DEFENDER POWER ON THE RISE

This research was conducted to understand the challenges and issues facing global businesses 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 global organisations' approaches to strengthening defences, ensuring confidence in their abilities to repel attacks and addressing concerns over the skills gap.

OCTOBER 2019
Globally 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 Global Threat Report, which found:

88% of 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 44% 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.

FOREWORD

THE 2019 GLOBAL CYBERATTACK LANDSCAPE

Rick McElroy
Head of Security Strategy, Carbon Black

Carbon Black commissioned a survey, undertaken by an independent research organisation, Opinion Matters in August 2019. 2012 CIOs, CTOs and CISOs were surveyed for this global research across multiple countries including: Australia, Canada, France, Germany, Italy, Japan, Singapore and the UK. Companies are from 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 Global Threat Report from Carbon Black, building on the first survey, which was undertaken in January 2019.
Despite the sustained nature and severity of threats to their business, 79% of businesses said 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 (88%), this time 90% of respondents say they are planning to increase cybersecurity spend in the coming months.

Security professionals reported significant concerns around how digital transformation projects and the implementation of 5G will affect their risk posture. 37.5% of the respondents fear they will prompt the development of more frequent, effective and destructive methods of cybercrime.

In the light of current and emerging risks nearly one third (30%) of CIOs surveyed said they would need a bigger team. However, 61% report that recruitment and training of specialist cybersecurity staff is more difficult than it was 12 months ago. This skills delta looms large on the horizon and will cause significant problems for global businesses as they adapt to the challenges of securing their business.

Threat hunting is delivering on its promise, with 89% of the businesses reporting that their threat hunting activities had strengthened company defences and 81% finding evidence of malicious cyberattack activity that would previously have gone undetected.
TOP SURVEY RESEARCH FINDINGS

88% REPORTED BEING BREACHED

BREACH FREQUENCY
88% of businesses surveyed reported being breached in the past 12 months compared to 87% in January 2019. Of those, almost one in three (32%) have been breached between three and ten times, with 126 of responding companies admitting to suffering more than 10 breaches. The average breach frequency across all countries is 3.40.

Breach frequency was highest in Italy at 4.78 and lowest in Canada at 2.45.

SUSTAINED ATTACK FREQUENCY
84% of businesses surveyed reported an increase in the frequency of cyberattacks in the past 12 months.

Manufacturing and engineering businesses had seen the biggest increase in the 201-300% category with 31%.

Once more, the research indicates that it is larger organisations that bear the brunt of sustained attacks. 77% of businesses with more than 100,000 employees reported a 201-300% increase in attack frequency. Likewise, Germany had the largest percentage of organisations reporting attacks increased by 201-300% range, with 69% stating this level of increase.

81% REPORTED THAT A DEGREE OF INCREASED ATTACK SOPHISTICATION WAS PRESENT

ATTACK SOPHISTICATION CONTINUES TO INCREASE
A degree of increased attack sophistication was reported by 81% of respondents who have had a cyberattack on their company – this compares to 86% in the previous report. Within those figures, 63% of companies reported that attacks had become moderately or significantly more sophisticated.
GLOBAL THREAT REPORT SERIES

PHISHING ATTACKS TOP THE LIST
Phishing attacks were the prime cause of breaches according to 34% of global respondents who have experienced a cyberattack on their company. Second to this was ransomware at 18% and third on the list was process weakness with 8%.

DEFENDER CONFIDENCE IS ON THE RISE
Overall, 79% of surveyed organisations said they are more confident 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?

GLOBAL CYBERDEFENCE SPENDING
90% of organisations surveyed plan to increase cyberdefence spending in the coming year compared to 88% in the previous report. 8% expect spending to remain the same compared to 9% in the last survey.
HAVE YOU SEEN AN INCREASE IN CYBERATTACKS ON YOUR COMPANY IN THE LAST 12 MONTHS? IF SO, BY HOW MUCH?

84% of businesses surveyed report an increase in the volume of cyberattacks against their company in the last 12 months compared to 82% of businesses back in January 2019.

Germany saw the highest increase in cyberattacks overall with 99% reporting an increase and 69% being in the 201-300% increase category. This was followed by Singapore who reported a 93% increase in cyberattacks. Japan saw the lowest increase in cyberattacks with just under half (49%) reporting increased volumes. Both Japan and Canada had the highest number of respondents - 8% each - stating that there had not been an increase in cyberattacks.

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

81% of respondents said cyberattacks on their company had grown more sophisticated in the past 12 months compared to 86% in the previous survey. 63% reported that they have seen significantly more sophisticated attacks compared to 65% in January 2019.

Italy experienced the greatest growth in sophistication with 41% of attacks being significantly more sophisticated than previously. This was closely followed by France who reported 38% and the UK was in third place with 29%. Interestingly Germany had the highest number of cyberattacks overall, particularly in the 200-300% increase category but experienced the lowest growth in sophistication of these attacks with only 15% saying attacks had significantly grown in sophistication.
Utilities experienced the greatest growth in sophistication with 54% of attacks being significantly more sophisticated than previously. This was followed by financial services companies with 38%.

51% of companies with between 50,001 to 100,000 reported 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 report indicates that custom malware was the most prolific type of attack reported by six out of eight countries in the study; it was cited by 28% of respondents, followed by ransomware at 12%, followed by fileless attacks at 10%.

Germany reported the highest prevalence of custom malware attacks with 74%.

Italy was more affected by cryptojacking than other countries, with 12% naming it as the most frequently encountered attack whereas other countries were below 6%.

The most prolific type of attack encountered in Japan and Singapore was ransomware, reported by 15% of organisations respectively.

The manufacturing and engineering sector was heavily affected by custom malware with nearly half (47%) of attacks taking this form.

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

88% of participating companies have suffered a breach in the last 12 months, compared to 87% in January 2019.

Of those, almost one in three have been breached between three and ten times, with 126 companies (7%) admitting to suffering more than 10
Government and local authorities reported the highest number of breaches. The average breach frequency across all countries is 3.40. Breach frequency was highest in Italy at 4.78 and lowest in Germany at 2.38.

Germany has the highest number of organisations being breached once with 77%. Italy had the highest number reporting more than 10 breaches with 15%. This was followed by France with 10%.

**WHAT WAS THE PRIME CAUSE OF SUCCESSFUL BREACHES?**

**Phishing attacks** were the primary cause of successful breaches with 34% of participating organisations affected, followed by ransomware with 18%. Process weakness was a problem in 8% of breaches and out of date security caused 6% of breaches, both of these causes had dropped from the January 2019 survey, where they were at 11% and 9% respectively.

Phishing attacks that lead to breaches have more than doubled in the last six months with 34% citing this as a problem compared to 16% in the last survey.

Phishing attacks were high in manufacturing and engineering companies with 51% saying they were the prime breach cause. This had increased from 14% in the last report.

Germany had the highest incidents of phishing attacks with 78% of respondents naming this a prime cause of breaches. Japan had the lowest with 17%. Ransomware was particularly high in Singapore with 29% and Canada had the highest number of breaches caused by process weaknesses (10%). Security being out of date was particularly high for Japan with 12% of respondents reporting this as a prime cause of a breach.

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

44% of respondents confirmed that a breach had caused negative financial impact to their company, with 12% saying that the impact was severe. However, 39% believed that there had been no negative financial impact due to data breaches.
20% of the food and beverage sector reported suffering severe financial impact following a breach.

Reputational impact was felt most keenly in the manufacturing and engineering sector, with 42% reporting severe damage.

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

90% of responding organisations have plans to increase their budget compared to 88% in the survey at the start of the year. 8% expect it to stay the same.

26% plan to increase expenditure by between 10-20%.

