Fieldwork by Citrix

The State of Security in a Hybrid Work Environment

Foreword

The years 2020 and 2021 have seen a significant rise in cyberattacks and incidents, with many directly exploiting the work from home situation. As the workforce has become so distributed, legacy security architectures have proven themselves inadequate in this expanded set of use cases. Businesses globally are finding themselves increasingly exposed, placing security teams under immense pressure; but as this study reveals, many of these teams have risen to the challenge phenomenally well. If we can cite one silver lining of the mass work from home event, it has been the renewed priority and focus organizations have placed on cybersecurity. Security is now a vital, shared responsibility that spans from individuals to IT, supply chains and the c-suite.

Ultimately, the pandemic has served as a catalyst for change for cybersecurity teams across the world, and our study goes some way towards proving that in 2021, the cybersecurity lifecycle has become a truly collaborative affair, extending into almost every aspect of the business. We have much to be thankful for to the security leaders who have steered us safely through heightened risks during the pandemic, often accelerating transformation plans from several years to realizing demonstrable benefits in months.
Of course, our work in cybersecurity is never done – and we need to be prepared for the next set of challenges.

Fieldwork by Citrix

About the study

The State of Security in a Hybrid Work Environment examines attitudes and experiences from security decision makers and knowledge workers in medium-large organizations (500+ employees in the US; 250+ employees in all other markets) as the knowledge economy transitions to a long-term hybrid work strategy. Citrix, in partnership with Sapio Research, ran an independent opinion research study, interviewing 1,250 security decision makers (job titles included Manager, Senior Manager, Director and Vice President), working in large and mid-market businesses. Respondents were based in the US (413 respondents), the UK (203), France (218), Germany (209), and the Netherlands (207). In addition, the study also polled 3,603 knowledge workers based in medium-large organizations in the US, UK, France, Germany and the Netherlands.

The interviews were carried out online by Sapio Research in September 2021 via an email invitation to an online survey. A series of qualitative CISO interviews were also conducted to support the research, although the identities of participants have been anonymized.

Fieldwork by Citrix

Executive summary

The pandemic has proven itself to be a catalyst for change and investment

- When the pandemic broke, 26% of security decision makers were “very prepared” for a remote or homeworking scenario, while 46% were “somewhat prepared”. A minority group of 16% admit they were not prepared for the event.
- 79% of security decision makers say the event created an opportunity to completely rethink their long-term information security strategy.
- 71% of security decision makers believe their IT environment is more secure now, than it was prior to the pandemic.
- Over the past 12 months, investment in security has increased for 58% of security decision makers, on average, by 40%.

The threat level has increased with widespread remote work

- 74% of security decision makers claim information security procedures, systems and controls have become more complex due to widespread home working.
- 73% of survey respondents agree that over the past 12 months, the volume of security events and data to process has increased significantly.
- 73% of respondents believe information security teams must tolerate a higher level of acceptable risk in a hybrid, work-from-anywhere environment.

Hybrid work is here to stay

- 52% of security decision makers believe in the future, most of their workforce will be permanently remote or hybrid.
- Knowledge workers are slightly more optimistic about a hybrid future and 59% expect most of the workforce will soon be permanently remote or hybrid.
- Two thirds of knowledge workers say it is very important to them to be able to work remotely or from home, on any device, in the future.

CISOs are enjoying a rise in status within their organizations

- 78% of security decision makers say that information security has become more of a business enabler.
- 72% of security decision makers believe CISOs are officially becoming part of the c-suite, spending more time in the boardroom.
- 81% agree information security teams are becoming more integrated into business operations.

Security is now a shared responsibility

- 76% of security decision makers agree information security is becoming more consultative in nature, driven by the increased understanding that security threats are a threat to the business, rather than just a threat to technology.
- 90% of knowledge workers agree that security is a shared responsibility, and 85% of security decision makers share this view.
- 73% of security decision makers believe their workforce is highly aware of potential security risks, and 64% of knowledge workers claim to have this awareness.

Modernizing IT is vital to improving the employee experience

- 86% of security decision makers rate providing a seamless employee experience remotely as very important, and 94% regularly ask how they can improve.
- 92% of security decision makers say they are actively measuring security's impact on the employee experience.
- 91% of knowledge workers say new security protocols have enhanced or have had no impact on their employee experience, and 90% say they have had no impact on productivity.

