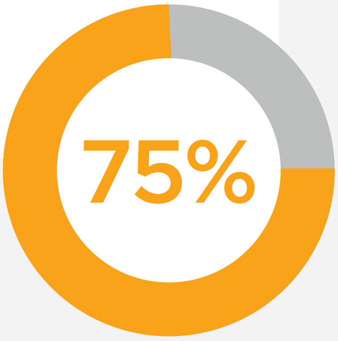
Rick McElroy
Head of Security Strategy, Carbon Black

Australian businesses are battling a sustained threat environment where attacks continue to grow in sophistication and complexity, making breaches an all but inevitable consequence. A glance at breach-related news headlines is all you need to further support the finding of our second Australia Threat Report, which found:

97% **of surveyed Australian organisations** participating in the study said they have suffered one or more breaches in the past 12 months due to external cyberattacks.

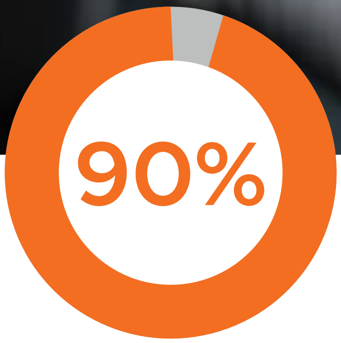
These breaches have caused negative financial impact in 56.5% of those organisations who reported being breached, but it is corporate reputations that are really feeling the effects in the face of a breach incident – 75% of responding businesses that had been breached reported damage to their company's reputation in the aftermath.

75% OF AUSTRALIAN BUSINESSES REPORTED DAMAGE TO THEIR COMPANY'S **REPUTATION**



90% REPORTED AN INCREASE IN **CYBERATTACKS**

90% **of participating Australian businesses** reported an increase in cyberattacks in the last 12 months, with 89% of respondents who had experienced an attack saying that these are becoming more sophisticated. This compares to 81% who reported an increase in attack volume in the previous report. The prevalence of phishing as the attack type resulting in breaches has seen a sharp increase, as attackers target the weakest link in the security chain – end users.



GROWING CONFIDENCE IN CYBERDEFENCE CAPABILITIES...

Despite the sustained nature and severity of threats to their business, 86% of Australian businesses said that they are more confident in their ability to repel attacks than they were 12 months ago. This is an encouraging sign of increased awareness of the tools and techniques available to mount robust defences and the growing maturity of security teams and technology deployments.

This is underlined by the fact that investment in cyberdefence is holding up across all sectors. Slightly ahead of the previous research (90%), this time 96% of respondents say they are planning to increase cybersecurity spend in the coming months.

...BUT INCREASING CONCERN AROUND NEW AND EMERGING TECHNOLOGY RISKS

Security professionals reported significant concerns around how digital transformation projects and the implementation of 5G will affect their risk posture. 49% of the respondents fear they will prompt the development of more frequent, effective and destructive methods of cybercrime.

SKILLS DELTA IS A MAJOR CONCERN

In the light of current and emerging risks over a quarter (27%) of CIOs surveyed said they would need a bigger team. However, 60% report that recruitment and training of specialist cyber security staff is more difficult than it was 12 months ago. This skills delta looms large on the horizon and will cause significant problems for Australian businesses as they adapt to the challenges of securing their business.

THREAT HUNTING IS MATURING

Threat hunting is delivering on its promise, with 93% of businesses reporting that their threat hunting activities had strengthened company defences and 86% finding evidence of malicious cyberattack activity that would previously have gone undetected.

TOP SURVEY RESEARCH FINDINGS

61%

LARGER ORGANISATIONS (WITH 10,001-20,000 EMPLOYEES) REPORTED AN AVERAGE INCREASE OF 61% IN ATTACK FREQUENCY

97%

REPORTED BEING

BREACHED

BREACH FREQUENCY

97% of participating Australian businesses reported being breached in the past 12 months compared to 89% in January 2019. Of those, 50% have been breached once and 38% have been breached between three and 10 times, with 14 companies admitting to suffering more than 10 breaches. That said, the average breach frequency has dropped to 3.78 down from 4.28 in the previous research.