25% plan increases of 21-30%, 17% plan to increase budgets by 31-40% and 20% plan a greater than 41% increase in spend. Germany is planning the largest IT spend increase with 71% planning uplift of between 41-50%. Interestingly, Japan had the greatest percentage (34%) of those companies that are not planning to increase their IT spend and the greatest percentage of those that are planning to decrease budget spend (4%).

36% of manufacturing and engineering organisations plan to increase budgets by 41-50%. Likewise 79% of those with more than 100,000 employees are planning to increase budgets by 41-50%.

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

**75% SUCCERED REPUTATIONAL IMPACT FOLLOWING A BREACH**

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

Severe negative financial impact was more keenly felt by France (19%). Whereas severe reputational impact was most keenly felt by Germany with more than three quarters of companies reporting this to be the case (76%).

**90% PLAN TO INCREASE SPENDING**
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?

89% of companies said threat hunting had strengthened their company’s defences to some degree, with 40% believing it had significantly improved their defensive posture. Only 7% of respondents said they were not threat hunting at all and only 5% that were threat hunting said it had made no difference to their company’s defences.

81% found evidence of malicious cyberattack activity through threat hunting. Germany was the country with the highest number of respondents reporting that threat hunting activity significantly strengthened company defences, with 79%, and it found more significant evidence of malicious cyberattack activity than any other country with 86%. Japan (17%) had the highest proportion of respondents who claimed not to have undertaken any threat hunting in the past 12 months.

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

92% of businesses said they have concerns around the implementation of emerging technologies and essential digital transformation projects and 5G.

38% felt there was a risk of more effective and destructive methods of cybercrime, while 46.5% felt there would be more opportunities for cyberattack activity.

Allied to this are the concerns of 27% who said they worried about having to be responsible for their own communications rather than relying on the communications of their providers, as well as concerns that it will create a lack of visibility (31%).

Nearly a third (30%) said they would need a bigger team to manage threats. More than a quarter (27%) cited the need for more specialised resources.
Interestingly it is respondents from companies with the biggest IT teams (more than 100 people) who are most concerned that they will need more staff. 47% of these organisations said that they would need more people to manage security risks associated with new digitisation initiatives and technology roll out.

Likewise Germany was most concerned with needing more IT staff with 58% citing that they would need a bigger team and 55% stated that they would need more specialised resources. 21% of Japanese companies stated that they had no IT security concerns around the implementation and management of 5G and digitisation.

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

79% of global companies are more confident than they were 12 months ago. 37% of companies said they are a lot more confident with 42% saying they were a little more confident.

More than a fifth (21%) of respondents said they either had the same level of confidence or were less confident than 12 months ago.

Respondents from Japan were most likely to say their confidence remained the same as 12 months ago, with 48% saying this.

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

When it comes to recruiting and training cybersecurity staff, 55% said they are finding it more challenging than a year ago. 14% of those said it has become a lot more difficult to recruit and train the right people.

The squeeze on talent is being felt most acutely in financial services, government and local authorities and manufacturing and engineering sectors.
HOW DOES RECRUITING AND TRAINING SPECIALIST IT STAFF COMPARE TO 12 MONTHS AGO?

61% of companies said that recruiting and training cybersecurity staff has become either a lot or a little more difficult. 28% said that it has remained the same and 12% said it has become less difficult.

Overall as a sector, manufacturing and engineering companies are finding recruitment a lot more difficult than other sectors with the highest score of 34%.

In general, the larger the company the more difficult it appears to hire, with more than three quarters (77.5%) 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 the most difficult to hire and train IT staff (73%).

Again, 65% of German companies find it a lot more difficult to hire specialist IT staff with Australia and Canada finding it the easiest with 16% each claiming it to be a lot or a little less difficult.
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 attacks are amplified and globally 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 you found our second Global Threat Report valuable and informative. Connect with me on Twitter if you’d like to speak 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.