Experiences of managing security during the pandemic

To gain some perspective on the current state of security, we asked security decision makers about their experiences during the early stages of the pandemic, particularly now that the dust has settled.

Fundamentally, the outbreak of COVID-19 took everyone by surprise. Despite robust business continuity plans, such global disruption was entirely unprecedented. One of the the Chief Information Security Officers (CISOs) interviewed offers the analogy that the initial pandemic response "was like changing an engine on a plane while it was in flight."

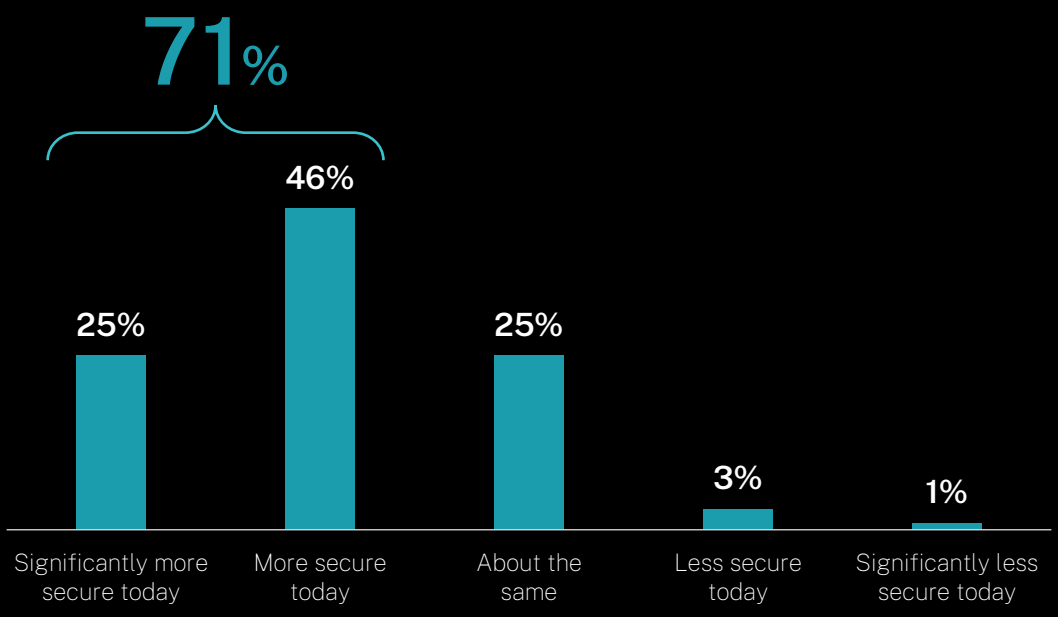
IT security became an indispensable part of the rescue mission, enabling organizations and their workforces to work from home effectively. Very few security teams were ready to cope with such an event, and our survey data reveals that only a quarter (26%) of security decision makers were "very prepared" for a remote or homeworking scenario, while 46% were "somewhat prepared". Germany was the country least caught off guard, with 29% of the security decision makers polled claiming to be "very prepared" for such an event, compared to The Netherlands, where just 18% of respondents were "very prepared".

Security plans have been accelerated

For many, the pandemic was a much-needed wake-up call, serving as a catalyst for change for security teams, globally. Our survey finds that 79% of security decision makers say the event created an opportunity to completely rethink their long-term information security strategy, beyond COVID-19. Security roadmaps were expedited, from years to months. “It was no longer a matter of growth; it was a matter of survival,” says one of the CISOs interviewed, who agrees business’ hands were forced into digital transformation and IT modernization. “It is spawning a lot of transformations that were previously thought to be five to 10 years away.”

As a direct result, the technology response has been swift, and 71% of security decision makers believe their IT environment is more secure now, than it was prior to the outbreak of COVID-19. This is critical because the reputational, operational, legal and compliance implications of ignoring IT security are incredibly high at present, amidst ongoing economic uncertainty. However, security leaders must remain mindful of the fact that the cyber threat level is increasing, and a more secure environment does not necessarily mean the business is more secure, overall.

Most feel more secure today than before the pandemic



Q: Overall, how secure is your company’s IT environment currently compared to before COVID-19? Select one.

