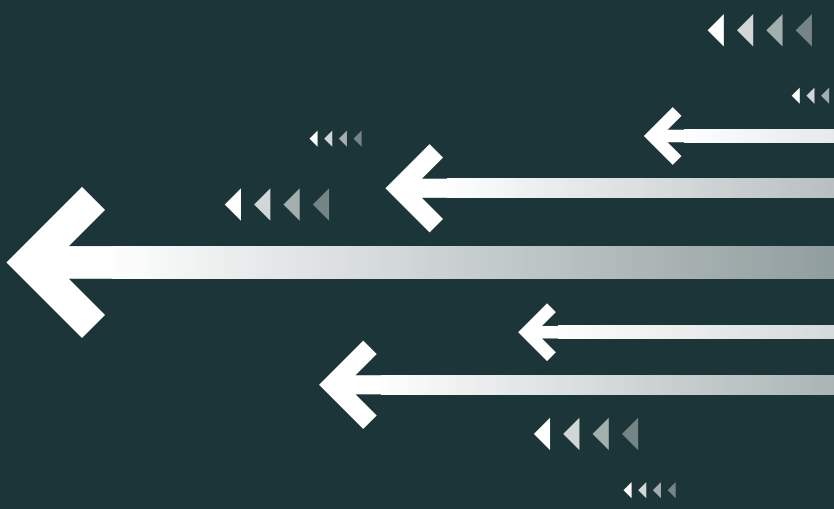
CROWDSTRIKE

2020 CROWDSTRIKE GLOBAL SECURITY ATTITUDE SURVEY

INSIGHTS INTO SECURITY TRANSFORMATION AND PREVALENT ATTACK VECTORS IN A WORK FROM ANYWHERE WORLD

As everyone is well aware, cybercrime is an increasingly profitable line of work for those with a questionable moral compass and the skills to turn an opportunity into the source of significant income. This spells trouble for businesses that rely on technology to perform tasks and hold any form of data that is considered valuable enough for hackers to steal.



And while much has changed during 2020, the complexity of cybersecurity was already increasing, but undoubtedly the COVID-19 pandemic and the subsequent necessity of supporting a remote workforce has made life even harder for IT security teams in organizations around the world.

Many cybercriminals out there have been trying and will continue to try their utmost to **capitalize on the chaos** and confusion that this pandemic has caused. However, as organizations begin to come to terms with a new way of living and working, these cybercriminals could become increasingly dangerous.

Any complacency when it comes to maintaining effective security of the organization would be extremely costly, so even for those that have not fallen victim to a successful cyberattack in recent times, now is the time to double down on your security transformation efforts.

If, for any reason, you find yourself unconvinced as to the threats posed by cybercriminals in the wake of the COVID-19 pandemic, then read on to find out why you should be more concerned. This white paper explores many different areas including, but not limited to, the following:

- ***How the threat of ransomware has changed and how costly this is when there is no other option but to pay the ransom***
- ***Why nation-state actors now seem to be more motivated than ever to target organizations***
- ***The critical importance of layering security transformation into your digital transformation strategies***
- ***Whether, over the course of the past year, organizations have moved any closer to the 1-10-60 ideal for detecting and containing a threat in their network***

At a time when the physical and mental health of your company's workforce is of paramount importance, performing a detailed health check of your organization's cybersecurity strategy and infrastructure is of paramount importance as well.

To form a picture of organizations' attitudes about cybersecurity around the globe, a total of 2,200 senior IT decision makers and IT security professionals were interviewed during August and September 2020, with representation across the U.S., EMEA and APAC regions. All respondents had to be from organizations with 250 or more employees and are from a range of private and public sectors.

Key findings

71%

of surveyed cybersecurity experts are **more worried about ransomware attacks** now as a result of the COVID-19 pandemic

56%

of respondents report that their organization **has suffered from a ransomware attack** in the last 12 months

27%

of those who experienced a successful attack **ended up paying the ransom**, at an average cost of $1.1 million (USD)

87%

of respondents believe that **nation-state-sponsored cyberattacks are far more common** than most people think

73%

agree that **nation-state-sponsored cyberattacks will pose the single biggest threat** to organizations like theirs in 2021

63%

report that their organization is **concerned about nation-state cyberattackers** - a steady increase since 2018 (54%) and 2019 (59%)

61%

report that their organization has **spent $1 million (USD) or more on digital transformation** in the last three years - on average $4.86m (USD)

84% of respondents' organizations have **accelerated their digital transformation efforts** as a direct result of COVID-19

Modernizing security tools (45%) and **increasing cloud rollout to support employees working remotely (44%)** have been key changes in response to COVID-19 challenges

79% believe that COVID-19 has had a **positive impact** on their organization's outlook regarding its **overarching security strategy and architecture** for the next 12 months

117 hours

Average estimated **time to detect a cybersecurity incident or incursion** – barely showing an improvement over the 120-hour average in 2019

52%

believe that **COVID-19 has slowed down the average time** it takes for their organization to detect a cybersecurity incursion

73%

report that **COVID-19 has proven to be a catalyst** for long-awaited approvals on security upgrades

The Proliferation of Ransomware

The threat of suffering from a successful ransomware attack has been a thorn in the side of organizations around the globe for many years.

The potential financial damage and severe negative consequences for a company's reputation that ransomware attacks carry will send shivers down the spines of even the most battle-hardened IT security professionals across all levels of a business.

These devastating impacts are clearly well understood by surveyed senior IT decision-makers (ITDMs) and IT security professionals, with 54% reporting that ransomware is among the attack vectors causing the most concern in their organizations looking ahead to the next 12 months. And since 2019, concern around ransomware has increased fairly dramatically, with just over four in ten (42%) respondents reporting last year that it was something their organization was worried about. In fact, this type of cyberattack has seen the largest proportional increase since the 2019 survey, even when compared to other common attack vectors such as general **malware** (53% in both 2019 and 2020) and **phishing/spear-phishing** (49% in 2019 vs. 52% in 2020).