SUSTAINED ATTACK FREQUENCY

90% of businesses surveyed reported an increase in the frequency of cyberattacks in the past 12 months.

Once more, the research indicates that it is larger organisations that bear the brunt of sustained attacks. Businesses with between 5001 and 10,000 employees reported an average 61% increase in attack frequency, while those with between 501-1000 report a 40% increase and those with less than 50 reported a 21% increase.

89%

REPORTED THAT A DEGREE OF INCREASED ATTACK SOPHISTICATION WAS PRESENT

ATTACK SOPHISTICATION CONTINUES TO INCREASE

A degree of increased attack sophistication was reported by 89% of respondents who have had a cyberattack on their company – this compares to 88% in the previous report. Within those figures, 71% of companies reported that attacks had become moderately or significantly more sophisticated.

86% OF AUSTRALIAN BUSINESSES REPORTED THEY ARE MORE CONFIDENT TO REPEL **ATTACKS**

PHISHING ATTACKS TOP THE LIST

Phishing attacks were the prime cause of these breaches according to 27% of Australian respondents who have had a cyberattack on their company. Second to this was ransomware at 17% and third on the list was process weakness with 10%.

DEFENDER CONFIDENCE IS ON THE RISE

Overall, 86% of surveyed Australian organisations said they are more confident that they can repel cyberattacks today than they were a year ago. Is this confidence a sign of a maturing industry, where awareness of threats is higher but businesses have more tools in their arsenal to enable them to defend effectively?

DIGITAL TRANSFORMATION AND 5G IMPLEMENTATION SPARK CONCERNS

96% of participating Australian organisations plan to increase cyberdefence spending in the coming year compared to 90% in the previous report.

27%

PHISHING

ATTACKS WERE REPORTED AS THE PRIMARY CAUSE OF SUCCESFULL BREACHES

17%

RANSOMWARE

ATTACKS WERE REPORTED AS THE SECONDARY CAUSE OF SUCCESFULL BREACHES

FULL SURVEY RESULTS

INCREASED ATTACKS

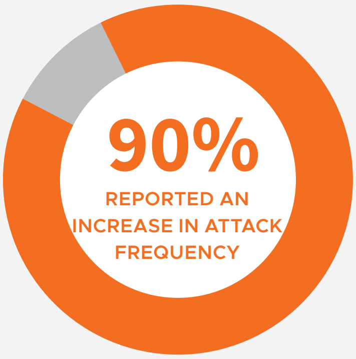
HAVE YOU SEEN AN INCREASE IN CYBERATTACKS ON YOUR COMPANY IN THE LAST 12 MONTHS? IF SO, BY HOW MUCH?

90% of businesses surveyed report an increase in the volume of cyberattacks against their company in the last 12 months compared to 81% of businesses back in January 2019.

33% of respondents have seen a 1-25% increase and 33.5% report an increase of 26-50%. 17% of companies have witnessed a 51-100% increase and 7% have seen anywhere from 100 – 300% increase. Interestingly, 2% stated that they have not had any cyberattacks on their company.

43% of surveyed **financial services** organisations had seen a 26-50% increase.

Government and local authority organisations consistently had a sustained level of attacks with the highest mean of 91%

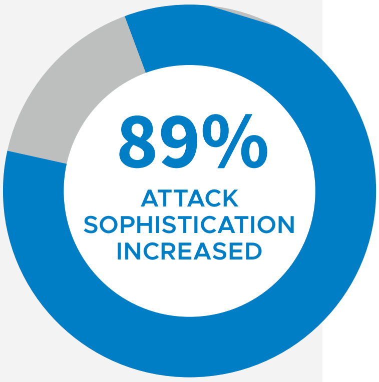


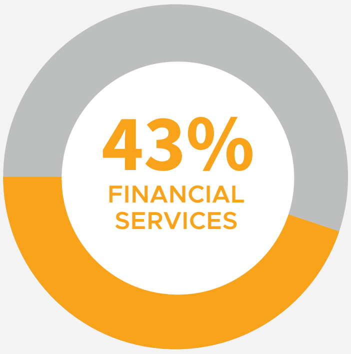
HAVE CYBERATTACKS ON YOUR COMPANY BECOME MORE OR LESS SOPHISTICATED IN THE LAST 12 MONTHS?

