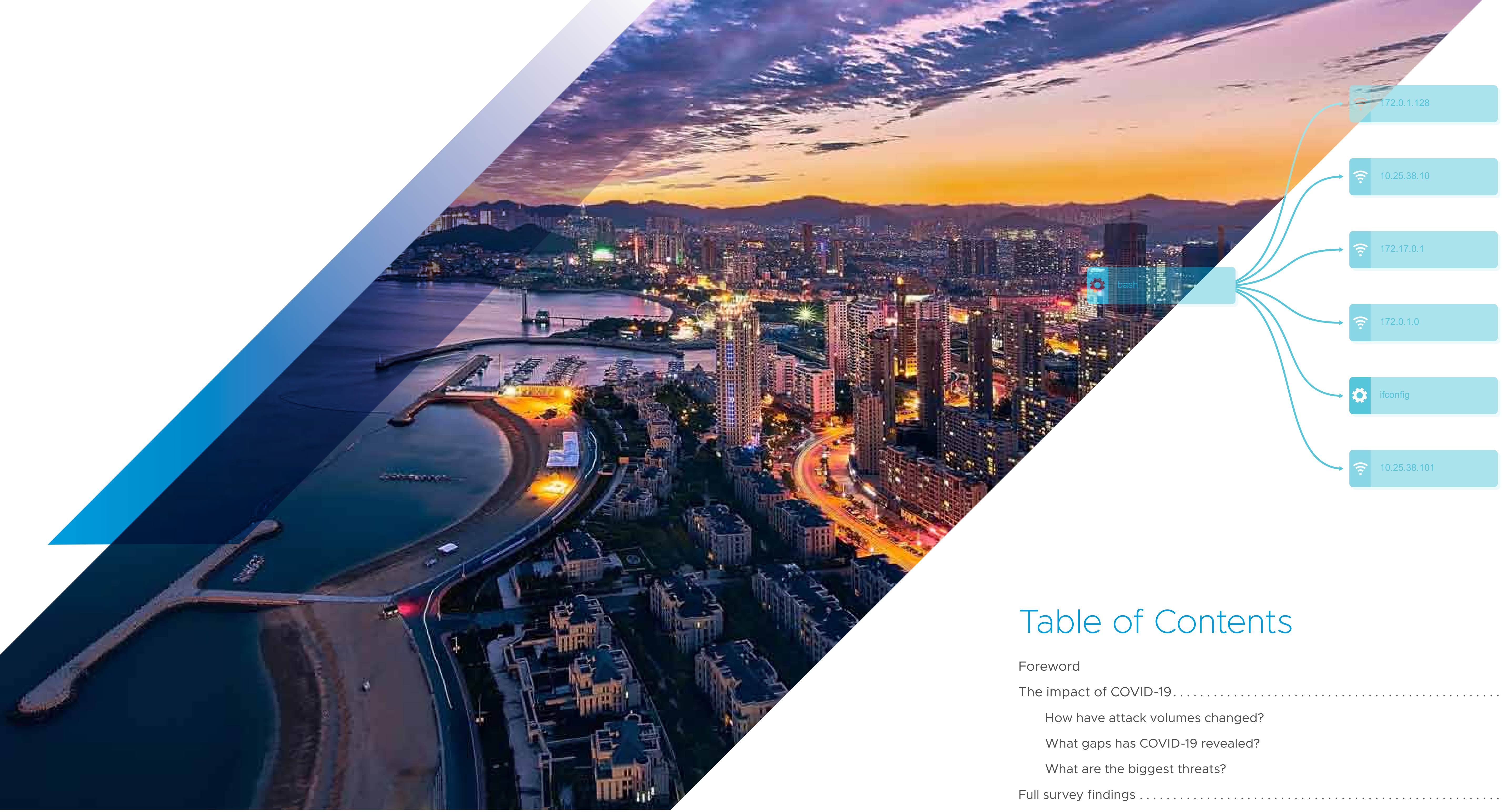
vmware® Carbon Black

Singapore Threat Report

Extended enterprise under threat

June 2020



Introduction

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

Table of Contents

THE 2020 SINGAPORE CYBERATTACK LANDSCAPE

Rick McElroy

Cyber Security Strategist, VMware Carbon Black

Foreword

The Singaporean cyber threat landscape appears to have plateaued somewhat. In this, our third Singapore threat report, we find that attack frequency and sophistication have lessened meaning either the technologies Singaporean companies have in place are working to subdue the adversary or that perhaps the attacker has become much more targeted with regard to the types of organization they attempt to infiltrate – certainly our analysis this time shows that mid-sized organisations are facing a much more intense threat environment than larger or smaller counterparts. Whilst only a modest 43% 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 common. Our research found that:

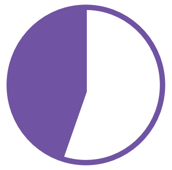
80% of Singapore organizations have suffered a data breach as a result of a cyberattack in the past 12 months and the average organization has experienced 1.67 breaches.

