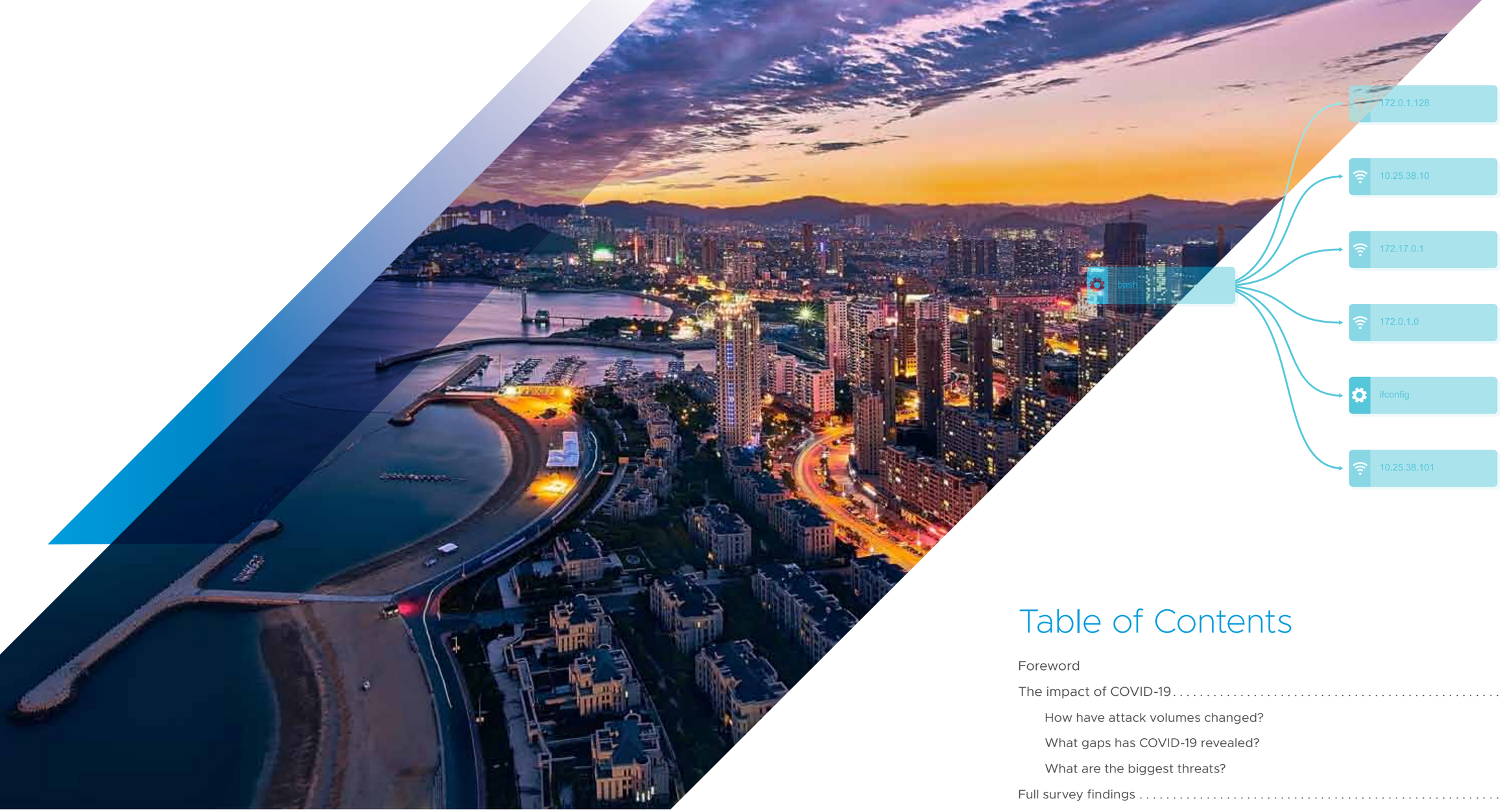
vmware Carbon Black

UK Threat Report

Extended enterprise under threat

June 2020



Introduction

This research was conducted to understand the challenges and issues facing UK 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 UK organisations' 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 organisation, Opinion Matters, in March 2020. 251 UK 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 fourth UK Threat Report from VMware Carbon Black, building on the previous surveys, which were undertaken in September 2018, 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 UK CYBERATTACK LANDSCAPE