89% of survey respondents said that cyberattacks on their company had grown more sophisticated in the past 12 months compared to 88% in the previous survey. 25% reported that they have seen significantly more sophisticated attacks compared to 29% in January 2019.

Travel and transport experienced the greatest growth in sophistication with 60% of attacks being significantly more sophisticated than previously. This was followed by **government and local authority** with 44% and **utilities** closely followed with 43%.

37% of responding companies with 50-100 employees in their IT team said that attacks had become significantly more sophisticated.





WHAT HAS BEEN THE MOST PROLIFIC TYPE OF CYBERATTACK YOUR COMPANY HAS EXPERIENCED IN THE LAST 12 MONTHS?

The most frequent and prolific types of attacks reported were **custom malware**, cited by 19% of respondents followed by Google Drive (cloud-based) attacks at 13%, and ransomware attacks were seen most frequently by 12% of respondents. Commodity malware accounted for 11% of attacks. In the last report malware (custom and commodity combined) accounted for 30% of attacks on Australian businesses, the same as in this report.

The **utilities** sector was heavily affected by custom malware with 43% of attacks taking this form.

HOW OFTEN HAS YOUR COMPANY BEEN BREACHED BY A CYBERATTACK IN THE LAST 12 MONTHS?

97% of surveyed Australian companies have suffered a breach in the last 12 months, compared to 89% in January 2019, with 38% of respondents who have had a cyberattack on their company reporting that they have been breached between 3-10 times.

3.78: average number of breaches suffered by the Australian companies per year compared to 4.28 in the previous report.

6% of respondents reported that they have been breached more than 10 times.

Travel and transport organisations in the report reported the highest average number of breaches suffered with 5.20.

Those companies with an IT team of more than 100 people suffered the highest average number of breaches, at 5.09.

97% BREACHED at least ONCE IN THE LAST YEAR

TRAVEL AND TRANSPORT

5.20

HIGHEST NUMBER OF BREACHES

RANSOMWARE

17%

SECOND MOST COMMON ATTACK

27%
PHISHING
ATTACKS WERE REPORTED AS THE PRIMARY CAUSE OF SUCCESFULL BREACHES

WHAT WAS THE PRIME CAUSE OF SUCCESSFUL BREACHES?

Results showed that **phishing attacks** were the primary cause of successful breaches with 27%, closely followed by ransomware with 17%. Process weakness was a problem in 10% of breaches and out of date security caused 6.5% of breaches.

Phishing attacks have more than doubled in the last six months with 12% citing this as a problem in the last survey.

Phishing attack-related breaches were high in **government and local authority** organisations. with 44%. Phishing attacks also topped the list in financial services with 25%, closely followed by **manufacturing and engineering** with 24.5%.

WHAT WERE THE CONSEQUENCES OF THOSE BREACHES FROM FINANCIAL AND REPUTATIONAL PERSPECTIVES TO YOUR COMPANY?

56.5% of respondents confirmed that a breach had caused negative financial impact to their company, with 17% saying that the impact was severe. However, 37% believed that there had been no negative financial impact due to data breaches.

One in three organisations in the **government and local authority** sector reported suffering severe financial impact following a breach. Interestingly, companies with more than 100 people in their IT team

When it comes to reputational impact, however, 75% said that they had suffered negative effects following a breach.

One in three organisations in the **government and local authority** sector reported suffering severe financial impact following a breach. Interestingly, companies with more than 100 people in their IT team were most likely to report severe financial damage following a breach, with 30% reporting severe financial impact. Reputational impact was also felt most keenly in the **government and local authority** sector, with 44% reporting severe damage, just ahead of **utilities**, where 43% suffered severe fallout.

75%
SUFFERED
REPUTATIONAL IMPACT FOLLOWING A BREACH

When it comes to reputational impact, however, 75% said that they had suffered negative effects following a breach.

HOW MUCH ARE YOU PLANNING TO INCREASE YOUR BUDGET SPEND ON CYBERDEFENCE IN THE NEXT 12 MONTHS?