Base security decision makers: 1250

Investment in security has become a business priority

Over the past 12 months, 58% of security decision makers have increased their investment in security, by an average of 40%; while security budgets have remained the same for 31%.

"COVID has accelerated everyone's roadmaps for security, and it is getting all the funds it needs right now," shares one of the CISOs interviewed, claiming the pandemic has enabled organizations to better understand the vital role that security plays.

Remote working has complicated security

However, the survey finds that the role of managing security has become more complicated, since the outbreak of COVID-19. Three quarters (74%) of security decision makers claim information security procedures, systems and controls have become more complex, due to widespread home working. Respondents also say that remote work has created more "noise" in the system and 73% of survey respondents agree that over the past 12 months, the volume of security events and data to process has increased significantly. This makes the role of IT security much harder, with teams having to oversee the day-to-day of keeping users secure and protecting the organization, while also needing time for innovation and transformation.

Automation technology has helped security teams to process some of that "noise". "We have automated 20% of our playbook for security operations, from end to end and this has helped to sort out what is important," shares one of the CISOs interviewed.

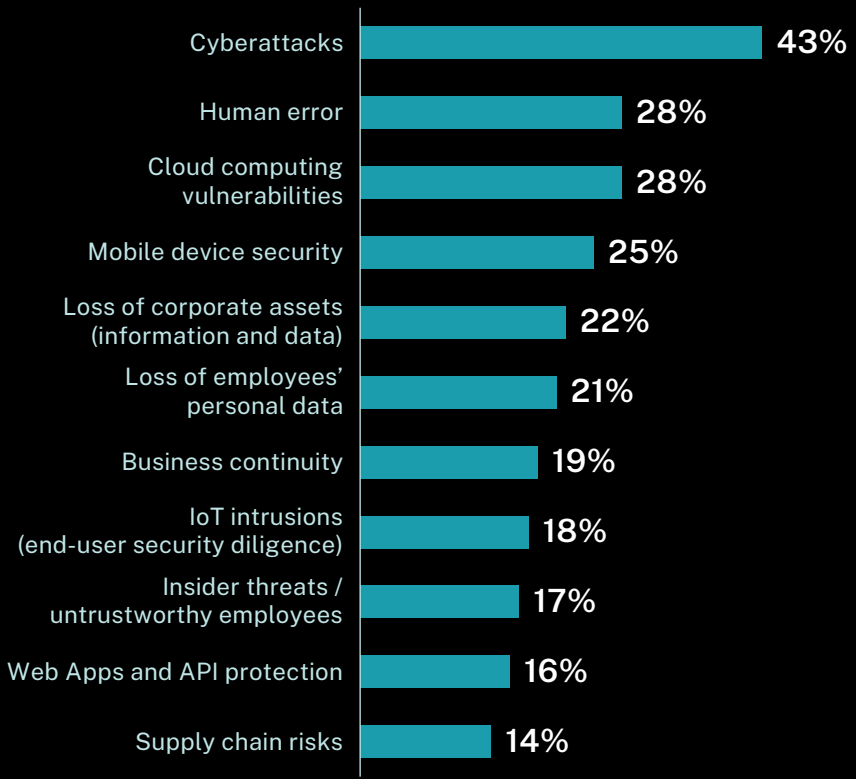
Current threats

COVID-19 has had a significant impact on the threat landscape for businesses. Not only have the volume of attacks increased, but also, as an INTERPOL assessment has shown, there has been a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure[1]. With organizations and businesses rapidly deploying infrastructure to support staff working from home, that shifts the security landscape and criminals have been exploring potential new vulnerabilities to steal data, generate profits and cause disruption.

Within our survey, 73% of respondents believe information security teams must tolerate a higher level of acceptable risk in a hybrid, work-from-anywhere environment. Security used to be confined within four walls, but today, with the perimeter gone, the attack surface is larger than ever, corporate data and assets are scattered and user endpoints “are the weakest link right now,” admits one CISO. “Today, my crown jewels aren’t in the data center [anymore]. They are in the cloud, they are in SaaS, they are in someone else’s data center,” another of the CISOs interviewed, shares.

Our survey explored the threats that security decision makers are most concerned about when securing a hybrid, remote or from home workforce (see below figure). Ranking most highly are cyberattacks, cited as a concern by 43% of respondents. Human error and cloud vulnerabilities are of equal, secondary concern, for 28% of security decision makers. Human error is the greatest threat in government, being cited as a concern for 40% of respondents in this sector.