When attacks do happen, they are succeeding: all but seven of the security professionals we surveyed, who had suffered a cyberattack in the past 12 months, said that their organization had suffered at least one data breach in that same time period. Of the remaining seven, two didn't know how many breaches they had suffered and the other five preferred not to say. The attack volume has fallen from October 2019.

The sustained attack frequency and sophistication revealed in this iteration of the report shows that, however fast Singaporean businesses may be adapting to the intensifying environment, the cyber threat landscape is evolving faster. 67% of security professionals say attacks have become more sophisticated, 22% 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 and commodity malware are among the most commonly seen attack types.

METHODOLOGY

VMware Carbon Black commissioned a survey, undertaken by an independent research organization, Opinion Matters, in March 2020. 251 Singaporean 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 Singaporean Threat Report from VMware Carbon Black, building on the previous surveys, which were undertaken in February 2019 and October 2019. This forms part of a global research project across multiple countries, including: Australia, Canada, France, Germany, Italy, Japan, Netherlands, Nordics, Singapore, Spain, the UK and the US.



43%

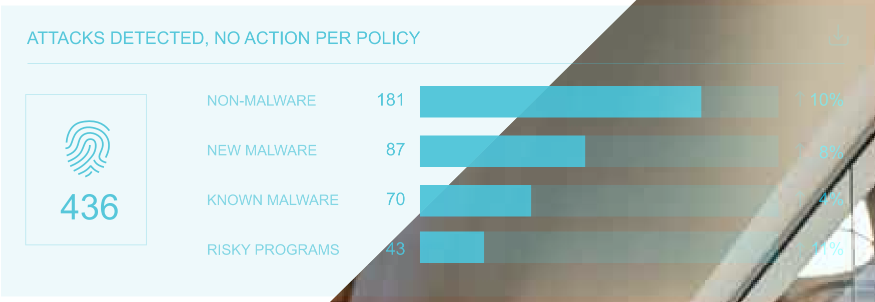
of security professionals said the volume of attacks they faced has increased

80%

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

67%

of security professionals say attacks have become more sophisticated, 22% of those say they have become significantly more advanced



Third Party Breach Risk On The Rise

Crucially, this report reveals a shift in the causes of successful breaches. OS vulnerability is the most common cause, comprising one fifth of breaches, but third party application breaches account for 15%, more than double the impact they had in our last report. Island hopping has more than trebled in attack frequency compared to October 2019 and is now the most commonly experienced attack for 10%. It has caused 12% of breaches. Clearly, the extended enterprise ecosystem is generating considerable security concerns.

Reputations In The Firing Line But Profits Less So

As public awareness of data protection rights has grown, and regulatory fines have hit the headlines, so you would expect the impact of breaches to continue to rise. However, whilst a slightly increased proportion of respondents reported severe reputational damage, fewer have indicated severe financial impact.

Budgets Rise Again But Will Spending Be Strategic Or Tactical?

Singaporean security professionals are responding to the current cyber threats by boosting cyber defense spending. 90% of our survey participants anticipated an increase in spend, a decrease from the 99% who planned increases last time, but a healthy number nonetheless.

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

In our October 2019 survey, 98% of respondents said they had security concerns around the implementation and management of digital transformation and 5G. But, when it comes to the crunch, opinion is split on the need for security spending. 54% say they will be adopting 5G and need to increase security spending and controls, while 33% will be adopting but won't be focusing their budgetary increases on securing 5G.

12%
Island hopping has more than trebled in attack frequency compared to October 2019 and is now the most commonly experienced attack for 10%.

90%
of our survey participants anticipated an increase in spend,

54%
say they will need to increase security spending and controls to support 5G rollout

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 eleven different consoles or agents to manage their security program. This indicates a security environment that has evolved reactively as security tools have been bolted on to tackle emerging threats, not built-in. This has resulted in siloed, hard-to-manage environments that hand the advantage to attackers from the start; evidence shows that attackers have the upper hand when security is not an intrinsic feature of the environment. As the cyber threat landscape reaches saturation, it is time for rationalization, strategic thinking and clarity over security deployment.

Recognition For 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. 82.5% 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.

11
Singapore respondents are using an average of more than nine different consoles or agents to manage their security program.