Results showed that 96% of organisations have plans to increase their budget compared to 90% in the survey at the start of the year. 2% expect it to stay the same.

34% of respondents plan to increase expenditure by between 10-20%. 29% plan increases of 21-30%, 14% plan to increase budgets by 31-40% and 19% plan a greater than 40% increase in spend.

26% of responding **manufacturing and engineering** and 33% of **financial services** organisations plan a greater than 30% increase in spending.

Overall, **utilities** (34%) closely followed by **travel and transport** (31%) and **professional services** (31%) plan the biggest average increase in spend.

Those with larger IT teams are generally looking to increase their budget spend on cyberdefence more than those with small IT teams.

DID YOUR COMPANY'S THREAT HUNTING ACHIEVE A GOAL OF STRENGTHENING ITS DEFENCES AGAINST CYBERATTACKS AND DID THE THREAT HUNTING FIND MALICIOUS CYBERATTACK ACTIVITY YOU WOULD NOT ORDINARILY HAVE FOUND?

93% of participating companies said that threat hunting had strengthened their company's defences to some degree, with 41% believing it had significantly improved their defensive posture. Only 5% of respondents were not threat hunting at all and only 2% that were threat hunting said it had made no difference to their company's defences.

86% said they found evidence of malicious cyberattack activity through threat hunting.

WHAT ARE YOUR COMPANY'S BIGGEST IT SECURITY CONCERNS AROUND THE IMPLEMENTATION AND MANAGEMENT OF DIGITAL TRANSFORMATION AND/OR 5G?

98% of participating Australian businesses have concerns around

96%
PLAN TO INCREASE
SPENDING

93%
THREAT HUNTING
STRENGTHENED
DEFENCES

95% of businesses in the **financial services** sector found evidence of malicious cyberattack activity through threat hunting, as did 100% of **travel and transport** companies and all utilities.

the implementation of emerging technologies and essential digital transformation projects and 5G.

49% felt there was a risk of more effective and destructive methods of cybercrime, while 48% felt there would be more opportunities for cyberattack activity.

Allied to this are the concerns of 34% who are worried about having to be responsible for their own communications rather than relying on the communications of their providers.

Just over a quarter (27%) felt that they would need a bigger team to manage threats. 39% said it will create a lack of visibility with 19% citing the need for more specialised resources.

HOW CONFIDENT IS YOUR COMPANY IN ITS ABILITY TO BE ABLE TO SUCCESSFULLY REPEL CYBERATTACKS AND PREVENT BREACHES NOW COMPARED TO 12 MONTHS AGO?

86% of surveyed Australian companies are more confident than they were 12 months ago. 43% of Australian companies said they were a lot more confident with 43% saying they were a little more confident.

Under one fifth (14%) of respondents said they either had the same level of confidence or were less confident than 12 months ago.

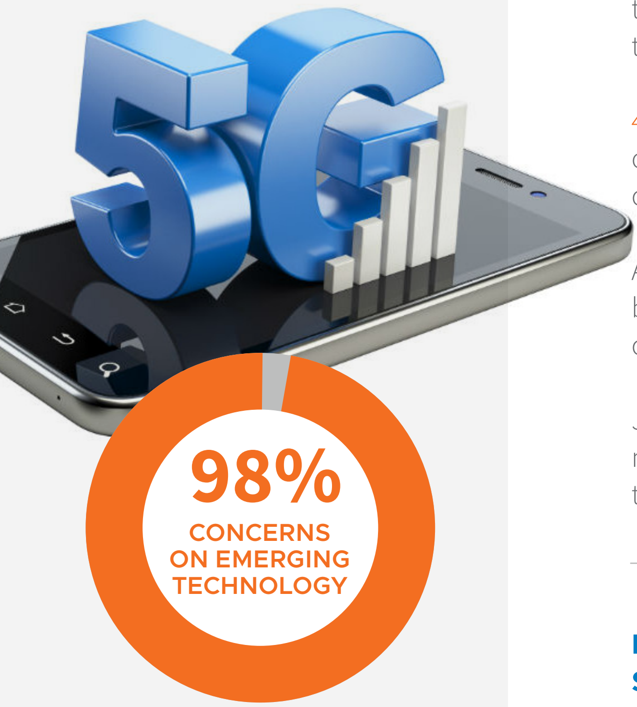
51% of **financial services** and 51.5% of **professional services** companies claimed to be a lot more confident.

