Trellix Cyber Readiness Research

Path to Cyber Readiness — Preparation, Perception and Partnership

Trellix

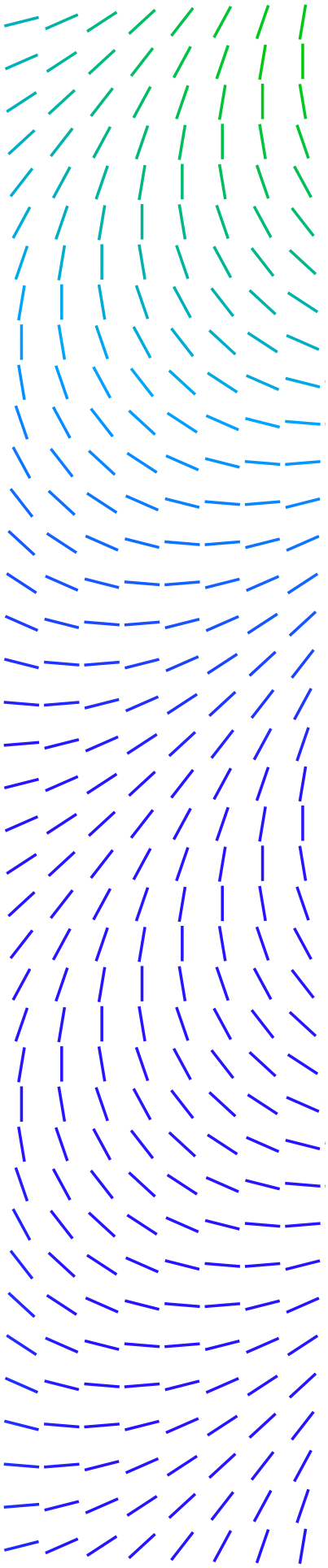


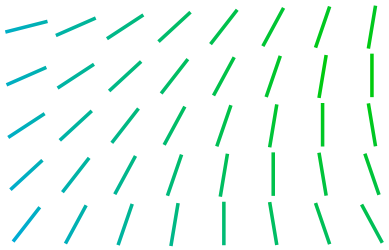
Table of Contents

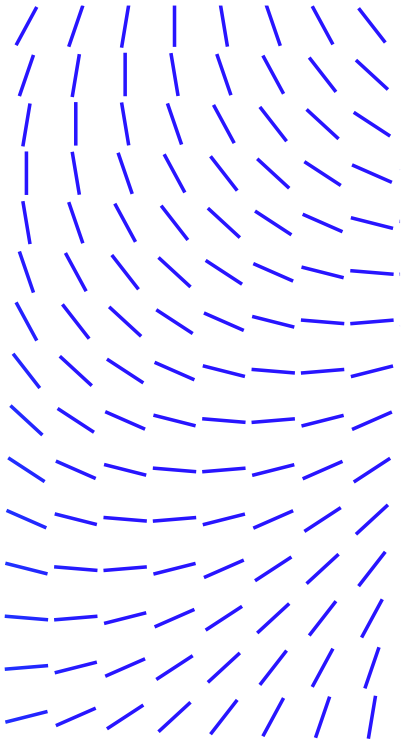
Introduction

In response to the unprecedented software supply chain attacks to SolarWinds and Microsoft in 2020 and 2021, the United States Executive Branch issued a major directive on cybersecurity policy: the Executive Order on Improving the Nation's Cybersecurity (EO 14028). The EO requires US federal agencies to adopt specific strategies and technologies to modernize and harden their infrastructure. In so doing, the agencies are to serve as an example to the private sector. The EO places particular emphasis on capabilities such as endpoint detection and response (EDR), extended detection and response (XDR), multifactor authentication (MFA) and zero trust architecture (ZTA) solutions that can support organizations in everything from endpoint and network protection to cloud modernization to encryption.

While the US led with a policy directive, it was not alone in responding to the SolarWinds and Microsoft attacks. The European Union (EU) published a declaration expressing solidarity with the US on the impact of the malicious cyber-attacks. In addition, the United Kingdom, Canada, Australia and NATO publicly blamed Russia for the SolarWinds attacks. The question remains, however: How do various nations' government agencies and critical infrastructure providers perceive the need for the advanced cyber defenses, standards and practices such as those called for in the US EO, and how do they compare in their progress towards implementing them?

Based on research conducted in the US, UK, France, Germany, India, Australia and Japan, this report explores the progress required to protect these entities from cyber-attacks, the perception of the requirements demanded by the US EO among US organizations, and the general state of relations between national governments and critical infrastructure providers on cybersecurity matters.