Top threats when securing a hybrid, remote or from-home workforce



Q: What are the threats your company is most concerned about when securing a hybrid, remote or from home workforce? Select up to three.

Base security decision makers: 1250

The supply chain risk is not being given enough credence

Interestingly, supply chain attacks are perceived as a low-level threat, being a concern for just 14% of security respondents.

"An organization could be vulnerable to a supply chain attack even when its own defences are quite good and therefore the attackers are trying to explore new potential highways to infiltrate them by moving to their suppliers and making a target out of them," The European Union Agency for Cybersecurity (ENISA) notes in its recently published report.[2]

“Anyone, even if they are paying attention, can easily be duped by [a supply chain attack],” admits one of the CISOs interviewed for this study. He claims, “this is why you can’t rely on your expertise alone: you have to have defense in-depth.”

Despite this, our research finds that only 18% of security respondents have prioritized hiring third party security experts, to better secure their remote or hybrid workforce. Part of the issue is recognizing that a cyber risk is also a business risk, and it should be treated as such. While IT infrastructure is a critical part of security, on its own it is not sufficient; human expertise is also a vital part of the equation.

The future of work and reimagining the office

Prior to the pandemic, remote work was already in play. The pandemic has only accelerated and cemented this trend, and our research confirms what we already knew, that working from anywhere is here to stay. We now face the challenge of revaluating the role the physical office will play moving forward, and security is a critical priority within this.

The data reveals that 52% of security decision makers believe that in the future, most of their workforce will be permanently remote or hybrid. Respondents in the US are more hesitant in this prediction, with 46% anticipating this scenario.

Knowledge workers are slightly more optimistic about a hybrid future and 59% expect most of the workforce will be permanently remote or hybrid, in the future. This sentiment is highest in the UK, where 68% expect this to be the case, while in France, 45% of respondents support this view. Positively, 84% of those expecting remote or hybrid work to continue say their company's information security systems are prepared to secure this workforce for the rest of this year, and longer term.

In many cases, employees are being given choice in whether they want to return to the office, work from home indefinitely, or adopt a hybrid model of work. The prospect of permanent hybrid working raises a multitude of questions and concerns for employees, and it is crucial that the process is managed positively, with a range of options made available. According to our study two thirds of knowledge workers (66%) say it is very important to them to be able to work remotely or from home, on any device, in the future. This sentiment is highest in the UK again, where 70% cite the option of hybrid or remote work being "very important", while in Germany, 60% of share this sentiment.

The CISO interviews, carried out for this report, express much optimism for hybrid work being the future, with the office environment being flipped to become a supportive space, where attendance is no longer the requirement. "Our office in essence is like a coffee shop, you come to our office to get internet and be with your co-workers, and that's it," says one of the CISOs interviewed.

The changing role of the Chief Information Security Officer

CISOs have enjoyed a rapid rise in status over the past 18 months, moving from a technical focus to becoming involved in all aspects of the business, from transformation and operations, through to procurement and supply chain. A standout data point within the study is that 78% of security decision makers say that information security has become more of a business enabler. As one CISO shares: “the CISO is becoming one of the most critical executive leadership roles. I have never spent so much time in front of the board of directors as I have done in the last year, which says a lot about where things are going.”

Our survey indicates that CISOs are being more positively perceived within the business, having earnt their stripes throughout the course of the pandemic. Almost three quarters (72%) of security decision makers believe CISOs are officially becoming part of the c-suite, while 81% agree information security teams are becoming more integrated into business operations, and this view is felt most strongly at the c-suite level (89%).

The expert interviews carried out for the study also confirm that the day-to-day role of the CISO is changing, spending less time reacting to problems, and more time on higher level, strategic thinking. “We went from police officer to FBI. We went from a law enforcement to a more investigative role,” shares one CISO. Ultimately, this means spending less time with technology alone. As one of the CISOs interviewed concludes, “CISOs are realising that they shouldn’t have their hands on things; they should have their eyes on things.”

Security as a shared responsibility

While traditionally, security has been upheld as an IT responsibility, today there is more awareness about the role that everyone must play in keeping their organization safe, and particularly so with remote and hybrid working. A notable finding of the study is that 76% of security decision makers agree information security is becoming more consultative in nature, with this figure rising to 84% in the technology sector.