HOW DOES RECRUITING AND TRAINING SPECIALIST IT STAFF TO FIGHT CYBERCRIME COMPARE TO 12 MONTHS AGO?

60% of surveyed Australian companies said that this has become either a lot or a little more difficult. 24% said that it has remained the same and 16% felt that it has become less difficult.

In general, the results suggest that the larger the company the more difficult it appears to be to find specialist staff, with 67% of companies that have more than 100,000 employees saying that recruitment has become a lot more difficult.

Similarly, those with an IT team size of more than 100 find it a lot more difficult to recruit.



98%
CONCERNS ON EMERGING TECHNOLOGY

60%
FIND RECRUITING
MUCH MORE CHALLENGING

REFLECTIONS

Rick McElroy

Head of Security Strategy, Carbon Black

As we publish our second Australia Threat Report, building on intelligence gained from previous research conducted in January 2019, we believe a clearer picture is emerging about the specific threats that Australian organisations face and the way they are responding.

Businesses appear to be adjusting to the "new normal" of sustained breach attempts. Greater awareness of external threats and compliance risks have also prompted businesses to become more proactive about managing cyber risks.

We found that companies are tightening up on the factors they can control, such as process weaknesses and out of date security technology, making incremental gains that improve their security posture from within. Nevertheless, phishing appears to remain the root cause of the majority of breaches, emphasising that businesses still have much work to do to get their employees on board and alert to phishing and social engineering.

Threat hunting is reaping rewards as teams identify threats that would previously have gone undetected. We believe this hands-on approach to tackling adversaries is undoubtedly contributing to companies' increasing confidence that they are now better placed to repel cyberattacks than they were 12 months ago. Allied with the sustained level of increase in investment in cyberdefence this is an encouraging sign that cybersecurity is maturing, and businesses are beginning to prioritise it effectively.

While they may be growing in confidence, CIOs shared that they are also seeing clouds building on the horizon revolving around mission-critical projects such as digital transformation and the roll-out of 5G networks. A larger attack surface and greater dependency on digital infrastructure means the risks of malicious attack are amplified and Australian businesses are concerned this will mean more opportunities for cybercrime, and the development of more effective and destructive methods.

There is concern that these emerging threats will require bigger security teams drawn from a talent pool that is small, and subject to intense competition, as more organisations compete for limited resources. There is a growing gap between the skill level, quantity needed and that which is available.

This will force companies to be creative and thorough in the way they approach cyberdefence. Greater automation, AI and tools that offer complete visibility of complex and evolving networks will be required. Resource efficiency will be a buzzword as businesses aim to maximise the capability of teams to detect and mitigate threats and invest intelligently in the tools that empower their teams to build on that growing confidence and maintain proactive cyberdefence.

We hope that you found our second Australia Threat Report valuable and informative. Connect with me on Twitter if you'd like to speak with me directly.

@infosecrick

ABOUT CARBON BLACK

Carbon Black (NASDAQ: CBLK) is a leader in cloud-native endpoint protection dedicated to keeping the world safe from cyberattacks. The CB Predictive Security Cloud® (PSC) consolidates endpoint protection and IT operations into an endpoint protection platform (EPP) that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analysing billions of security events per day across the globe, Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks.

More than 5,600 global customers, including approximately one third of the Fortune 100, trust Carbon Black to protect their organisations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use Carbon Black's technology in more than 500 breach investigations per year.

Carbon Black, CB ThreatSight and CB Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and/or other jurisdictions.

Carbon Black.

Sydney, Australia
Suite 2003, Level 20
Tower 2, Darling Park
201 Sussex Street
Sydney NSW 2000

Melbourne, Australia
Suite 12, Level 15
330 Collins Street
Melbourne VIC 3000

carbonblack.com