Unfortunately, on top of the social and economic impacts that the COVID-19 pandemic has had around the world, a further consequence has been the increased opportunities for cybercriminals to take advantage of compromised IT networks, while organizations have been grappling with their transition to remote working.

This is possibly best demonstrated by the fact that 71% of surveyed cybersecurity experts are more worried about ransomware attacks now, as a direct result of COVID-19 — this attitude shift is particularly prevalent among respondents from India (83%).

Types of cyberattack causing the most concern over the next 12 months
2020 vs. 2019

56% admit that their organization has suffered from a ransomware attack in the last 12 months, while a further 28% believe that their business will fall victim to such an attack in the future

Perhaps the more concerning point is that these increasing fears around ransomware are partly the result of many organizations having already been on the receiving end of a successful attack. Approaching six in ten (56%) respondents admit that their organization has suffered from a ransomware attack in the last 12 months, while a further 28% believe that their business will fall victim to such an attack in the future. And it would appear that the concern levels displayed by respondents from India are well-founded, with 75% working for an organization that has fallen foul of a ransomware attack in the last year – the highest proportion of any surveyed country.

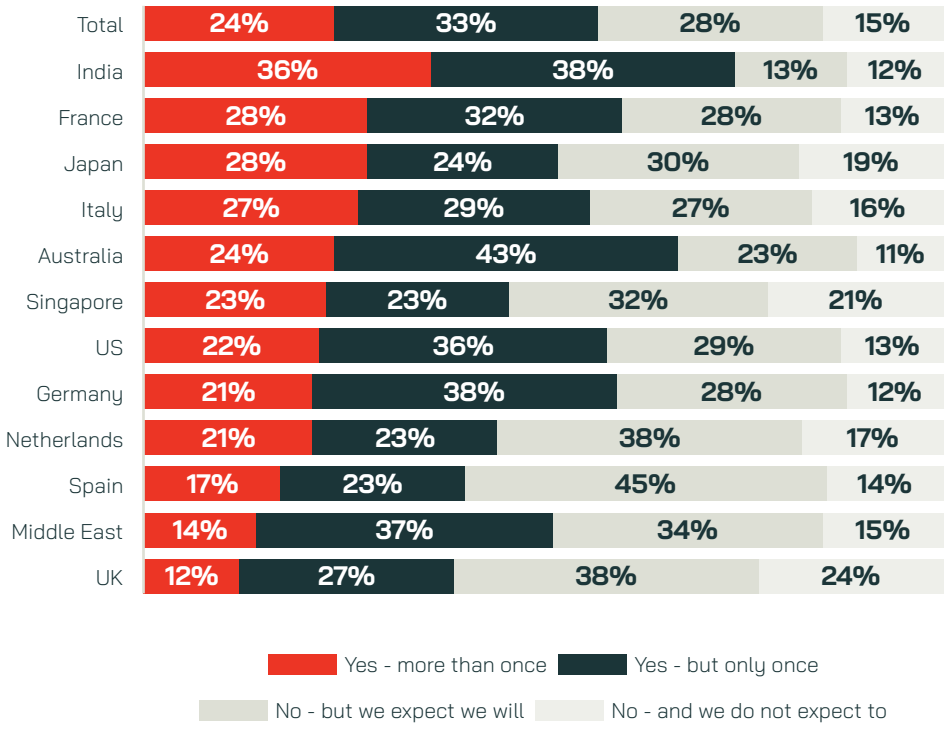
Given these figures, it seems that the question is no longer about if an organization will suffer a ransomware attack, but rather when it will happen.

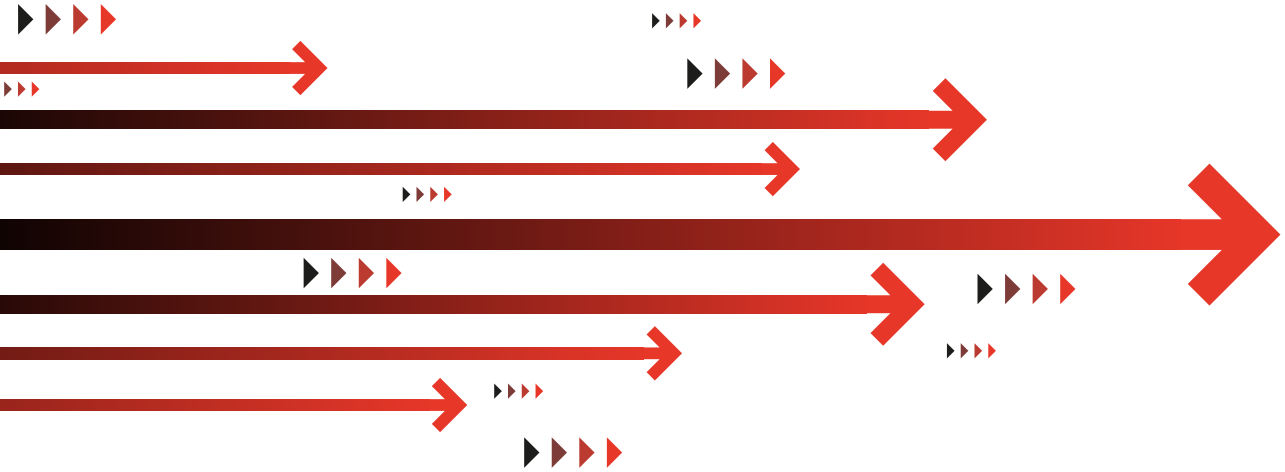
But how have organizations reacted when a successful ransomware attack has struck?

Well, largely the response has been a positive one. More than three-quarters (76%) of respondents report that in the wake of a successful ransomware attack, their organization upgraded its security software and infrastructure in order to reduce the risk of future attacks, while 65% upgraded their security staff with the same purpose in mind.

Extent of ransomware attacks in the past 12 months

By country





However, regardless of these positive improvements, for a notable minority (27%) of respondents' organizations, they were left with no other option but to pay the ransom, which cost them $1.1 million (USD), on average. And in the APAC region, this average is markedly higher at $1.18 million (USD).

Further, the dangers of ransomware for smaller organizations are amplified and could carry more severe consequences. Even though the average ransom paid by those with 250-1,999 employees is slightly lower ($1.07 million USD) than those with 2,000 or more employees ($1.13 million USD), as a proportion of profits or revenue, a large ransom payment such as this could deliver a knockout blow to a smaller company. For the 8% of these smaller companies that paid at least $2.5 million (USD), their fears might well have turned into an extremely harsh reality.

The financial rewards available to cybercriminals brazen enough to carry out a ransomware attack are too lucrative for them to forego, and as such, this attack vector is here to stay. This means that organizations around the globe must modernize their approach to cybersecurity if they hope to protect themselves against ransomware because paying in excess of $1 million (USD) each time they are victimized is clearly not a sustainable business model. And that is without even considering the sanctions that could be imposed and reputational ramifications that often come with suffering such an attack.

With the clear upward trend in levels of concern about ransomware among surveyed respondents, it stands to reason that there is the potential for the prominence of ransomware attacks to also move on this upward trajectory. Therefore, it is of paramount importance that organizations act upon the fears of their cybersecurity professionals and take the necessary steps to avoid falling victim to ransomware.

The financial implications of not doing so are far too great!

Paying the ransom

27%

report that their organization had no other option but to pay the ransom following an attack

$1.1m

Average ransom amount paid

$0.99m	$1.06m	$1.18m
US	EMEA	APAC

Nation-States Present a Huge Threat Regionally

Undoubtedly, these are uncertain times, and they provide opportunities for all forms of cybercriminal.

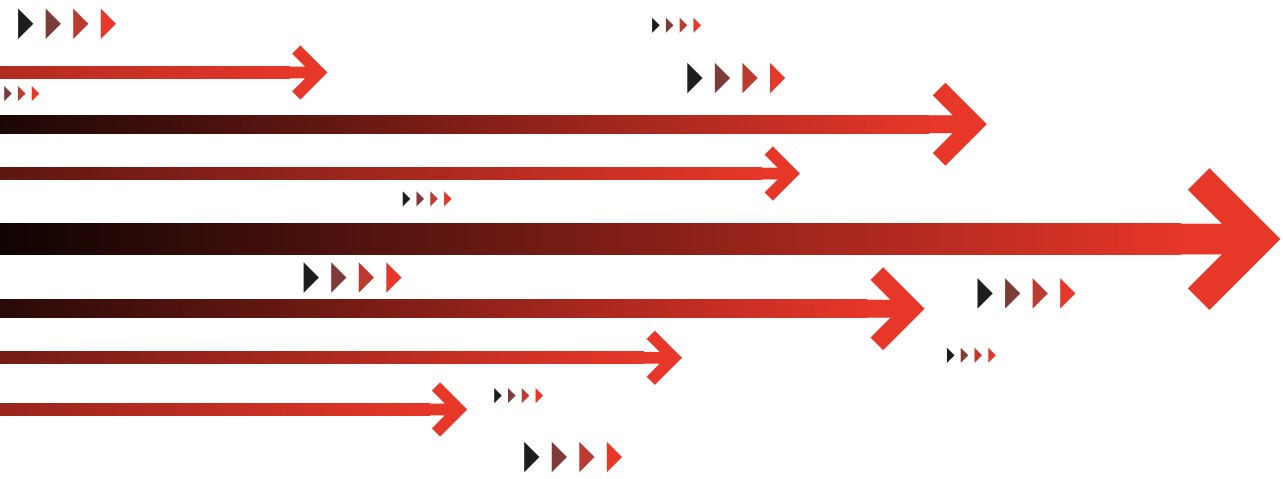
And not just your average hacker living in a basement either — nation-states have a vested interest in sponsoring sophisticated and targeted cyberattacks against both public and private organizations within countries that they view as rivals or adversaries. Whether the intention is to steal confidential information or to destabilize a government, the attacks are difficult to defend against and often seem to fly under the radar.

87% of respondents agree that nation-state-sponsored cyberattacks are far more common than most people think

This is demonstrated by the fact that 87% of surveyed cybersecurity experts agree that nation-state-sponsored cyberattacks are far more common than most people think, which is an increase from 81% who agreed with this in 2019.

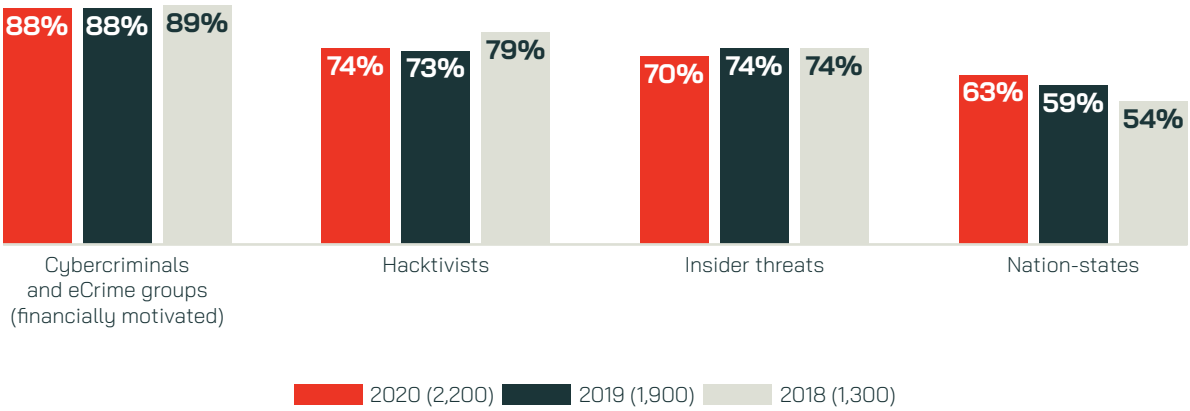
Clearly, most of the time nation-states will have very good reasons for wanting their cyberattacks to go undetected — any exposure could easily lead to a backlash from the international community. But the increased proportion of respondents reporting that state-sponsored attacks are far more common than people think does indicate that these covert attackers are becoming more prolific and perhaps aren't concealing their actions quite as well as they think.

Furthermore, it would appear that these attacks are set to become even more prevalent, with almost three-quarters (73%) of respondents believing that nation-state-sponsored cyberattacks will pose the single biggest threat to organizations like theirs in 2021. This is even considering the proliferation of ransomware already discussed.



81% of respondents believe that their organization cannot rule out being the target of a nation-state-sponsored cyberattack by any government, including their own

Which types of cyberattackers are the biggest concern?
2020, 2019 & 2018

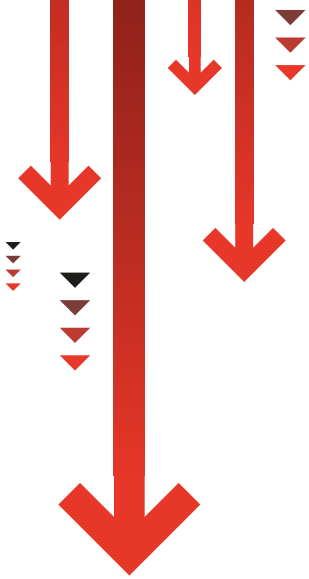


Reinforcing this point is the steady increase in levels of concern around nation-state attacks over the last three years, with approaching two-thirds (63%) admitting that their organization is concerned this year, compared to 59% in 2019 and 54% in 2018. This could also be a symptom of the fact that many global elections have taken place in 2020, with some still to go — recent election interferences are fresh in the memory of everyone who has access to the news, and as a result, the fears around this type of attack have naturally begun to resurface.

When it comes to which nations are most likely to carry out an attack, approaching six in ten (58%) respondents are more concerned about China perpetrating a devastating nation-state attack against their organization, compared to 37% who are more concerned about Russia. Perhaps unsurprisingly, respondents from the EMEA region are the most likely (45%) to be fearful of Russia, but even there, 49% are worried about China.

And with concerns already mounting around the threat that nation-states pose, further global unrest will not help the situation. Almost nine in ten (89%) respondents believe that growing international tensions, such as the U.S.-China trade war, are likely to result in a considerable increase in cyber threats for organizations. With businesses already having a raft of threats that they must deal with, the last thing they need is for political tensions to boil over and spark a peak in cyber warfare. Coupled with the fact that 81% of respondents believe that their organization cannot rule out being the target of a nation-state-sponsored cyberattack by any government, including their own, cybersecurity professionals have a real problem on their hands.

But what are the key motivating factors for nation-states to carry out a cyberattack?



As with any type of cyberattack, key motivating factors of nation-state attacks are centered around access to valuable customer data (51%) and financial/intellectual property gain (50%). However, with the added complications presented by the COVID-19 pandemic, it is not all that surprising to see approaching half (47%) of respondents citing that the exploitation of vulnerabilities caused by the crisis is a key driver of malicious nation-state activity.

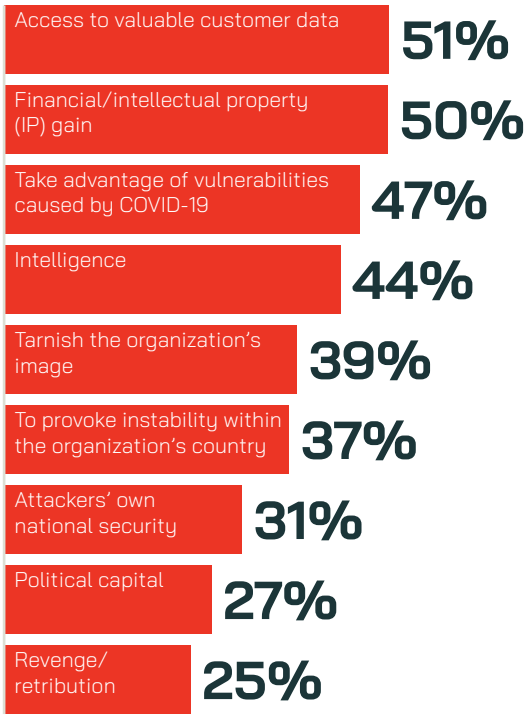
On average, respondents reported four separate possible motivations, and even though some are slightly less common, they are still potentially very dangerous for the organizations and countries that are targeted. These include intelligence gathering (44%), to provoke instability within the organization's country (37%), and political capital (27%). For all of these factors, respondents from the biotechnology and pharmaceuticals sector are the most likely of any industry to report them (52%, 44% and 36%, respectively), highlighting the value of the products and services that these organizations offer, but also showing how important their ties to the government often are.

And with the potential benefits for the aggressors when carrying out targeted attacks, it is clear to see why 83% of respondents agree that nation-states are now more motivated than ever to pursue attacks against organizations.

The world has been in turmoil during 2020, providing the ideal breeding ground for all forms of crime, including cyber. Nation-state activity can thrive when the rest of the world has its back turned, and as such, concerns are on the rise about this type of cyberattack.

This factor further highlights why organizations simply must transform their security infrastructure to ensure that they are doing everything within their power to protect their critical assets and data.

Motivations for nation-states to attempt cyberattacks



Guarding against malicious actors with almost unlimited resources will often feel like an unwinnable fight — a David vs. Goliath-type battle — but we all know what happened there, and that is why organizations have a fighting chance if they take the appropriate course of action.

After all, the stability of the country in which they are based might depend on their winning that battle.

The Need for Both Digital Transformation and Security Transformation

In order to make progress, change must happen — and even though this is an almost universally accepted mantra, significant change still often requires a catalyst before the wheels are set in motion.

This most unusual of years has been an obvious catalyst for digital transformation, although given the increasing threat posed by ransomware and nation-state activity, security transformation is also a rapidly increasing need. These two changes simply must go hand-in-hand, or organizations could leave themselves hopelessly exposed, compromising everything that they have worked toward.

Digital transformation clearly hasn't just surfaced in 2020 — it's been on the to-do list of organizations around the globe for many years. This is best portrayed by the percentage of respondents (61%) who reported that their organization has spent at least $1 million (USD) on digital transformation over the past three years, with the average spend being $4.86 million (USD).

While digital transformation is a marathon not a sprint, COVID-19 has provided a need for the pace of change to increase. Organizations have reacted to this need, with 84% of respondents indicating that their company has accelerated digital transformation to some extent — this includes 51% that have accelerated by at least six months.

From a financial standpoint, this acceleration translates into an average additional spend of $1.05 million (USD) by organizations in order to adapt to the challenges posed by the pandemic, with 90% of respondents reporting that their business has spent $100,000 (USD) or more. And it is respondents from organizations in the US who report the highest average additional spend of any region or individual country, at $1.47 million (USD), showing the size of the task at hand for these businesses as they try to react to the pandemic.

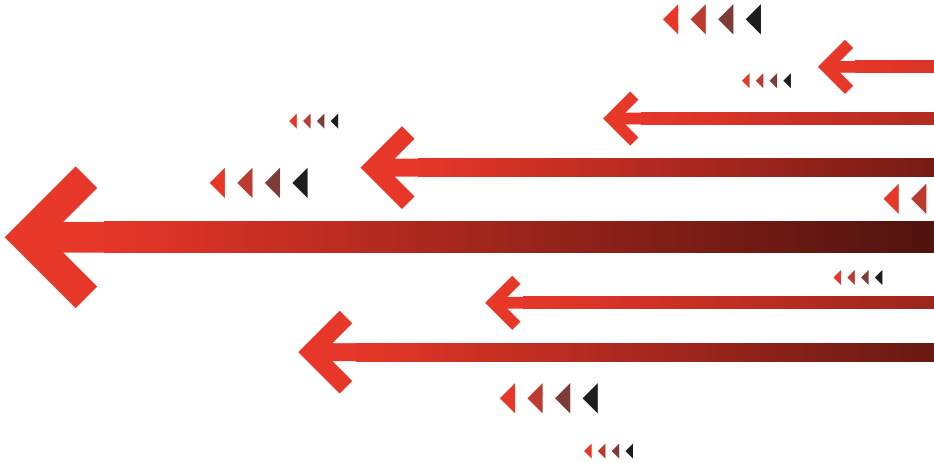
In light of the proliferation of ransomware and given the average ransom paid, this means one successful attack over the past 12 months could easily have wiped out the funds that organizations have needed in their response to the pandemic. If this point doesn't highlight the urgent need for security transformation as well as digital transformation, then nothing will.

$1.05m **Average additional spend on accelerating digital transformation to adapt to the challenges posed by COVID-19**

$1.47m **Respondents from organizations in the US report the highest average additional spend vs. $0.92m in EMEA, $0.98m in APAC**

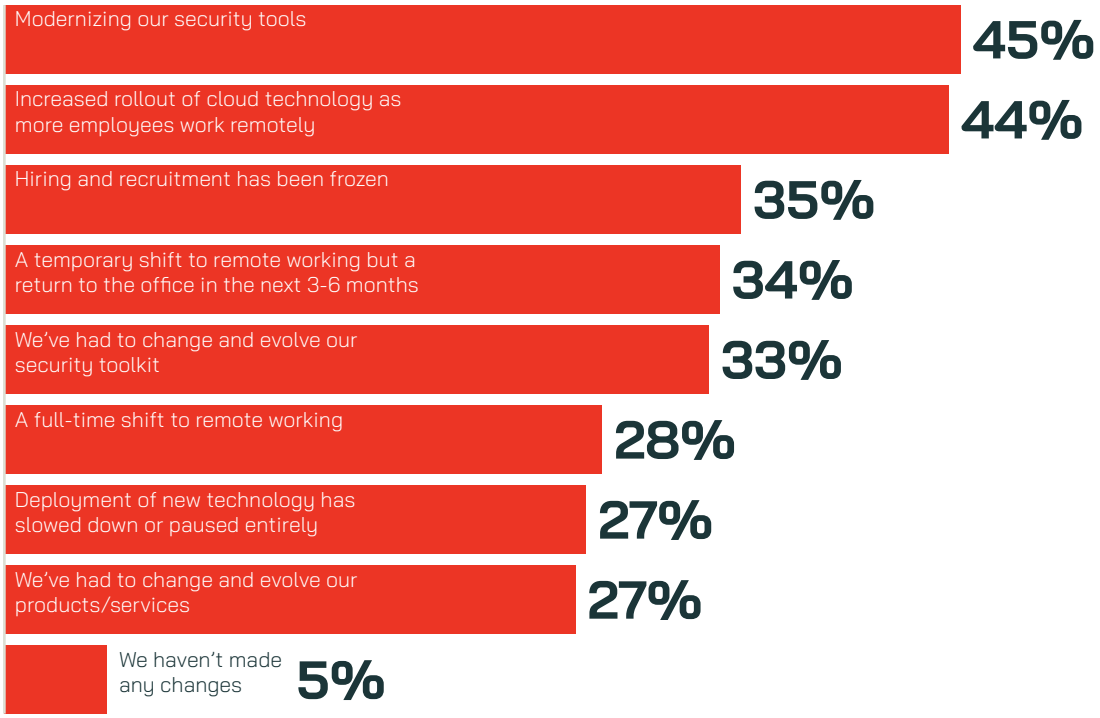
90% **of respondents say that their organization has spent $100,000 or more on digital transformation acceleration**

One in three (32%) report that legacy security tools, such as firewalls and antivirus, let their organization down when adapting to the COVID-19 pandemic



It appears as though organizations have understood the intrinsic links between digital and security transformation. Approaching half (45%) of respondents identify that their organization has been modernizing its security tools in response to the pandemic, while a similar proportion (44%) report that their organization has increased the rollout of cloud technology in order to better support a remote workforce. Overall, 95% of respondents' organizations have had to make at least one change in response to the challenges posed by COVID-19. But it's very telling that security tools and cloud technology have been fundamental to their response, as these are the two adaptations that can guarantee the agility and resilience so desperately required at a time like the present.

Changes undertaken to meet the challenge of COVID-19



In addition, by modernizing their security tools, many organizations are plugging a gap in their infrastructure that has needed addressing for a substantial amount of time. This is demonstrated by the proportion of respondents (32%) who report that legacy security tools, such as firewalls and antivirus, let their organization down when adapting to the COVID-19 pandemic. This is a perfect example of how change has been needed for a long time, but despite this need, a catalyst has still been required to make it a reality.

Where spending has accelerated as a result of COVID-19

76% Security tools

73% Cloud technology

66% IT operations/ user support

62% IT hardware

60% Technology skills training

52% Software development

Further highlighting the idea that organizations have realized the urgent need to transform their security posture, 76% of respondents say that spending on security tools has accelerated as a result of the pandemic. Almost the same proportion (73%) highlight this acceleration when it comes to cloud technology, making these two areas the most likely to have seen such concerted acceleration efforts.

The most modern and advanced security tools should not be viewed as a "nice to have" accessory by organizations. They are an absolute necessity to combat the most dangerous and targeted cyberattacks that can have devastating consequences if successful, so spending acceleration is vital moving forward.

The need for security transformation is further underscored by the fact that many countries are not out of the woods yet in relation to the pandemic. Yes, the world has begun to settle into its new way of living and working, but the real economic impacts of the crisis are yet to be fully understood. However, it seems reasonable to assume that the global economy should brace itself for a lengthy period of economic recession.

Suffice to say, this forecast signals more bad news for organizations, but according to respondents, their concern is not limited to the obvious financial implications, with 74% agreeing that economic recession leads to increased cybercriminal activity leveraged against their organization. Given that 60% of those surveyed admit that it has already become harder to prevent a cyberattacker from reaching their objective since the pandemic began, economic uncertainty is a real cause for concern among cybersecurity professionals and their employers.

79% believe that the COVID-19 pandemic has had a positive impact on their organization's outlook regarding its overarching security strategy and architecture

Despite the gloomy forecast over the coming months and years, respondents appear to be trying to maintain a positive mindset — 79% believe that the COVID-19 pandemic has had a positive impact on their organization's outlook regarding its overarching security strategy and architecture for the next 12 months.

Clearly there has been a mindset shift within surveyed organizations, where they now have more clarity on, not only the urgency of their current situation, but also the longer-term positive impact that making the right changes can have for their cybersecurity further down the road.

This is a moment in time that will define the direction of companies around the world – there are many factors at play, but if the security of their data, intellectual property, and remote workforce are not top of mind for organizations, then realistically it is only a matter of time before they become a victim of their own negligence.

The only viable option is end-to-end security transformation. Anything less than that would be tantamount to self-sabotage.

The Changing Cybersecurity Landscape: Have Organizations Gotten Better at Response?

Unquestionably, the global landscape in which we live and work changed forever during 2020, and the cybersecurity landscape is no exception.

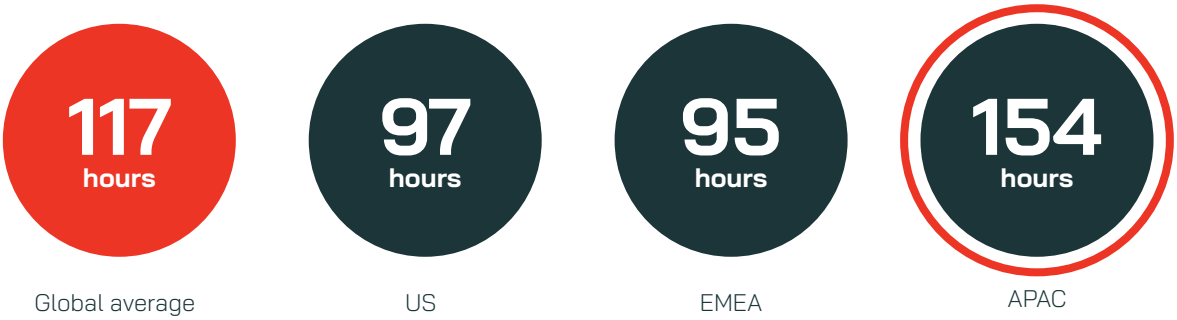
But amid all of the chaos, cybersecurity professionals have a very important job to do — a job that if not done properly will expose their organization to untold levels of risk that could leave them with irreparable damage.

Given the range of threats now being targeted at organizations, it is unrealistic to expect IT security teams to prevent every single one of these from gaining access to their network. This means that the key to defending the most valuable assets of the business lies in their response to an intrusion.

The 1-10-60 paradigm is something that all organizations should be working toward if they hope to mitigate the risks of an intruder accessing their systems. The goal is to take one minute to detect an incursion, 10 minutes to investigate, and 60 minutes to contain and remediate.

Unfortunately, most organizations are missing this benchmark by a significant amount, often falling at the first hurdle. Nine in ten (90%) respondents admit that it takes their organization longer than a minute to detect a cybersecurity incursion — in fact, the average estimated detection time is a lengthy 117 hours (almost five days), which if not handled correctly could put organizations in direct breach of regulations, such as GDPR and other regional breach notification regulations. Further, this average reflects very little improvement over the 120-hour estimate in 2019. The average estimated detection time in the APAC region is particularly concerning at 154 hours, with respondents' organizations from India contributing to this higher number, with an average time of 228 hours.

Average estimated detection time of cybersecurity incursions
By region

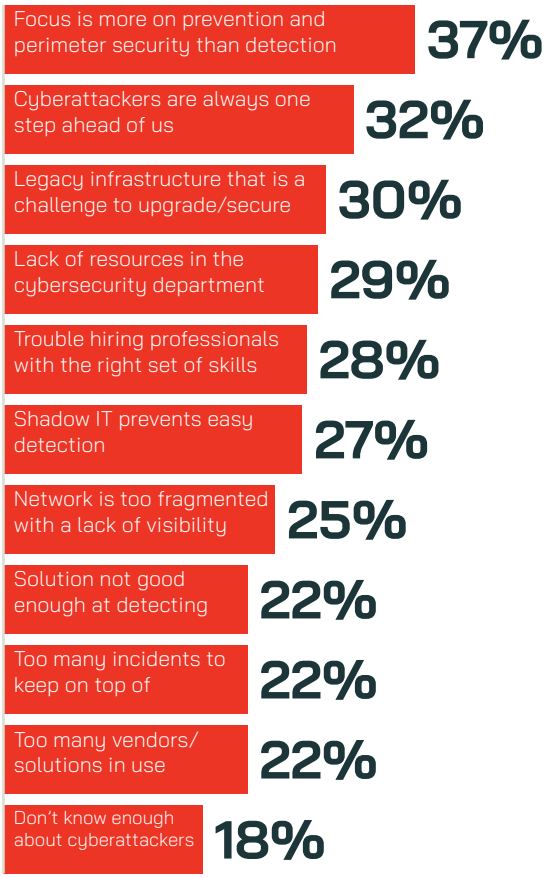


Just over half (52%) of respondents believe that the COVID-19 pandemic has slowed the speed with which their organization can detect a cybersecurity incident

The alarming lack of progress over the past year clearly demonstrates the challenge that organizations are facing and will likely continue to face in the aftermath of the pandemic. Just over half (52%) of respondents believe that the COVID-19 pandemic has slowed the speed with which their organization can detect a cybersecurity incident. For almost one in ten (8%), this detection time could be slowed by a week or more.

This lack of speed is not something that organizations can allow to continue — they need to address the question of why improvement is taking so long.

Barriers to detecting cybersecurity incursions/incidents faster



The reasons for why organizations are struggling so much to detect cybersecurity incidents are multi-faceted, ranging from difficulties with knowing enough about cyberattackers (18%) and defending against attackers that are always one step ahead (32%), to well-known difficulties in hiring professionals with the right skills (28%) and dealing with a lack of resources (29%).

One reason stands out from the rest: 37% of respondents report that their organization focuses more on prevention and perimeter security than on detection. This approach to cybersecurity seems to have become increasingly futile given the level of sophistication that cybercriminals are now demonstrating in their attacks.

This is not to say that organizations should get rid of their prevention and perimeter security measures altogether — far from it — but in all likelihood, cyberattackers will be able to access their network regardless of the effectiveness of the barrier these companies put up. Therefore, they must shift their focus to detection and prioritize the 1-10-60 approach if they hope to effectively protect their most valuable assets.

Fast detection becomes even more important considering that 55% of respondents believe that the COVID-19 pandemic will lead to their organization encountering increased cybersecurity risk, while 58% point toward an increased risk of cyberattacks for their industry.

Almost three-quarters (73%) of those surveyed believe that COVID-19 has proven to be a catalyst for long-awaited approvals on security upgrades

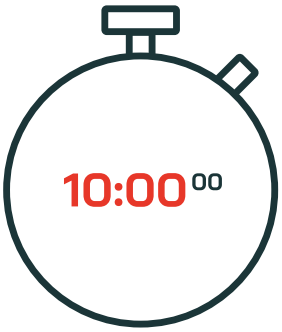
Speed of detection is of paramount importance for organizations across all sectors moving forward because focusing on trying to close the gates entirely will inevitably leave gaps that cannot be covered, and this scenario is when cyberattackers are at their most dangerous — left unhindered to work toward their objectives.

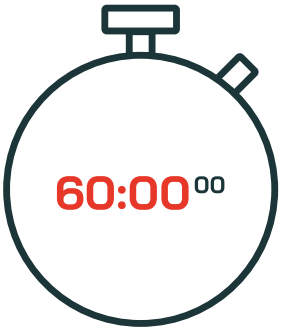
It appears that organizations have realized the precarious nature of their situation and understand that any hesitation in their decision-making could prove disastrous. Almost three-quarters (73%) of those surveyed believe that COVID-19 has proven to be a catalyst for long-awaited approvals on security upgrades.

It shouldn't take a global pandemic for organizations to take action, but understanding the urgent importance of transforming their security is a move in the right direction.

While familiar problems continue to be a challenge for organizations, the cybersecurity landscape has changed in the past year and will continue to evolve in the years to come. Cybersecurity professionals and their organizations must do everything that they can to get ahead of this and put their security transformation strategies into action.

The most important first step is moving significantly closer to the 1-10-60 ideal. Without this goal, protecting their crown jewels becomes almost impossible and the consequences that follow are unthinkable.





CrowdStrike perspective:

With 2020 truly the year of hyper-accelerated digital transformation, it's not unusual to see organizations delivering many years' worth of migrations and implementations over a much shorter period. There has been a noticeable surge in organizations replacing their legacy, on-premises technologies with cloud-native platforms that were built with hybrid working environments in mind. But as many enterprises remain mid-transition, your security teams may still feel out of control now that the work-from-anywhere approach is encouraged and embraced by many employers and expected by most employees.

CrowdStrike Falcon® addresses these security challenges because the remedy was purpose-built into the platform from the very beginning. The CrowdStrike® Falcon platform is cloud-native, and the lightweight Falcon agent does not require reboot, unlike most CrowdStrike competitors, so customers can easily and remotely deploy, manage and protect workloads at scale.

Many of the security risks and operational concerns related to digital transformation are rooted in traditional approaches to security — frameworks implemented decades ago that revolve around network access control. Despite evidence showing that traditional methods did very little to prevent security breaches, these network architectures remained pervasive and even "best practice" until the well-documented shift in work culture this year.

Traditional security models built around network perimeters are all but dead, pointing to the impending demise of an enterprise's server room with racks full of expensive firewalls, switches and security hardware. When you can no longer trust network security, you are left with two controls — the workloads themselves (whether they are applications, services or endpoint devices) and the identities and credentials. Eighty percent of breaches are a direct result of compromised identities or credentials, meaning that a shift from perimeter- and network-based security to identity-centric security can prevent or nullify the impact of the majority of successful attacks.

When identity protection is combined and integrated with the run-time protection of workloads, endpoints and mobile devices, it's possible to alleviate the strain on IT teams and remain secure while planning, implementing and migrating to the cloud-native applications that will keep your business running and secure wherever your employees are.

Conclusion

Cybercrime is not a new phenomenon — it has been causing headaches for cybersecurity professionals all too frequently for years.

New threats are popping up all the time, and existing threats are evolving and becoming more prolific, making it an almost impossible task for organizations and their security teams to keep up.

And the COVID-19 crisis has added complexity to an already problematic situation for cybersecurity professionals.

With the threat of ransomware and with nation-state actors more motivated than ever to cause disruption and upheaval, organizations must act fast if they hope to effectively protect their critical assets from those with criminal intentions.

Digital transformation has been the cornerstone of successful businesses for many years, and it must now go hand-in-hand with security transformation. Without an updated focus on security, organizations will leave themselves horribly exposed to the raft of security threats that could do them damage.

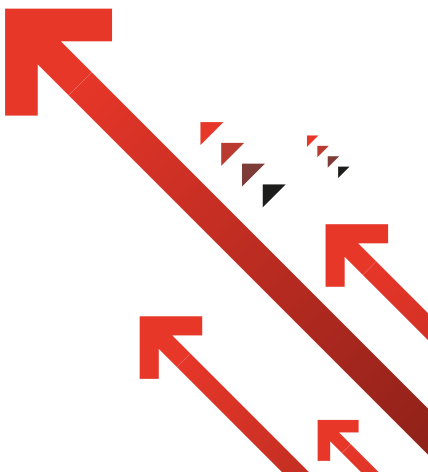
Many organizations have realized the nature of the challenge that they face and have responded to the COVID-19 pandemic by beginning to put long overdue changes into action. But the vast majority cannot currently get close to the 1-10-60 industry ideal for threat detection and remediation.

The 1-10-60 benchmark must be top of the agenda for security decision makers aiming to effectively prevent attackers from reaching their objectives. Trying to prevent all potential attackers from gaining access to your network is not the right goal to focus on.

Transforming your security strategy and architecture to focus on detection and containment is your best strategy. The threats will keep coming, but how you deal with them must change if you are going to keep your organization safe.

Falling victim to any form of cyberattack fills cybersecurity professionals with an unimaginable sense of dread, but this fear drives them to be better. With a new awareness of how security must transform in the wake of the COVID-19 pandemic, your organization can avoid becoming the next high-profile ransomware or nation-state attack victim.

The only question now is, why wait any longer?



Methodology

2,200
senior IT leaders and security professionals

3
regions: US, EMEA and APAC

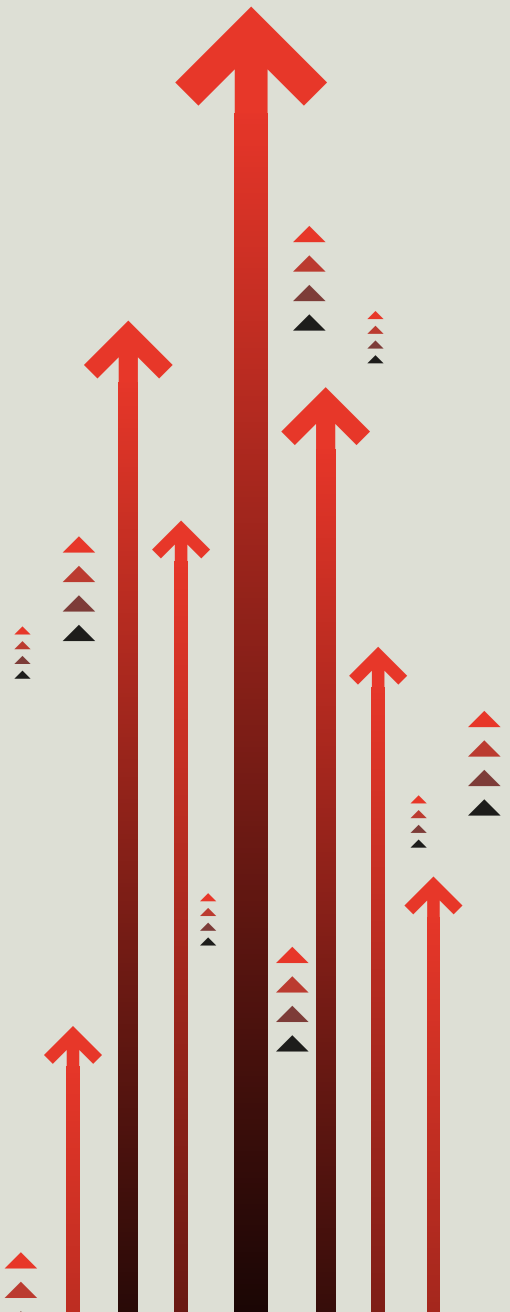
250+
employee organizations

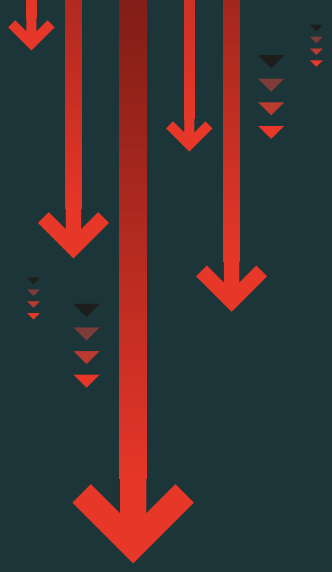
CrowdStrike commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this whitepaper is based. A total of 2,200 senior IT decision makers and IT security professionals were interviewed during August and September 2020, with representation across the US, EMEA and APAC regions.

All respondents had to be from organizations with 250 or more employees and are from a range of private and public sectors.

Online and telephone interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated the results discussed are based on the total sample.

Country	Number of interviews
US	400
UK	200
France	200
Germany	200
Spain	100
Italy	100
Netherlands	100
Middle East	100
India	300
Japan	200
Singapore	100
Australia	200





CROWDSTRIKE

CrowdStrike Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates 4 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Qualifying organizations can gain full access to Falcon Prevent™ by starting a free trial.

Learn more: https://www.crowdstrike.com

Follow us: Blog | Twitter

VansonBourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit www.vansonbourne.com