82.5% vs 56%
82.5% are aware of the MITRE ATT&CK® framework and 56% 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 third Singapore Threat Report useful and informative.

COVID-19 Supplemental Research Findings

250 Singaporean 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 organizations."

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

An astounding 93% of all Singaporean respondents stated that they had seen an increase in overall cyberattacks as a result of employees working from home.

Just over a **quarter (26%)** recounted that attack increases had gone up by between 25 and 100% with 8% of these 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 because of COVID-19 and the mean percentage increase in attacks for Singaporean respondents excluding this one person was **20.44.**

The financial services sector mean percentage was below the overall average at 19.37 with three quarters of organizations (75%) witnessing the majority of increase in the less than 25% category.

Companies with between **251 and 500** and **501 and 1000** employees experienced a mean increase in attacks of **21.53 and 21.73** respectively with 30% in the **501 and 1000** category stating that they had witnessed increases in attacks between 25 and 100%.

93%

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

52%
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?

Over half (52%) 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, 86% reported gaps, be that severe or slight, in communication with external parties.

Over a third (36%) reported very significant gaps in disaster recovery planning in **IT operations** including hardware and software roll outs. Overall, 86% reported gaps, be that severe or slight.

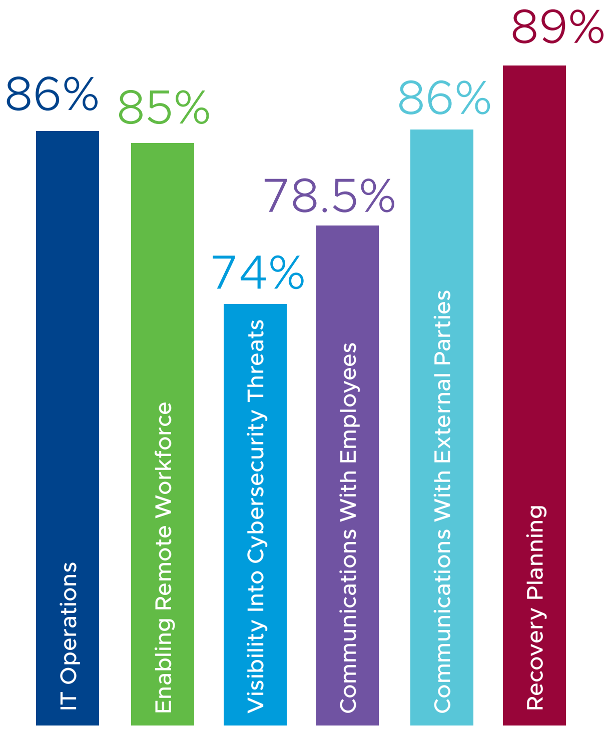
In terms of enabling a remote work force, severe and significant gaps were felt by 22% of survey respondents, and overall, 85% of respondents felt that there were gaps in their planning.

Just over a third (35%) of Singaporean respondents felt that there were very significant gaps in their **visibility into cybersecurity threats** with an additional 38.5% stating that these were slight.

27.5% admitted to severe gaps in dealing with the situation in terms of **communication with employees** and overall, 78.5% of respondents stated that these were either slight or very significant.

With regard to **recovery planning** 31% of respondents identified very significant gaps and 89% highlighted gaps of some kind.

Three respondents opted out from answering this question.



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

32%
Nearly a third of respondents (32%) 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?

Nearly a third of respondents (32%) recounted the **inability to institute multi-factor authentication** as the biggest threat to their company. Second to this was **COVID-19 malware** with 14% and third was **phishing emails** (12%). 9% cited **spear phishing,** 8% stated inability to roll out timely **software patches, and IoT exposure.**

Other notable threats were **social engineering** (4%), **masquerading** (3%), and **ransomware** (2%).

The **inability to institute multi-factor authentication** was the biggest threat for financial services organizations with 47% claiming this to be the case. Likewise, COVID-19 related malware (12%) and phishing emails (13%) was also an issue for this vertical.

For company sizes of 251 to 500 employees the biggest impact was the **inability to institute multi-factor authentication** (42%).

Those with IT team sizes of 21-30 reported the biggest threat impact (50%) was the **inability to institute multi-factor authentication.** This was followed by teams with 31-40 staff with 43%.

90%
The highest increase in threat changes during COVID-19 was seen with COVID-19 related malware, phishing, an inability to institute multi-factor authentication and IoT exposure

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

The highest increase in threat changes during COVID-19 was seen with COVID-19 related malware, phishing, an inability to institute multi-factor authentication and IoT exposure which all saw 90% reporting overall threat change increases. That said, COVID-19 related malware reported more than half (52%) in increases from 51 to over 100% which was far higher than the other three.

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 surprisingly the lowest with respondents only reporting 60% in overall threat change increases.

Nearly a third of Singaporean respondents (32%) 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 also high with 90% reporting overall threat change increases and 30% of the respondents reporting increases between 51 and more than 100%.

Full Survey Findings

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

A surprisingly low 43% of Singapore organizations have seen an increase in the number of cyberattacks on their company in the last twelve months. This is a considerable decrease from 93% in the October 2019 report. A significant percentage of respondents were reticent this time, preferring not to say whether attacks had increased.

Respondents reported an average increase in attack frequency of 33%. Of these, 24% said there had been a 1-50% increase (compared with 58% who said this last time). 18% said there had been between a 51%-100% increase (28% last time). A fifth of respondents (20%) preferred not to say whether or not they had seen an increase in cyberattacks in the past 12 months.

63% of **financial services** had seen a 51-100% increase. Large percentages of **healthcare** respondents (32.5%) and an even larger percentage of **food and beverage** respondents (43%) preferred not to say.

Mid-sized companies are the target with 43.5% of respondents from organizations in the 501-1000 employee bracket reporting an increase in cyberattacks of between 51-100%.

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

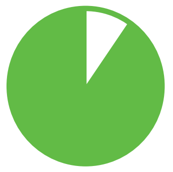
67% of respondents who have suffered a cyberattack in the past 12 months say the attacks have grown more sophisticated – this compares with 92% in October 2019. Of these, 22% said they had become **significantly** more sophisticated (a slight decrease on 27% last time). 16% said **moderately** more sophisticated (46% last time) and 29% said **slightly** more (19% last time.)

64% of **financial services** respondents say attacks were significantly more sophisticated and 41% of **media and entertainment** say either **moderately** or **significantly** more sophisticated.

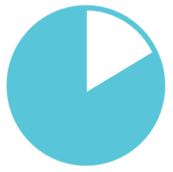
Surprisingly 23.5% of **healthcare** respondents say slightly **less** sophisticated and 18% say no change in sophistication at all.

Again, mid-sized companies seem to be the target for more sophisticated attacks. 49% of companies with 501-1000 employees say attacks have become **significantly** more sophisticated.

This correlates with mid-sized IT teams (31-40 headcount) where 56% say the attacks have become **significantly** more sophisticated.



43%
of Singapore organizations have seen an increase in the number of cyberattacks on their company in the last 12 months



67%
of respondents say attacks have grown more sophisticated

80% 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 with 28% (up from 13% 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 with 28% (up from 13% last time). **SSH (brute force attacks)** are second on the list (19%) up from 7% last time. This is followed by **island hopping** which accounts for 10% up from 3% on the last report. **Commodity malware** (9%) and **Formjacking** (9%) make up the top 5.

Interestingly **ransomware** has dropped from being the most prolific (15%) in our last report to being tenth on the list (2%) this time around.

Financial services are at the mercy of custom malware with 75% saying this was the most frequently experienced attack (compared with an average of 28% and compared with 7% on our last report). **Food and beverage** (35%), **healthcare** (38%) and **media and entertainment** (23%) were most likely to see SSH attacks.

Mid-sized companies in Singapore with between **501-1000** employees are more affected by **custom malware** (55%). This correlates to mid-sized IT teams of between **31-40** where 57% say **custom malware** is most prevalent.

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

80% 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 down from 96% who said they had been breached in October 2019.

The average number of breaches suffered by organizations is 1.67, down from an average of 3.82 in our last report. The largest group of respondents (59%) said they had suffered one breach. 24.5% admitted to two breaches. Only 3% said they had had 5 or more breaches.

Singaporean SMEs had higher breach frequency, with companies with 50-500 employees reporting 1.92 breaches per year on average.

Media and entertainment organizations reported the highest average number of breaches at 1.77, and 4.5% of these respondents had suffered five or more breaches.

OS Vulnerabilities

The top cause of breaches was identified as OS vulnerabilities

4%

There is a significant drop in ransomware attacks which were responsible for 29% of breaches last year and just 4% this year.

18%

of respondents said they had suffered negative reputational impact as a result of 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. **3rd party application** breaches were in second place at 15%, up from 6.5% last time. **Web application attack** is third with a slight increase (12.5% compared to 9% last report) and island hopping is 4th responsible for 12% of breaches compared with 6% last time.

There is a significant drop in ransomware attacks which were responsible for 29% of breaches last year and just 4% this year. Likewise, phishing attacks have also dropped as a cause of successful breaches – it was the number two last year (19%), but has dropped to just 9% on this report.

Financial services (66%) companies are most affected by OS vulnerability breaches. Island hopping is most prevalent in **food and beverage** (22%) **healthcare** (15%) and **media and entertainment** (18%). Despite its drop, **phishing** is still the cause of 21% of **healthcare** breaches.

OS vulnerability is the biggest cause of breaches for organizations sized 501-1000 (49%). It is also most prevalent in companies with IT sizes of 31-40 (53%).

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 significantly and the percentage of organizations severely financially impacted as a result of a breach is also down.

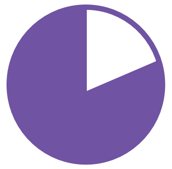
Just 1% of repondents reported severe financial impact compared with 15% in October 2019. **Media and entertainment** organizations were most likely to report severe financial impact (9%).

Almost one fifth (18%) of respondents said they had suffered **severe** reputational impact as a result of a breach, up slightly from 17% who said the same in October 2019. But **financial services** companies seem to buck this low severity trend with 59% saying breaches had caused **severe reputational impact.**

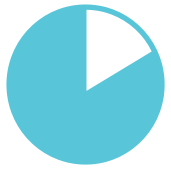
In The Last 12 Months Did Your Company's Threat Hunting Achieve A Goal Of Strengthening Its Defenses Against Cyberattack And Did The Threat Hunting Find Malicious Cyberattack Activity You Would Not Have Ordinarily Found?

Threat hunting is becoming ubiquitous, with 98% of respondents using it as part of their cybersecurity strategy, equal to the number reported in October 2019. It is also proving effective; overall 92% said it had strengthened their company's defenses, with 24% of those saying it significantly strengthened them, a decrease from 41% on the previous survey.

The percentage finding **significant evidence** of malicious activity more than halved to 22% (compared to 49% last time) while overall 77% found some evidence of malicious activity through threat hunting – this is a decrease on the 91% who reported finding evidence in the October 2019 report.



22%
the percentage finding significant evidence of malicious activity more than halved to 22%



98%
of respondents are using threat hunting as part of their cybersecurity strategy.

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

90% of the CISO/CIOs we surveyed said they plan to increase budget spend on cyber defense in the next 12 months, with an average expected increase of 32%. 47% say they plan to boost budget by 31-40%.

68% of **financial services** companies are planning to increase budgets by 31-40%. 55% of **healthcare** organizations plan to increase by the same. 10% of **food and beverages** respondents are planning to increase spend by 41-50%.

90%
of the CISO/CIOs surveyed said they plan to increase budget spend on cyber defense

87%
of CISOs and CIOs plan to adopt 5G in the next 6 – 12 months

11.01
is the average number of technologies deployed

26%
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)?

87% of the CISOs/CIOs we surveyed said they were planning to adopt 5G over the coming 12 months, with 29% expecting to do so in the next six months. They are split on the security implications. 54% say they will need to increase security spend to manage adoption, while 33% don't believe they will need to invest.

Financial services organizations are most likely to adopt in next 6 months with 40% saying they will be investing in related security and controls. However, 31% believe they will not need to increase spend due to their adoption in the next 6 months.

61.5% of **media and entertainment** respondents will be adopting in the next 12 months and will need to increase security spends and controls as a result.

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

Over half (58%) of companies have between 5 and 10 different technologies deployed to manage their security program. 36% have 11-25 different technologies.

The average number of technologies deployed is 11.01 – this rises to a staggering 13.45 in **food and beverages** where 57% have between 11-25 different technologies.

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 Singapore, but respondents are split over whether to adopt it. 26% are aware of it but have no plans to implement it, while 56% are aware and plan to use it.

The **healthcare** sector is the most positive about the framework, with 62.5% aware of it and planning to use it. The most sceptical are respondents from the **financial services** sector, where 47% say they are aware of it but don't plan to use it.

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

Networks lead the field at 62.5%, followed by **mobiles** at 53%, then **endpoints** – 50% – and finally **workloads/applications** at 37.5%.

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

Network is seen as the biggest risk, cited by 47% of respondents, followed by **workload/apps,** identified by 21%. The next most commonly cited risk is **mobile devices** 18%, with **endpoints** such as laptops and desktops coming in at 12%.

Food and beverage organizations see higher than average risk from their network (63%), as do respondents from the **travel and transport industry** (59%). **Media and entertainment** organizations see higher than average risk from workload/applications (31%) and **financial services** from mobile (56.5%).

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