Within our survey, 90% of knowledge workers agree that security is a shared responsibility, and 85% of security decision makers share this view. Promisingly, 70% of security decision makers says “yes”, their employees already believe security is a shared responsibility. A small proportion of knowledge workers (37%) say they would rather not think about security at all, which shows that overall, most knowledge workers understand the role they must play in helping to keep their organization secure.

“Users have an understanding that they are our front line,” says one of the CISOs interviewed. “Ultimately, they are responsible for making sure they handle data securely, and our customers are entrusting them with that responsibility. That is always how we try to position it. Employees might be more likely to be able to figure out when something is going wrong, than we might be with all our tools.”

A heightened sense of awareness is required in a hybrid work scenario

In a hybrid work scenario, users may be in a more casual environment, such as home or café, but they are still an employee. They are still vulnerable, and possibly more so; meaning, having a heightened sense of awareness is critical as we shift to a hybrid work model. Reassuringly, 73% of security decision makers believe their workforce is highly aware of potential security risks, and 64% of knowledge workers claim to have this awareness.

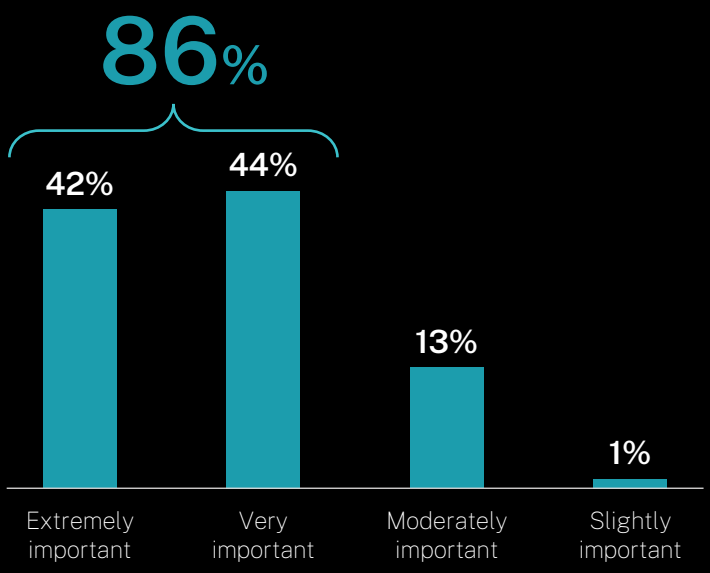
One silver lining of the pandemic situation is that user knowledge of their individual security profiles has improved, and 81% of respondents agree the workforce has become savvier about technology since working remotely or from home.

Modernize IT to improve the employee experience

Employee experience and IT security have historically seemed at odds with one another; however, it is becoming critical that security measures enhance, rather than hinder, the employee experience. Within all decision making, security leaders must be mindful of how employees work, their tools, and processes, and ensure they deliver a seamless experience that empowers employees to do their best work and be productive, without friction. As one CISO interviewed for this report shares, “it is important that users see us as a partner, and not the department to avoid.”

The employee experience is central to global business effectiveness, and thankfully, our data shows that security professionals appreciate this and are taking a people-centric approach. Within the survey, 86% of security decision makers rate providing a seamless employee experience remotely as extremely or very important, and 94% regularly ask how they can improve, with just over a third (37%) asking for feedback monthly. Additionally, 92% of security decision makers say they are actively measuring security’s impact on the employee experience, either formally (39%) or informally (53%).

