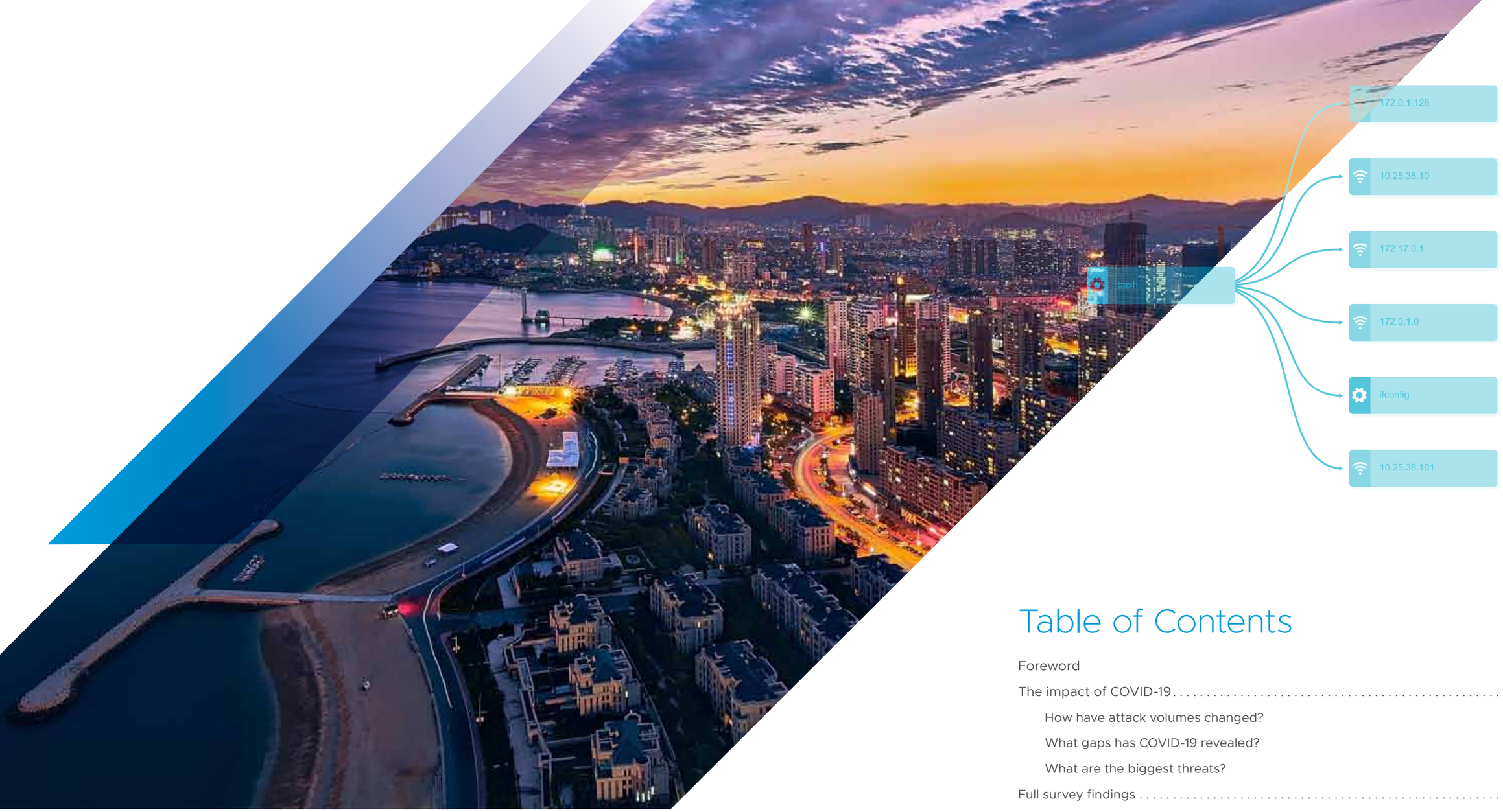
vmware Carbon Black

USA Threat Report

Extended enterprise under threat

June 2020



Introduction

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

Table of Contents

THE 2020 USA CYBERATTACK LANDSCAPE

Rick McElroy
Cyber Security Strategist, VMware Carbon Black

Foreword

In this, our first USA threat report, we find that cyberattack frequency is at unprecedented levels; 92% of security professionals said the volume of attacks they faced has increased. Attackers are employing a diverse range of tactics and techniques as they bid to extort, disrupt and infiltrate organizations.

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

97% of USA organizations have suffered a data breach as a result of a cyberattack in the past 12 months and the average organization has experienced 2.70 breaches.

49% of organizations have been breached between 3 and more than 10 times

The level of attack frequency revealed in this report shows that, however fast USA businesses may be adapting to the intensifying environment, the cyber threat landscape is evolving faster. 84% of security professionals say attacks have become more sophisticated, 18% of those say they have become significantly more advanced with 66% stating that attacks have become moderately or slightly more sophisticated. This confirms what VMware Carbon Black Threat Analysis Unit research has been finding: adversaries are adopting more advanced tactics as also the commoditization of malware is making more sophisticated attack techniques available to bigger cohort of cybercriminals. The most prolific types of cyberattacks were custom and commodity malware followed by supply chain attacks.

METHODOLOGY

VMware Carbon Black commissioned a survey, undertaken by an independent research organization, Opinion Matters, in March 2020. 250 North American 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 first USA Threat Report from VMware Carbon Black and forms part of a global research project across multiple countries, including: Australia, Canada, France, Germany, Japan, Italy, Netherlands, Nordics, Singapore, Spain, UK and the USA.

92%

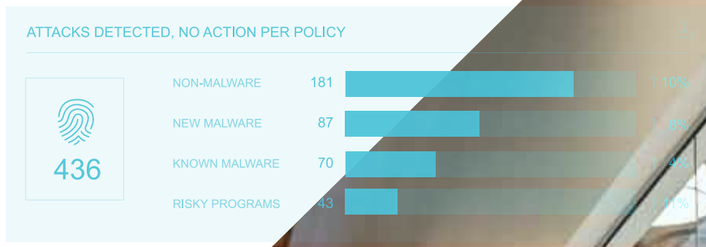
of security professionals said the volume of attacks they faced has increased

97%

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

84%

of security professionals say attacks have become more sophisticated, 18% of those say they have become significantly more advanced



Third Party Breach Risk On The Rise

In addition to the general escalation in intensity, this report reveals the prime causes of successful breaches. OS vulnerability was the top cause of breaches for US organizations (27%) followed by web application attacks and ransomware but breaches via the supply chain (9%) and island hopping (5%) are starting to creep up. 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 a significant proportion of respondents reporting financial and reputational damage.

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

North American security professionals are responding to the uptick in cyber threats by boosting cyber defense spending. 95% of our survey participants anticipated an increase in spend.

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 survey 83% of respondents plan to implement 5G in the next 6 to 12 months. But, opinion is split on the need for additional security spending. 43% say they will need to increase security spending and controls, while 40% 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 nine 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. As the cyber threat landscape reaches saturation, it is time for rationalization, strategic thinking and clarity over security deployment.

27%
OS vulnerability was the top cause of breaches for US organizations (27%)

95%
of our survey participants anticipated an increase in spend,

43%
say they will need to increase security spending and controls to support 5G rollout

Understanding The Value Of Security Frameworks

Visibility and validation of security posture can be significantly enhanced by the application of the MITRE ATT&CK® framework, and North American respondents are aware of the relevance and value of this approach. 84% are aware of it, and 74% plan to use it to validate security posture, 16% were not aware of it and 11% were aware of it but didn't plan to use it. This demonstrates that while awareness is high there is still some work do to establish this framework as the gold standard among enterprises.

Networks Seen As Biggest Breach Risk

Networks top the list for breach risk among respondents, with nearly half saying it's their biggest breach risk. But close behind is workloads and apps; cited as the biggest risk for a third of organizations. This is perhaps not surprising as businesses run more and more apps in a bid for flexibility and productivity gains; ensuring their security will become of critical importance.

9
US respondents are using an average of more than nine different consoles or agents to manage their security program.

84% vs 74%
84% are aware of the MITRE ATT&CK® framework and 74% 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 first USA Threat Report useful and informative.

COVID-19 Supplemental Research Findings

250 North American 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?

88% of all North American respondents stated that they had seen an increase in overall cyberattacks as a result of employees working from home.

Just under **a third (32%)** recounted that attack volumes had gone up by between 25 and 100% with 4% 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 North American respondents excluding this one person was **19.39.**

The financial services sector mean percentage was below the overall average at **16.47** with more than three quarters of organizations (78%) witnessing the majority of increases in the less than 25% category.

Companies in the **501 - 1000** employee category experienced the highest mean percentage increase in attacks of **24.58,** with 38% stating that they had witnessed increases in attacks between 25 and 49%.

Team sizes between **31-40** had the highest mean average of **23.55** and 40% said they had experienced an increase in cyberattacks of between 25 and 49%.

88%

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

NEARLY HALF

(49%) 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?

Nearly half (49%) 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, 83% reported gaps ranging from severe to slight in communication with external parties.

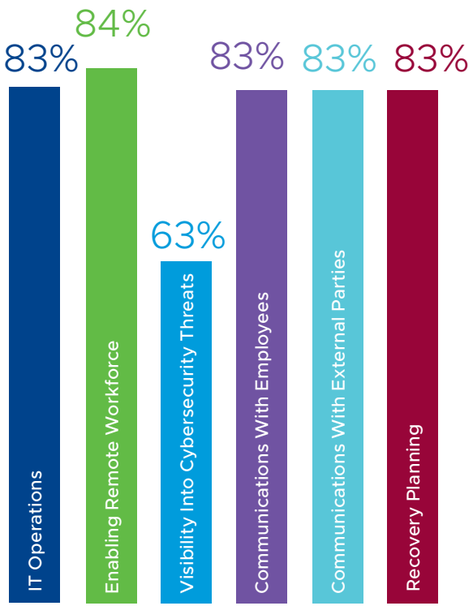
One third (33%) reported very significant gaps in disaster recovery planning in **IT operations** including hardware and software roll outs. Overall, 83% reported gaps, be that severe or slight.

In terms of **enabling a remote work force,** severe and significant gaps were felt by 26% of survey respondents, and overall, 84% of respondents felt that there were gaps in their planning.

Just under a third (31%) of North American respondents felt that there were very significant gaps in their **visibility into cybersecurity threats** with an additional 32% stating that these were slight.

30% admitted to severe gaps in dealing with the situation in terms of **communication with employees** and overall, 83% of respondents stated that these were either slight or very significant.

With regard to **recovery planning** 30% of respondents identified very significant gaps and 83% highlighted gaps of some kind.



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 **inability to roll out timely software patches** with 17% and together in joint third were **phishing emails** and **COVID-19 related malware** with (8%). 7% cited **IoT Exposure,** 6% stated **masquerading.** Other notable threats were **spear phishing** (6%), **ransomware** (4%), and **social engineering** (4%).

The **inability to institute multi-factor authentication** was the biggest threat for **financial services** organizations with 61% claiming this to be the case.

For company sizes of **251 to 500** employees the biggest impact was the **inability to institute multi-factor authentication** (51%).

Those with team sizes of **21-30** reported the biggest threat impact (52%) was the inability to **institute multi-factor authentication.** This was followed by teams with **31-40** staff with 30%.

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 89% and more than a third (36%) of these increases were in the 51 to over 100% category. Second to this was **phishing emails** with 87% reporting threat change increases, and a quarter of these were in the 51 to over 100% category. **Masquerading** was also significantly high with 86% overall increases in threat changes and over a quarter (27%) of these were also in the 51 to over 100% category.

89%

The highest increase in threat changes during COVID-19 was with COVID-19 related malware, which saw overall threat change increases of 89%

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 70% in overall threat change increases.

Nearly a third of North American 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 in general during COVID-19, this was also high with 83% reporting overall threat change increases and 21% 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 staggering 92% of North American organizations have seen an increase in the number of cyberattacks on their company in the last 12 months.

23% of respondents reported an increase in attack volumes between 1-25%, 42% between 26-50% and 24% saw an increase between 51-100%. 4% actually reported increases between 101 and 300%.

The **financial services** sector had by far the highest average increase in attacks experienced at 56%, above the norm of 45%. In particular 43% of respondents in this sector witnessed rises in the 51-100% category. **Healthcare** was also above average with 49% increases, with 48% of respondents reporting rises in the 26-50% category.

42% of companies in the 501-1000 employee bracket had seen a 51-100% increase which again was above average.

IT team sizes of between 31-40 reported above average attack increases with an average increase of 58% 49% of these teams reported increases in the 26-50% range while 35% of respondents with teams of this size said attacks had increased between 51-100%.

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

84% of respondents say attacks have grown more sophisticated over the last 12 months. Of these, 18% said they had become **significantly** more sophisticated and 38% said moderately more sophisticated. 13.5% said that there had been no change while 3% felt that attacks had either become slightly, moderately or significantly less sophisticated

38% of **healthcare** respondents felt that attacks had grown significantly more sophisticated compared to the overall average of 18%. 60% in **financial services** felt that attacks had become moderately more sophisticated compared to an average of 38%. Overall, **financial services** scored highly with 93% saying that attacks have become more sophisticated.

Nearly a quarter (23%) of companies in the 501-1000 category stated that attacks had become significantly more sophisticated. Likewise, 47.5% said that attacks have become moderately more sophisticated. 91.5% of those with an IT team size of between 31-40 have seen either significantly, moderately or slightly more sophisticated attacks.

92%

of North American organizations have seen an increase in the number of cyberattacks on their company in the last 12 months

84%

of respondents say attacks have grown more sophisticated

97% of the CISO/CIOs that took part in our research said they had suffered a breach following a cyber attack in the past 12 months.

Custom malware tops the table with over a quarter of respondents (29%) seeing it as the most frequent attack type

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 over a quarter of respondents (29%) seeing it as the most frequent attack type. Commodity malware (11.5%), supply chain attacks (9%), and ransomware (7%) also figured in the top 5.

Indicating a growing attacker focus on gaining undetected access to networks, the frequency of **process hollowing** attacks was quite high, at 5%. Also appearing on the attack radar is **island hopping,** seen in 2% of incidents. While this figure may seem relatively low, these types of attacks are proving effective, as later analysis shows.

Custom malware was highest in the **financial services** sector with 62% of companies citing this. Followed by commodity malware at 12%. **Healthcare** saw above average attacks in commodity malware with 14%.

Custom malware was cited highest in companies from 501-1000 employees, with 49%, and in IT team sizes of between 31-40 (39%).

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

97% of the CISO/CIOs that took part in our research said they had suffered a breach following a cyber attack in the past 12 months.

The average number of breaches suffered by organizations is 2.70. 49% of respondents said they had suffered between 3 and 10 breaches. 18% reported they had been breached twice.

Media and entertainment organizations had the highest average breach frequency at 3.44. 50% of **manufacturing and engineering** companies have been breached 3 times.

38% of organizations in the 251-500 employee category say they had been breached 3 times

The 21-30 size IT teams have seen above average persistent breaches with 28% of them being breached 3 times.

OS Vulnerabilities

The top cause of breaches was identified as OS vulnerabilities

5%

despite only featuring in 2% of the attacks experienced, island hopping was the cause of 5% of breaches.

62%

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 vulnerability (27%).** This was followed by web application attacks (13.5%) and ransomware (13%).

Financial services (70%) are most affected by **OS vulnerability** breaches.

Interestingly, despite only featuring in 2% of the attacks experienced, **island hopping** was the cause of 5% of 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. Breaches caused via the supply chain also features quite highly at 9%.

Surprisingly, **phishing attacks** were fifth on the list as a cause of successful breaches at 9%.

Companies in the 501-1000 category suffered very high rates of breach caused by OS vulnerability attacks (59%)

IT Teams in the 31-40 member category were very prone to OS vulnerability with 44% claiming this to be the prime cause of breaches compared to the average of 27%.

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 was 19% with 68% claiming that there had been no negative impact financially.

However, 62% of respondents said they had suffered negative reputational impact as a result of a breach, and 12% of these said that this impact was severe.

90% of companies in the financial services sector said they had suffered reputational impact as a result of a breach.

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 more effective; overall 87% said it had strengthened their company's defenses, with 8% saying it significantly strengthened them.

The percentage finding **significant evidence** of malicious activity was 27%, while overall 86% found some evidence of malicious activity through threat hunting.

86%
found some evidence of malicious activity through threat hunting

88%
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?

95% of the CISO/CIOs surveyed said they plan to increase budget spend on cyber defense in the next 12 months, with an average expected increase of 25%. 42% say they plan to boost budget by 21-30%, 21% by 31-40% and 3% say they plan to increase budget by as much as 41 to 50%.

Financial services organizations are planning budget increases slightly above average at 30% with 46% of these respondents saying they plan increases of between 31-40%.

50% of **healthcare** companies are also planning a 21-30% increase.

Organizations in the 501-1000 employee category are planning above average increases at 29%.

51% of organizations in the 251-500 employee category are planning increases of 21-30%. 43.5% of organizations in the 501-100 employee category are planning increases of 31 to 40%.

95%
of the CISO/CIOs surveyed said they plan to increase budget spend on cyber defense

83%
of CISOs and CIOs plan to adopt 5G in the next 6 – 12 months

9
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)?

83% of CISOs and CIOs plan to adopt 5G in the next 6 – 12 months. 53% expect to do so in the next six months and 14% say they expect to have to increase spend on security and controls, 39% of respondents don't expect to have to increase spending. 29% are adopting 5G in the next 12 months and will need to change security controls and security spend. Only 17% of the IT leaders that were surveyed said they had no plans to adopt 5G in either the next 6 or 12 months.

In the next 6 months, **financial services** is going to be a big adopter of 5G with 77% stating this to be the case but only 13% will need to increase security spend and controls, as 64% stated that they won't need to invest any additional budget. In **healthcare** 43% believe they'll need to support their 5G rollout with security spend over the next 12 months. Overall **healthcare** is the biggest adopter with only 7% stating that they have no plans to adopt 5G.

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

Just over two thirds (68%) of companies have between 5 and 10 different technologies deployed to manage their security program. 21% have 11-25 different technologies.

The average number of technologies deployed is 9. IT teams of 31-40 people are using more tools on average – 11.93 compared with an average of 9.25.

The **financial services** sector had a very high average at 11.36 with 56% adopting 5 to 10 technologies and 39% adopting 11 to 25.

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, with 84% stating they are familiar with it. Of those that are aware of it 74% plan to use it while 11% are aware of it but have no plans to implement it. Only 16% were not aware of the framework at all but 10% said that they would like to understand more about it.

The **financial services** sector is the most familiar with the framework; 84% are aware of it and plan to use it, likewise so do 79.5% of healthcare companies.

84% of those in the 501 – 1000 employee company category plan to use the framework.

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 led the field needing a reprioritization of budget for 68% of respondents, followed by workload/applications - 59%, then mobiles – 27% and finally endpoints at 15%.

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

Networks are seen as the biggest risk, cited by 44% of respondents, followed by **workload and applications,** identified by one third (33%). The next most commonly cited risk is **mobile devices** (13%), with **endpoints** such as laptops and desktops coming in at 6%.

Financial services see higher than average risk from mobile devices (33%). 27% of organizations in the 501-1000 category view mobiles as the second biggest breach risk behind networks.