Rick McElroy
Cyber Security Strategist, VMware Carbon Black

Foreword

The UK cyber threat landscape has escalated. In this, our fourth UK threat report, we find that attack frequency and sophistication have reached unprecedented levels; 98% of security professionals said the volume of attacks they faced has increased. The increase in attack volume has jumped from 84% in October 2019 as attackers employ a more diverse range of tactics and techniques than ever before in a bid to extort, disrupt and infiltrate organisations.

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

99% of UK organisations have suffered a data breach as a result of a cyberattack in the past 12 months and the average organisation has experienced 2.63 breaches.

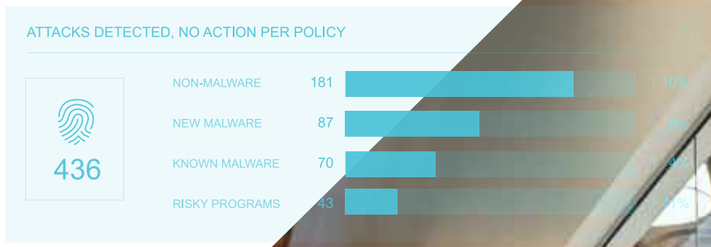
All but two of the security professionals we surveyed said that their organisation had suffered at least one data breach in the last 12 months. Of the remaining two, one didn't know how many breaches they had suffered and the other preferred not to say.

The considerable leap in attack frequency and sophistication revealed in this iteration of the report shows that, however fast UK businesses may be adapting to the intensifying environment, the cyber threat landscape is evolving faster. 96% of security professionals say attacks have become more sophisticated, 39% of those say they have become significantly more advanced, an increase on the 28.5% that noted an increase in attack sophistication in October 2019. This confirms what VMware Carbon Black Threat Analysis Unit research has been finding: adversaries are adopting more advanced tactics as the commoditisation of malware is making more sophisticated attack techniques available to a bigger cohort of cybercriminals. It's not surprising that custom and commodity malware are the most commonly seen attack types.

98%
of security professionals said the volume of attacks they faced has increased.

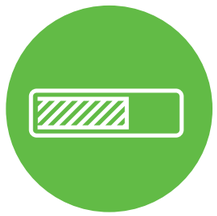
99%
of UK organisations have suffered a data breach as a result of a cyberattack in the past 12 months

96%
of security professionals say attacks have become more sophisticated, 39% of those say they have become significantly more advanced



15%

Despite only featuring in a small percentage of attacks experienced island hopping was the cause of one sixth of breaches (15%).



99.6%

All but one (99.6%) of our survey participants anticipated an increase in spend,

51%

say they will need to increase security spending on cybersecurity programmes

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 Vulnerability was the top cause of breaches with 15.5% closely followed by Island hopping with 15%, despite only featuring in a small percentage of attacks experienced, together with third party applications. Furthermore, 6% of breached businesses had been compromised via their supply chain. Clearly, the extended enterprise ecosystem is generating considerable security concerns.

Reputations And Profits 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 financial and reputational damage.

Budget Rises Are Robust, But Will Spending Be Strategic Or Tactical?

UK security professionals are responding to the uptick in cyberthreats by boosting cyber defence spending. All but one (99.6%) of our survey participants anticipated an increase in spend, an increase from the 93% who planned increases last time.

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, 89% 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. 51% say they will need to increase security spending and controls, while 49% 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 eight different consoles or agents to manage their security programme.

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 rationalisation, 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. 94% are aware of it, but only 51% 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.

8

UK respondents say they use an average of more than eight different consoles or agents

94% vs 51%

94% are aware of the MITRE ATT&CK® framework but only 51% 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 cyber security 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 fourth UK Threat Report useful and informative.

COVID-19 Supplemental Research Findings

250 UK respondents took part in these supplemental questions from March to April 2020

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 organisations."

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

92% of all UK respondents stated that they had seen an increase in overall cyberattacks as a result of employees working from home.

A **quarter (25%)** recounted that attack volume had gone up by between 25 and 49% with 2% stating that attacks had increased by between 50 and 100%.

1 respondent out of 250 stated that they did not have more of their employees working from home than usual during COVID-19 and the mean percentage increase in attacks for UK respondents excluding this one person was **18.45.**

Companies in the **501 and 1000** employee category experienced the highest mean increase in attacks of **23.42%** with 39% stating that they had witnessed increases in attacks between 25 and 49%.

92%

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

NEARLY HALF

45% of those surveyed reported very significant gaps in terms of the effectiveness of their disaster recovery planning 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?

45% of those surveyed reported very significant gaps in terms of the effectiveness of their disaster recovery planning 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.

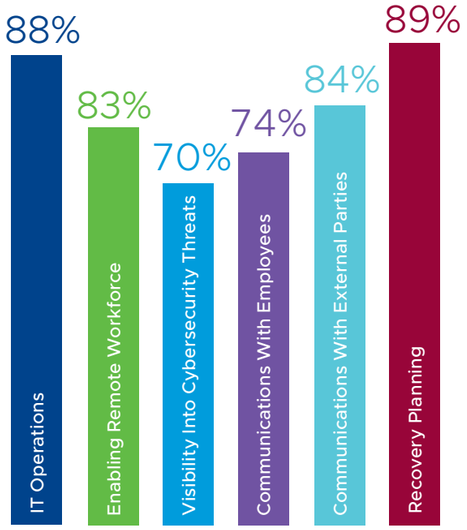
With regard to **recovery planning** 36% of respondents identified very significant gaps and 89% highlighted gaps of some kind.

29% reported very significant gaps in disaster recovery planning in **IT operations** including hardware and software roll outs. Overall, 88% reported gaps, be that severe or slight.

In terms of **enabling a remote work force,** very significant gaps were felt by 27% of survey respondents, and overall, 83% of respondents felt that there were gaps in their planning.

Just under a quarter (24%) of UK respondents felt that there were very significant gaps in their **visibility into cybersecurity threats** with an additional 46% stating that there were slight gaps.

26% admitted to severe gaps in dealing with the situation in terms of **communication with employees** and overall, 74% of respondents stated that these were either slight or very significant.



What gaps did COVID-19 reveal in your company's disaster recovery planning? (those saying very or slightly significant)

28%

28% 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?

28% recounted the **inability to institute multi-factor authentication** as the biggest threat to their company. Second to this was **COVID-19 related malware** with 20% and third was the **inability to roll out timely software patches** with 16%. 7% cited **phishing,** 5% stated **spear phishing.** Other notable threats were **ransomware** (4%), and **social engineering** (2%).

The **inability to institute multi-factor authentication** was the biggest threat for **financial services** organisations with 48% claiming this to be the case.

COVID-19 related malware impacted more on the smaller organisations.

Those with IT team sizes of **21-30** reported the biggest threat impact (45%) was the **inability to institute multi-factor authentication.**

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 93% and more than half (54%) of these increases were in the 51 to over 100% categories. Second to this was IoT Exposure with 89% reporting threat change increases and 14% of these were in the 51 to over 100% categories. Phishing emails and spear phishing were also significantly high with 88% and 85% respectively reporting overall increases in threat changes and 17% and 22% of these were in the 51 to over 100% category.

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 65% of respondents reporting an overall threat change increase.

28% of UK 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 the pandemic, this was also high with 81% reporting overall threat change increases and 20% of the respondents reporting increases between 51 and more than 100%.