Security and employee experience can’t be separated



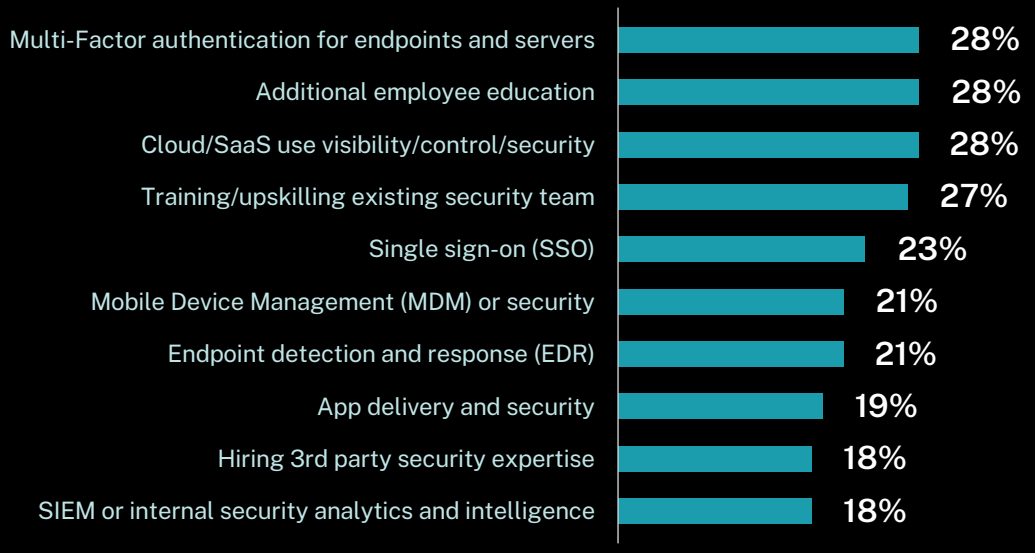
Q: How important is it to your company to create a seamless employee experience when working remote or from home, on any device? Select one.

Base security decision makers: 1250

A rise in new security protocols for staff

Eighteen months into the pandemic, the security landscape is already looking very different for employees. Information security protocols that have been prioritized to support hybrid and remote work include Multi Factor Authentication (MFA) (28%), additional employee education (28%) and Cloud/SaaS for enhanced visibility and control (28%). While these changes have had the potential to disrupt, an important finding of the survey is that 91% of knowledge workers say new security protocols have enhanced or have had no impact on their employee experience, and 90% say they have had no impact on productivity.

Top information security protocols that companies have prioritized to better secure remote and hybrid workforces



Q: What information security protocols has your company prioritized to better secure a hybrid, remote or from home workforce? Select up to five.

Base security decision makers: 1250

Simplicity is a critical part of security

Indeed, it appears CISOs are prioritizing the employee experience within their IT transformation plans, and 78% of security decision makers agree that in the last 12 months, security teams have been exploring ways to simplify security strategies. The proof is in the pudding, and within our survey, only a quarter (27%) of knowledge workers admit to finding their security protocols difficult to understand, and only 30% struggle to remember complex security procedures. This is important since user friction can significantly hamper security efforts. “If you make someone’s life harder, they will find the worst way to do what they are doing. If we are making it easier for our users to get what they need, and they are not having to enter a password, then they are going to be more likely to attribute positive satisfaction to security, which makes us a better partner overall,” explains one CISO.

Zero Trust and Single Sign On (SSO) were the top technologies advocated by the CISOs interviewed for the study, and password-less technologies such as MFA, all with the intention of simplifying the user experience. “The reality is, every time a user needs to think, what is my password, you are creating a human imposed risk. If you can eliminate that, you are not only improving the user experience, but you are vastly improving the security of your systems,” shares one CISO. The survey findings support this view, with 40% of knowledge workers saying a password-less environment is very important to them, while a further 32% say it is moderately important.

Conclusion: A hybrid future

Few security decision makers were prepared for the remote working situation that hit the world stage in March 2020, but the majority have emerged from the situation positively. Not only have they succeeded in securing the much larger attack surface that comes with having a distributed workforce, but they have gone above and beyond what was expected, accelerating security roadmaps from years to months, and seizing the opportunity for change. In many cases, they have managed to create an organization that is more secure than it was prior to the pandemic.

It comes as little surprise that perceptions around security have shifted significantly over the past 18 months: once the department to avoid, a partnership is now forging between security teams and the rest of the organization, and a more collaborative and shared approach to security is emerging.

A people-centric approach to security is ultimately the future, that combines adaptive access with robust network security, so that workforces can readjust to life beyond the pandemic, and a hybrid future of work. IT will play a critical role in delivering this. With the right technology, security teams will be able to provide consistent, secure, and reliable access to the resources employees need to get work done, wherever it needs to get done, and empower them to be and do their best.

Learn more about how Citrix products and solutions can support security and hybrid work, here.

Endnotes

1. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

2 https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks