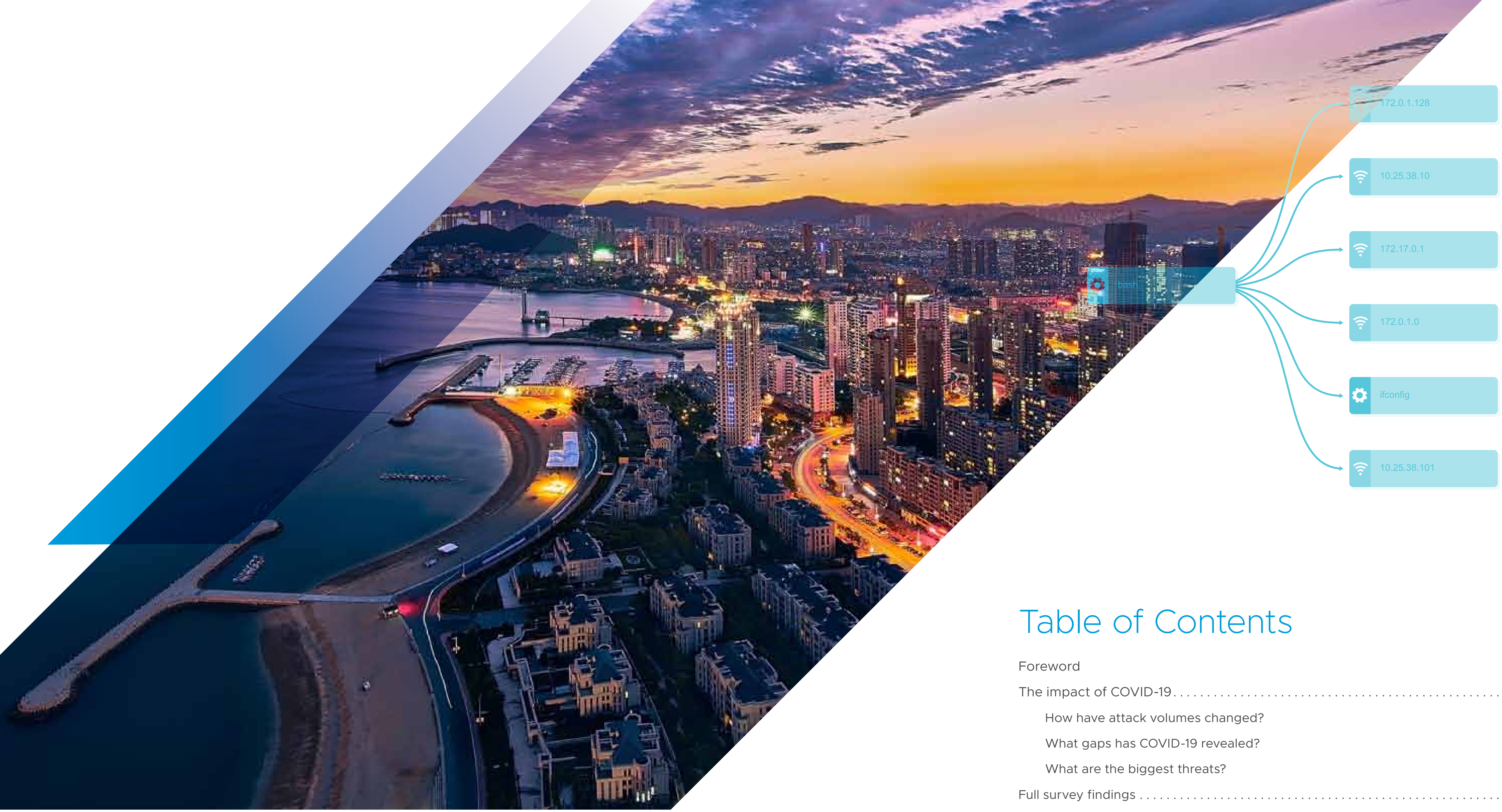
vmware® Carbon Black

Global Threat Report

Extended enterprise under threat

June 2020



Introduction

This research was conducted to understand the challenges and issues facing global 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 organizations' plans for securing new technology, for adopting cybersecurity frameworks and the complexity of the current cybersecurity management environment.

Table of Contents

THE 2020 GLOBAL CYBERATTACK LANDSCAPE

Rick McElroy
Cyber Security Strategist, VMware Carbon Black

Foreword

The global cyber threat landscape has escalated. In this, our third Global Threat Report, we find that attack frequency has reached unprecedented levels; **90% 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:

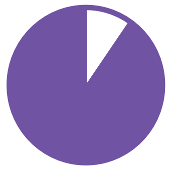
94% of organizations worldwide have suffered a data breach as a result of a cyberattack in the past 12 months and the average organization has experienced 2.17 breaches.

The increase in attack volume has jumped from 84% in October 2019 and 82.5% in February 2019, demonstrating a clear upward trend. At the same time, however, the number of breaches has dropped once more, down from 3.4 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 global businesses may be adapting to the intensifying environment, the cyber threat landscape is evolving faster. **80% of security professionals say attacks have become more sophisticated, 18% 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 joint most commonly seen attack type.

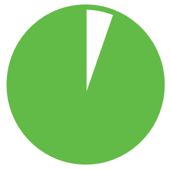
METHODOLOGY

VMware Carbon Black commissioned a survey, undertaken by an independent research organization, Opinion Matters, in March 2020. 3012 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 Global Threat Report from VMware Carbon Black, building on the previous surveys, which were undertaken in February 2019 and October 2019. The countries surveyed were: Australia, Canada, France, Germany, Italy, Japan, Netherlands, Nordics, Singapore, Spain, the UK and the US.



90%

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



94%

of organizations worldwide have suffered a data breach

80%

of security professionals say attacks have become more sophisticated

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 most common cause of breaches, at the root of 18% of compromises. Third party application breaches were joint second on the list, leading to 13% of breaches. **Island hopping, despite only featuring in 4.5% of attacks experienced, shared second place as the most common cause of breaches, at the root of 13%.** Furthermore, 7% of breached businesses had been compromised via their supply chain. Clearly, the extended enterprise ecosystem is generating considerable security concerns.

At the other end of the scale, breaches from direct attacks through ransomware and phishing have dropped considerably. In October 2019, phishing caused 34% of breaches and ransomware accounted for 18%. This time they each accounted for only 6%. It appears that unsophisticated "spray and pray" tactics are being rejected in favour of accessing networks undetected and gaining persistence for longer term campaigns.

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 continues to be felt. Security professionals feel that the reputation of their business is more likely to be affected by a breach, with 70% saying they had suffered image damage.

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

Security professionals worldwide are responding to the uptick in cyber threats by boosting cyber defense spending, more of them than ever before told us that they are expecting to increase their budgets. **96% plan a greater spend,** up from 90% in October 2019 and 88% in February 2019.

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, 92% 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. **46.5% say they will need to increase security spending** and controls, while 48% won't be focusing their budgetary increases on securing 5G.

96%
Plan to increase budgets

46.5%
Say they will need to increase security spend and controls around 5G

8.91
The average number of different tools being used to manage cybersecurity programs

A Complex, Crowded, Multi-Technology Environment

Perhaps this is because they're already supporting multiple security technologies. Respondents are using an average of **8.91 different security tools** 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. 80% worldwide are aware of it, but only 56% 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.

Workloads/Applications Top Breach Risk List

The main concern for cybersecurity professionals globally is workload/applications, cited as the biggest risk for 35% of them. This is perhaps not surprising in light of the jump in third party app-related breaches. As businesses run more and more apps in a bid for flexibility and productivity gains, ensuring their security will become of critical importance.

Consensus Between Territories

What was striking about this edition of our research project was the broad consensus between different countries. More geographies than ever before reported their highest ever figures for attack volume increases and subsequent breaches, while budget increases are also at their highest. What this really shows is that cyber defense is a borderless challenge on a global scale. The analysis below highlights the key statistics and outlying responses of interest.

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

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 third Global 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.

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 beacuse 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

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 recovery 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.

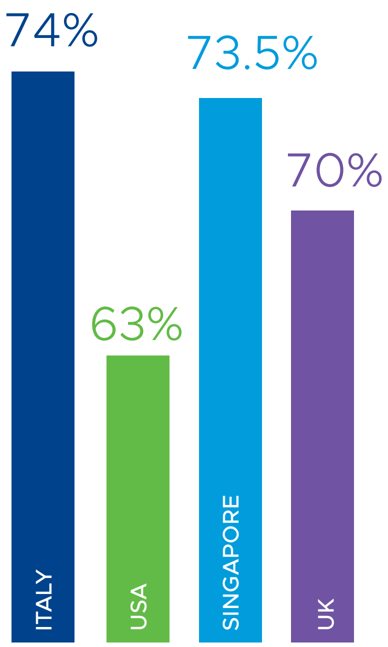
In terms of **enabling a remote work force**, severe and significant gaps were felt by over a quarter (28%) of survey respondents, and overall, 85% of respondents felt that there were gaps.

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 Cybersecurity 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 organisations, 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%).

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%.

92%

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

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 90% of organizations worldwide 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 82.5% in the previous February, making it the highest increase in attack frequency we have ever witnessed.

Respondents reported an average increase in frequency of 63%, and 45% overall said there had been an increase in attack volumes of between 51% and 300% - this is a jump from the October report where only 34% reported increases of this magnitude.

The majority of countries reported increases in attack volumes. The exceptions were **Germany,** where more than a quarter of survey respondents said they hadn't suffered any cyberattacks at all, and **Singapore,** where 17% hadn't suffered any cyberattacks and one fifth of respondents preferred not to say.

Globally, **manufacturing and engineering** companies are bearing the brunt of increased attack volumes, with 60% of respondents reporting attack volumes have increased between 51-300%. Half of **professional services** company respondents said they had seen volume increases at the same level, as did 49% of **media and entertainment companies.**

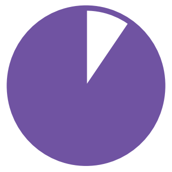
Have Cyberattacks On Your Company Become More Or Less Sophisticated In The Last 12 Months?

80% of respondents say attacks have grown more sophisticated over the last twelve months – a figure that has held steady from October 2019 (81%) and dropped slightly since February 2019 (86%). Of these, 18% said they had become significantly more sophisticated, and 62% said they were **moderately** or **slightly** more sophisticated.

Despite reporting a lower level of attack frequency, the sophistication faced by organizations in **Germany** is the highest, with 41% of respondents saying attacks have become **significantly** more sophisticated. The **UK** is not far behind, with 39% of attacks rated significantly more sophisticated and a further 46% **moderately** more so.

At the other end of the scale, just 1% of respondents from **France** and 5% from **Italy** said attacks were **significantly** more sophisticated.

Respondents from the **financial services** sector are facing an above average increase in attack sophistication – 31% say attacks have grown **significantly** more sophisticated.



90%

A staggering 90% of organizations worldwide have seen an increase in the number of cyberattacks on their company in the last twelve months.

80%

80% of respondents say attacks have grown more sophisticated over the last twelve months.

94% 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 and Google Drive™ attacks (cloud-based attacks) top the table,

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

Custom malware and **Google Drive™ attacks** (cloud-based attacks) top the table, both cited by 18% of respondents as the most frequently experienced.

The frequency of **process hollowing** attacks has more than trebled from 3% to 9.5% since October 2019, indicating a growing attacker focus on gaining undetected access to networks. Also appearing on the attack radar is **island hopping**, with 4.5% 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.

Google Drive (cloud-based attacks) are disproportionately affecting **manufacturing and engineering** companies, with 34.5% of respondents in this sector saying they were the most frequently experienced attack type.

Financial services are at the mercy of custom malware with 45% saying this was the most frequently experienced attack type (compared with an average of 18%).

France suffered by far the highest frequency of Google Drive (cloud-based attacks) with 71% naming it most commonly experienced. Custom malware was a greater than average problem in the **Netherlands** (28% compared with an average or 18%)

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

94% 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 increased notably from 88% who said they had been breached in October 2019 and 87% who said the same in February 2019.

The average number of breaches suffered by organizations is 2.17, which is a drop from 3.4 in October 2019, a positive indication that, overall, organizations are heading in the right direction. The largest group of respondents (51%) said they had suffered one breach, while almost one fifth (18%) said they had suffered two.

Breach frequency was highest in **France** where respondents reported 3.7 breaches on average. It was lowest in **Canada** with just one breach per organization.

Respondents from the **manufacturing and engineering** sector reported the highest average number of breaches at 2.56.

Overall, larger organizations tend to report higher breach frequencies. Respondents from companies with **5001-10,000 employees** said they had suffered 3.12 breaches on average, while those with between **50,001-100,000** had 3.83 breaches.

18%
identified OS vulnerabilities as the top cause of breaches

Phishing
phishing attacks dropped dramatically as a cause of successful breaches.

70%
say they had suffered damage to their corporate image following a breach

What Was The Prime Cause Of These Breaches?

The top cause of breaches was identified as **OS vulnerabilities** (18%) as hackers take advantage of poor patching hygiene. Joint second was third party application breaches (13%). Despite only featuring in 4.5% of attacks experienced, **island hopping** was equal second most common cause of actual 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 (18%) and **manufacturing and engineering** (15%), though the **media and entertainment** sector also suffered from breaches in this way (18%).

US organizations have suffered more than most from OS-related breaches, a factor in 27%, while **Australia** and the **Netherlands** were more likely to have suffered a third-party application breach (both 18%). **Island hopping** is a big issue in **Italy,** accounting for 26% of breaches. **Canada** stood out as much more likely to have suffered a breach due to **web application attacks** (21%), whereas in **Spain** 35% of all breaches were caused by either process weaknesses or out of date security.

Surprisingly, **phishing attacks** dropped dramatically as a cause of successful breaches. In October 2019 phishing was the cause of 34% of successful breaches, but this has dropped to just 6%. The same was true of **ransomware,** which dropped from 18% to 6%.

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

The percentage of respondents reporting negative financial impact following a breach has dropped from 44% to 30% stating that there had been a negative effect. 9% said that the financial impact they had experienced had been severe.

Respondents from **Japan** reported the highest level of severe financial impact, with almost one quarter (24%) saying this had been the result. Respondents from the **Nordics** reported a similar level of severity (22%). In contrast, 78.5% of French respondents and 70.5% of **Netherlands** respondents said there had been no financial impact at all.

The effect on reputations was more pronounced, with 70% saying they had suffered damage to their corporate image following a breach and 17% saying it was severe. This figure held steady from the October 2019 report.

The UK (31%) and Germany (33.5%) had most respondents saying they had suffered severe reputational damage after a breach.

44% of Government and local authority respondents said they had suffered financial impact due to a breach and 18% said it had been severe. **Food and beverage** companies were also more likely to have suffered financial damage, with 14% saying it was severe.

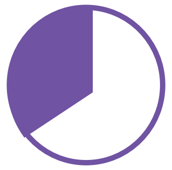
Financial services companies saw the most reputation effect from breaches, with 34% reporting severe reputational damage.

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?

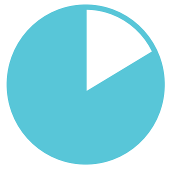
Threat hunting is becoming ubiquitous, with 88% of respondents using it as part of their cybersecurity strategy. It is also proving effective; overall 86% said it had strengthened their company's defenses, with one quarter saying it significantly strengthened them.

There were some notable regional variations, however. Threat hunting was not popular among **French** respondents, with 67% saying they had not threat-hunted at all. Similarly, one quarter of **Japanese** respondents and 24% of those from the **Netherlands** had not used threat hunting in the last year. In contrast only one respondent from the **UK** and one from the **Nordic** region said they hadn't threat hunted. This was borne out in the figures finding significant evidence of malicious cyber threat activity: 65% of UK organizations and 44% of **Nordics** respondents found significant evidence.

Financial services respondents found the most defense strengthening from threat hunting, with 96% seeing a security benefit. They were also the most likely to find significant malicious activity within their networks.



36%
36% of respondents said they had found significant evidence of malicious activity thanks to their threat hunting program.



88%
Threat hunting is becoming ubiquitous, with 88% of respondents using it as part of their cybersecurity strategy

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

96% of the cybersecurity professionals we surveyed worldwide said that they planned to increase budgets, by an average of 27%.

This is a robust uptick on October 2019, when 90% planned to increase spend and February 2019, when the figure was 88%.

Almost one third (32%) say they expect to boost budgets by 31-40%, compared with 17% who said this last time. Among these are 59% of **French** respondents and 47% of **Singaporean** respondents.

40% of **financial services** respondents said they anticipate increasing budgets by between 31-40%, as do 41% of those from the **manufacturing and engineering** sector.

96%
96% of the cybersecurity professionals we surveyed worldwide said that they planned to increase budgets, by an average of 27%.

95%
of the CISO/CIOs we surveyed worldwide said they were planning to adopt 5G over the coming 12 months,

8.91
is the average number of technologies deployed

80%
were aware of 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)?

95% of the CISO/CIOs we surveyed worldwide said they were planning to adopt 5G over the coming 12 months, with 62% expecting to do so in the next six months. They are divided on the security implications.

46.5% say they will need to increase security spend to manage adoption, while 48% don't believe they will need to invest. 5% have no plans to adopt 5G.

All UK respondents said they were planning to adopt 5G, with 51% expecting to increase security spend. At the other end of the scale only 87% of **Singaporean** organizations plan to adopt 5G. 70% of respondents from **France** said they didn't plan to support 5G rollout with security investment, as did 55% of both **Australian** and **Japanese** respondents.

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

68% of companies have between 5 and 10 different technologies deployed to manage their security program. 20% have 11-25 different technologies.

The average number of technologies deployed is 8.91. This rises to 11 in **Germany** and almost 10 in **Canada,** while **Nordics, Spain** and the **USA** have an average of 9.

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– 80% know what it is - but respondents are split over whether to adopt it. 23% are aware of it but have no plans to implement it, while 56% are aware and plan to use it.

The highest awareness was among **French** respondents, where 97% know about it and 87% plan to use it. Awareness was lowest in **Italy** where only 57% have heard of the framework and just 39% 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)

Networks lead the field, requiring adjustment by 58% of respondents, followed by **workload/applications** (55%) then **mobile** (48%). Endpoints were lowest on the list, needing investment adjustment by just over one quarter (27%)

Respondents from **France** were far more likely than those from other territories to need to reprioritize investment in mobile technology, with 84% selecting this option compared with 48% on average. Italy and **Singapore** respondents showed greater than average concern over endpoint investment levels.

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 35% of respondents, followed by **network,** identified by 34%. **Mobile devices** were seen as the biggest risk by around one fifth (21%). **Endpoints** such as laptops and desktops were the top risk for 7%.

Again, **French** respondents are more concerned about mobile devices, with 77% saying this was the biggest risk they face. **German** respondents were more concerned by **endpoints** than average, with 17% saying this was their biggest risk.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com