93%

The highest increase in threat changes during COVID-19 was with COVID-19 related malware, which saw overall threat change increases of 93%

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 98% of UK organisations have seen an increase in the number of cyberattacks on their company in the last twelve months. This is a considerable increase from 84% in the October 2019 report and the highest attack frequency we have ever witnessed.

Respondents reported an average increase in frequency of 53%, and 37% 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 29% reported increases of this magnitude.

44% of respondents in the **healthcare** sector had seen a 51-100% increase and 49% of **financial services** had seen a 26-50% increase.

The biggest companies are facing above average attack volumes: those with between **20,001-100,000** employees saw an average attack frequency increase of 75% - this is 20% higher than the overall average.

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

96% of respondents say attacks have grown more sophisticated over the last twelve months – this compares with 90% who said the same back in October 2019 and 89% in February 2019. Of these, 39% said they had become **significantly** more sophisticated, again a notable leap compared with the last report, where 28.5% noted a significant sophistication increase.

Half of **government and local authority** and 55% of **manufacturing and engineering** respondents had witnessed a significant increase in the sophistication of the attacks they faced.

96%

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

89%

said they had become significantly more sophisticated

99% of the CISO/CIOs that took part in our research said they had suffered a breach following a cyberattack in the past 12 months.

Custom malware tops the table again, with a quarter of respondents seeing it as the most frequent attack type (up from 21% 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 quarter of respondents seeing it as the most frequent attack type (up from 21% last time). **Commodity malware** has seen a 6% jump from last time, comprising 16% of the attacks faced.

The frequency of **process hollowing** attacks has quadrupled from 3% to 12% since October 2019, indicating a growing attacker focus on gaining undetected access to networks. Also appearing on the attack radar for the first time is **island hopping,** seen in 6% of incidents. While this figure may seem low, these types of attacks are proving effective, as later analysis shows.

Interestingly **ransomware** has dropped from the second most-frequently experienced attack to 9th on the list, comprising just 5% of attacks compared to 15% in October 2019.

Financial services are at the mercy of custom malware with 47% saying this was the most frequently experienced attack type (compared with an average of 25%).

Manufacturing and engineering company respondents were proportionally more affected by commodity malware, with 26% experiencing it most frequently compared with an average of 16%.

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

99% 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 is the highest reported breach figure in the history of our research and leaps from 84% who said they had been breached in October 2019.

The average number of breaches suffered by organisations is 2.63. The largest group of respondents (46%) said they had suffered one breach. However, a concerning 17% said they had suffered five or more breaches.

Government and local authority organisations reported the highest average number of breaches at 3.08, while 19% of **financial services** respondents had suffered five or more breaches.

Size matters, too. Almost one third of companies with between **10,001-20,000 employees** reported having suffered six breaches.

OS Vulnerabilities

The top cause of breaches was identified as OS vulnerabilities

6%

despite only featuring in 6% of the attacks experienced, island hopping was the cause of 15% of breaches.

71%

said they had suffered reputational impact after a breach

What Was The Prime Cause Of These Breaches?

The top cause of breaches was identified as **OS vulnerabilities** as hackers take advantage of poor patching hygiene.

Financial services (30%) and manufacturing and engineering (23%) companies are most affected by OS vulnerability breaches.

Interestingly, despite only featuring in 6% of the attacks experienced**, island hopping** was the cause of 15% of breaches. This indicates the vulnerability of extended enterprises to attacks originating in vendor organisations. 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 (21%) and **food and beverage** industry (18%).

Third party application breaches have also jumped, to 15% of successful breaches, 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 33% of successful breaches, but this has dropped to just 6%. The same was true of **ransomware,** which dropped from 20% to 11%.

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 slightly but, when organisations are affected, the severity of impact has intensified.

The percentage of organisations saying they had suffered **severe** financial impact following a breach almost doubled, with 17.5% reporting severe financial impact compared with only 9% in October 2019. Almost one third (32%) of companies in the **manufacturing and engineering sector** said they had suffered severe financial impact as a result of a breach, while a quarter of **government and local authority** and a fifth of **food and beverage companies** had also suffered severe impact. In contrast 70% of **financial services** respondents said there had been no negative financial impact.

Almost one third (31%) of respondents said they had suffered severe reputational impact as a result of a breach, a jump from just 13% who said the same in October 2019. Overall, 71% said they had suffered reputational impact after a breach, which is broadly in line with the findings in October 2019.

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

Threat hunting is becoming ubiquitous, with 99.6% of respondents using it as part of their cybersecurity strategy, up from 92% in October 2019. It is also proving more effective; overall 98% said it had strengthened their company's defences, with 58% of those saying it significantly strengthened them, a jump of 30% compared with the previous survey.

The percentage finding **significant evidence** of malicious activity more than doubled, to 65%, while overall 95% found some evidence of malicious activity through threat hunting (compared with 78.4% last time). **Healthcare** organisations have been particularly successful at uncovering malicious activity, with 76% finding significant evidence.

99.6%
of respondents are using threat hunting as part of their cybersecurity strategy up from 92% in our last report

65%
The percentage finding significant evidence of malicious activity more than doubled, to 65%

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

All but one of the CISO/CIOs we surveyed said they plan to increase budget spend on cyber defence in the next 12 months, with an average expected increase of 26%. 33.5% say they plan to boost budget by 31-40%, compared with 18% who said this last time.

Among these are two fifths (40%) of **healthcare** organisations and 42% of **manufacturing and engineering** companies.

Bigger companies are planning bigger increases: on average, companies with over 20,000 employees are planning increases of 30% or more.

All but one
All but one of the CISO/CIOs we surveyed said they plan to increase budget spend

46%
of Government and local authority organisations are adopting 5G in next six months

8.24
is the average number of technologies deployed

43%
were aware of the MITRE ATT&CK® framework but have no plans to implement it

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)?

Every CISO/CIO we surveyed said they were planning to adopt 5G over the coming 12 months, with 86% expecting to do so in the next six months. They are almost equally split on the security implications. 51% say they will need to increase security spend to manage adoption, while 49% don't believe they will need to invest. **Government and local authority** organisations are most likely to say they are adopting 5G in next six months and will be investing in related security and controls (46%). 55% of **financial services** companies believe they will not need to increase spend due to 5G adoption.

Larger companies are more likely to say they won't need to increase security spend - in companies of 20,001-50,000 employees 74% say they won't.

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

Three quarters of companies have between 5 and 10 different technologies deployed to manage their security programme. 13.5% have 11-25 different technologies.

The average number of technologies deployed is 8.24 – this rises to 9.74 in financial services. IT teams of 31-40 people are using more tools on average - 9.34 compared with an average of 8.24.

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 the UK, but respondents are split over whether to adopt it. 43% are aware of it but have no plans to implement it, while 51% are aware and plan to use it.

The financial services sector is the most positive about the framework, with 64% aware of it and planning to use it, closely followed by government and local authority organisations (62.5%). The most sceptical are respondents from the manufacturing and engineering sector, where 61% 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-Prioritisation Of Budget) (Tick All That Apply)

Networks lead the field at 59%, followed by **workload/applications** at 50%, **then mobiles** – 35% – and finally **endpoints** at 18%.

Workload/applications have caused more reprioritisation in **government and local authority** and **healthcare** organisations, with 75% and 56% having to take action respectively. This makes sense in the light of UK public sector's drive to digitise.

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

Network is seen as the biggest risk, cited by 46% of respondents, followed by **workload/apps,** identified by one third. The next most commonly cited risk is **mobile devices (**15%), with **endpoints** such as laptops and desktops coming in at 6%.

Financial services see higher than average risk from mobile devices (21%), as does **healthcare** (27%). 58% of **government and local authority** organisations see the biggest breach risk as the network, as do mid-sized companies of between 1001-2000 employees (56.5%)

Bigger IT teams are more concerned about workload/apps in general than network risk.