Key findings

1. For US government agencies, the recent EO is a likely catalyst towards implementing more modern cybersecurity tools, however, all (100%) respondents from these organizations face barriers in the implementation of these technologies to meet the mandate's requirements.

2. As many as 91% of US critical infrastructure providers and 94% of government agencies and critical infrastructure providers around the world also report challenges in implementing endpoint detection and response, extended detection and response, multifactor authentication and zero trust architecture technologies.

3. On balance, US government agencies are ahead of their private sector critical infrastructure peers in the implementation of these cybersecurity technologies. Just 29% of US critical infrastructure providers have fully developed and implemented ZTA solutions compared to 40% of those in US government agencies.

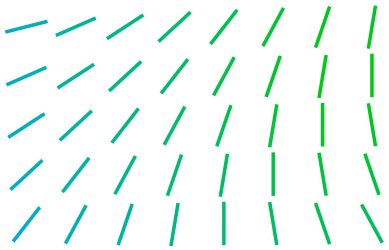
4. EDR and XDR are the most difficult cybersecurity solutions to implement (66%) for US respondents, while MFA is the least difficult (57%).

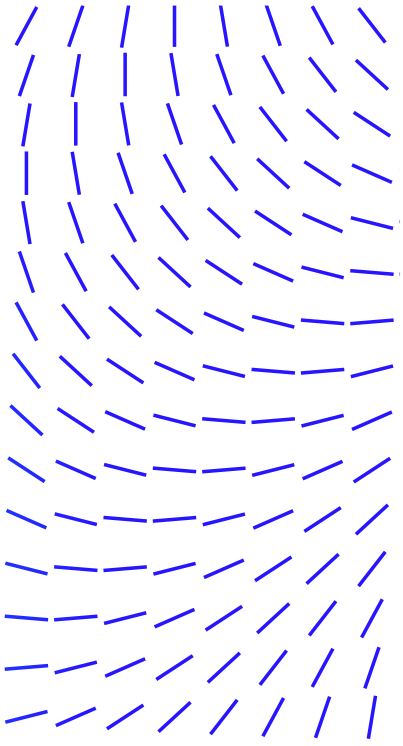
5. As many as 76% of US government agency respondents agree that currently there is no real consistency as to how organizations respond to a cyber incident, prompting calls for the government to introduce more standardized incident response playbooks.

6. In the US, 90% of those in government agencies believe that the EO will result in some level of improvement in changing how well organizations are protected and defended against cyberthreats.

7. For those across the rest of the globe, 89% of those surveyed in APAC and 87% in Europe believe that similar formalized, government-led initiatives will lead to improved protection against cyberthreats.

8. On top of these mandates, there are calls for improved cooperation and coordination between critical infrastructure providers and government agencies, as almost all respondents (99.7%) believe that there are areas where greater support is needed from their country's government.





Section I: Preparation

"Outdated security models and unencrypted data have led to compromises of systems in the public and private sectors."

(White House EO)

To maintain pace with increasingly sophisticated and impactful cyber-attacks, organizations must adopt more modern cybersecurity solutions to protect an ever-growing attack surface. Indicating that preparations are already underway, and have been for some time, most organizations have implemented cybersecurity solutions, but are at different stages across this journey.

Casting the spotlight on solutions that have been developed, implemented, and with full capabilities deployed, this research shows that within the US respondents from government agency organizations are more likely to be ahead compared to critical infrastructure entities, according to respondents. Almost half (47%) of US government agency respondents have fully developed MFA compared to just 37% of those in the critical infrastructure sector. Zero trust architectures are fully deployed by less than a third (29%) of US critical infrastructure organizations represented compared to 40% of those from US government agencies.

One notable area where US agencies lag critical infrastructure providers is cloud cybersecurity modernization, where 41% of these entities' respondents report having implemented these measures compared to only 29% among their government agency peers.

There could be a number of explanations for these differences. It is likely that government agencies in the US have been pushing especially hard to accelerate their efforts in terms of technologies such as MFA and ZTA given the vast quantities of highly sensitive data that they manage as well as the undoubtedly large target on their back from threat actors across the globe. The sensitive nature of government work has been traditionally on premise, and this perhaps explains US agencies' slower adoption of cloud technologies and the security measures to protect them.

Showing IT cybersecurity solutions that are "developed, implemented, with full capabilities deployed'

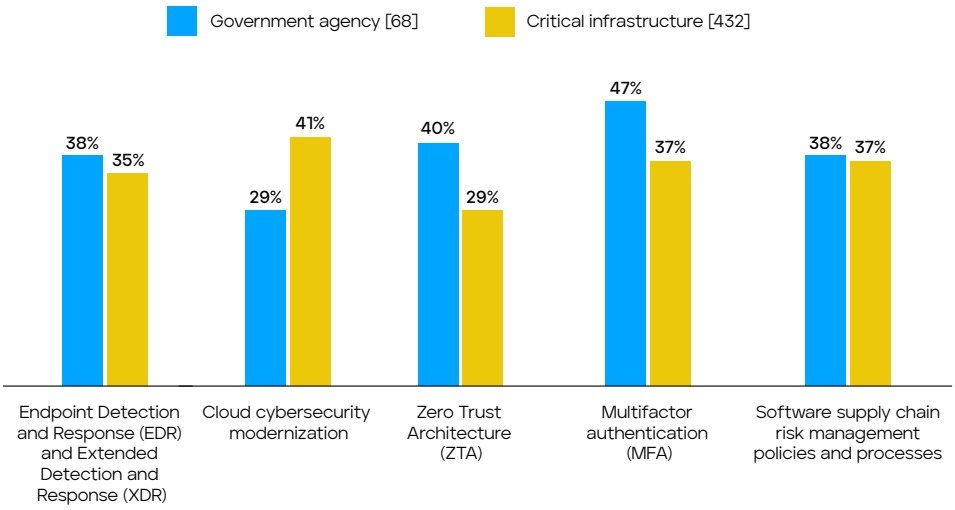


Figure 1: How far along the implementation process is your organization for the following IT cybersecurity solutions? [base numbers in chart] split by respondent type within the US, omitting some answer options

Are some elements of the EO more important or difficult to implement than others?

Further differences between government agency and critical infrastructure sector groups are uncovered when exploring the importance of these cybersecurity elements for both respondents' own industries as well as their national security. For example, cloud cybersecurity modernization is most likely to be the IT solution that is important to individual sectors in the US (82% for those in government agencies; 87% for those in critical infrastructure) while zero trust architectures are least likely to be deemed important (81% for those in government agencies; 78% for those in critical infrastructure). However, this research does show that while there are just 6% who are yet to begin implementing ZTA, almost all have the intention to do so in the future.

The lag in ZTA implementation is evident across both the US government and critical infrastructure sectors and respondents suggest this could simply be attributed to the difficulty of implementing the technology. A notable 81% of US government agencies say that ZTA is highly or extremely difficult to implement, compared to 59% of those from critical infrastructure organizations. Overall, however, EDR and XDR are the most likely to be difficult to implement (66%) among all US respondents, while multifactor authentication is the least likely.

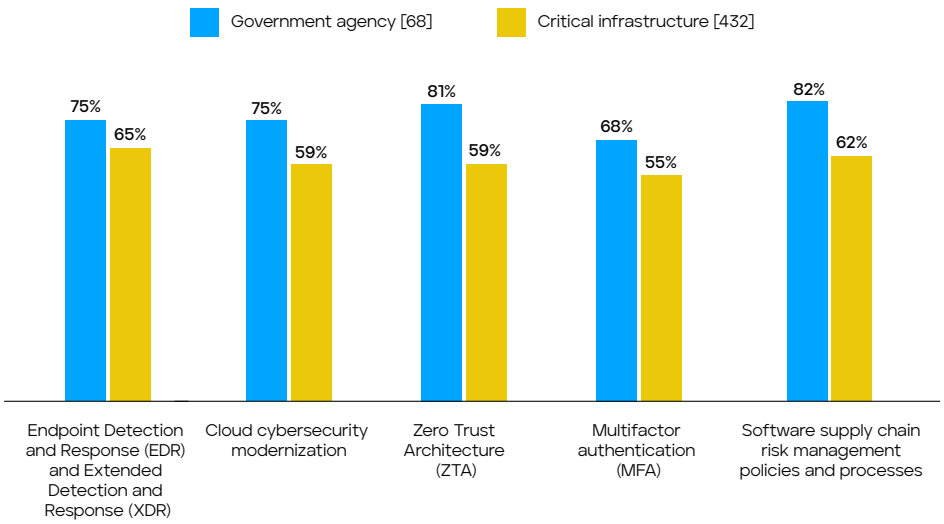


Figure 2: Please rate each of the following elements of cybersecurity enhancement in terms of difficulty for organizations to implement [base numbers in chart] split by respondent type within the US, omitting some answer options. Showing a combination of "extremely difficult" and "high level of difficulty"

Why are some yet to fully adopt new cybersecurity technology?

The majority (93%) of US respondents cite at least one barrier when thinking about this, with those in government agencies more likely to do so (100%) than those from critical infrastructure organizations (91%). The most common challenges in the US are related to a lack of staff resources and skill sets (40%) and a lack of staff implementation expertise (39%). However, when looking at those who selected "lack of leadership recognition for the need to invest" (37%), those from government agencies (46%) were far more likely to cite this as a challenge compared to critical infrastructure organizations (36%), which could be concerning considering that the US EO gives a concrete requirement for such technologies to be put in place within government.

Lack of staff resources, skills and expertise slow US implementation

When considering that the final decision on cybersecurity technology adoption is most likely to lie with the most senior IT role/CIO/CTO within an organization, the importance of leadership recognition for the need to invest becomes even more clear, given these individuals have the final say on purchases and priorities. Similar trends are true when looking at "lack of resource/skillset in-house" (government agency = 49%; critical infrastructure = 38%) and "lack of trusted vendors to work

with" (government agency = 53%; critical infrastructure = 33%), further highlighting the size of the challenge facing government agencies.

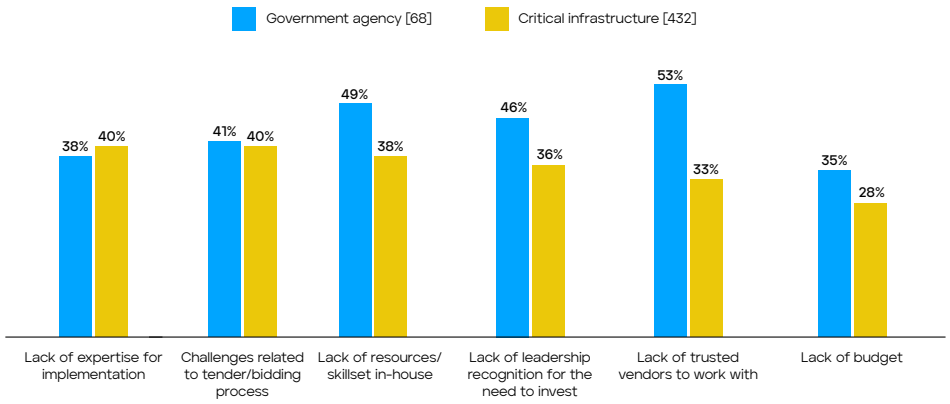


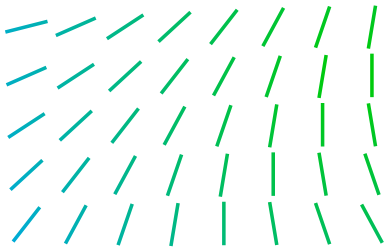
Figure 3: When thinking about the adoption of new cybersecurity technology, what are the biggest barriers that your organization experiences? [base numbers in chart] split by respondent type within the US, omitting some answer options

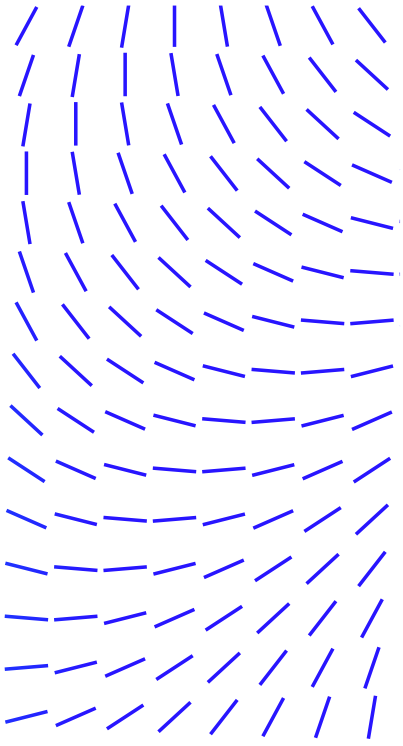
On top of these somewhat more typical and expected challenges, the COVID-19 pandemic has introduced further challenges for organizations who have had to organize working from home arrangements for employees who are now communicating and working beyond the traditional security firewalls. To support remote working, digital transformation has certainly accelerated for most, but it is important that these changes are equally accompanied by security transformation and appropriate personnel to support this shift. In fact, 89% believe that securing remote access to corporate facilities has become more important because of the pandemic. On top of pre-existing challenges surrounding cybersecurity protection, 76% agree that with the migration from totally on-premise computing environments to hybrid, cloud-based environments, network defenders are losing visibility into the actions and operations of organizations. If there was ever a time to enforce an EO to improve the nation's cybersecurity, doing so during a global pandemic is likely to have made this more challenging than anticipated.

76%

of all respondents agree that historically there has been little oversight of how cybersecurity solutions were developed and where

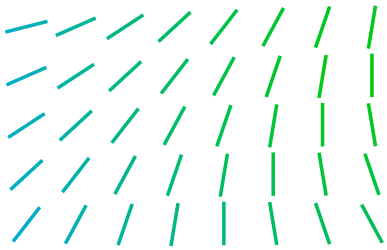
It is therefore clear that there are a number of challenges being faced by organizations when it comes to protecting themselves against cyber-attacks. With calls for IT solutions and products to be adopted to support modernization, it is concerning that three quarters (76%) of all respondents agree that historically there has been little oversight of how cybersecurity solutions were developed and where. It is important that there are improvements in the security

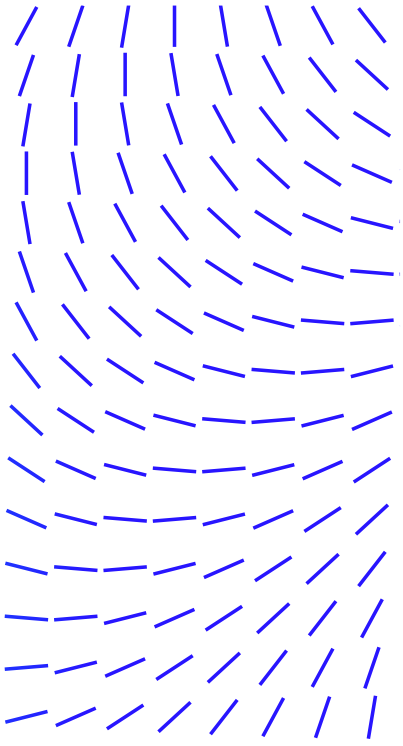




standards outlined for the development of software sold to organizations. In fact, the US EO explicitly states that in response to the SolarWinds attack, the US government administration must ensure that agencies focus on improving the integrity of the software supply chain. Moving forward, the security practices of developers and suppliers of cybersecurity software must be evaluated to make sure these practices are conforming with criteria and guidance being developed. If the government demanded higher standards of cybersecurity, 82% of respondents agree that this would raise standards across the software industry as well.

While the overall message makes it clear that organizations must improve and modernize their end-to-end cybersecurity practices to protect themselves from threatening cyber-attacks, this is unlikely to be completely straightforward. There are several challenges standing in the way of both critical infrastructure organizations and government agencies which will need to be overcome. However, while some are further ahead in their implementation journey than others, organizations are showing clear signs of developing and implementing new IT cybersecurity tools to improve their cybersecurity posture. For those in government agencies in the US, the recent EO may have been the catalyst for this, while for others across the globe, the global pandemic may have accelerated efforts as a result of remote working. Either way, the cybersecurity landscape is set to see a great deal of change.





Section II: Perception

What are the general views on the US EO, and how those in other markets feel about such government mandates?

One of the aims of the US EO is to standardize the guidelines and playbooks for responding to cybersecurity vulnerabilities and incidents among government entities. This is likely to be a welcome goal as 76% of those in US government agencies agree that currently there is no real consistency as to how organizations respond to a cyber incident. This is hardly exclusive to the US, as 83% of those in Australia agree with this too, making it clear that elsewhere across the globe there is room for improvement.

76%

of those in US government agencies agree there is no real consistency as to how organizations respond to a cyber incident

As with any period of change, there must be a leader to set the example of exactly what such change should entail, and many believe this should sit with those mandating these efforts, as 92% of respondents globally agree that it should be government agencies who set the example in cybersecurity for others to follow suit.

However, with government agencies expected to be the ones to lead the change, is it possible that they have set themselves optimistic expectations? The EO sets out deadlines from as little as within 30 days of its release, and so it is unsurprising that 89% of government agencies agree that organizations will face difficulties meeting the expected timelines of the EO (i.e.: to review, and report where they stand, and to execute improvements).

89%

of government agencies agree that organizations will face difficulties meeting the timelines of the EO

On top of deadline pressures, it seems that these mandates are likely to be a costly affair as there are concerns over having sufficient funding to fulfill the requirements outlined in the EO. Overall, 40% of those in US government agencies say that they have sufficient funding to fulfill all requirements of the EO, leaving the majority (60%) who do not. However, of those who do not have the sufficient funding, all (100%) anticipate using the EO as justification in a business case to obtain it.

But the outlook is brighter for some. For example, if you are a larger US government agency with 3,000 employees or more, then you are more likely to be in a better position, with 41% saying that they have sufficient funds for all elements, compared to 38% of smaller agencies with 500-2,999 employees.

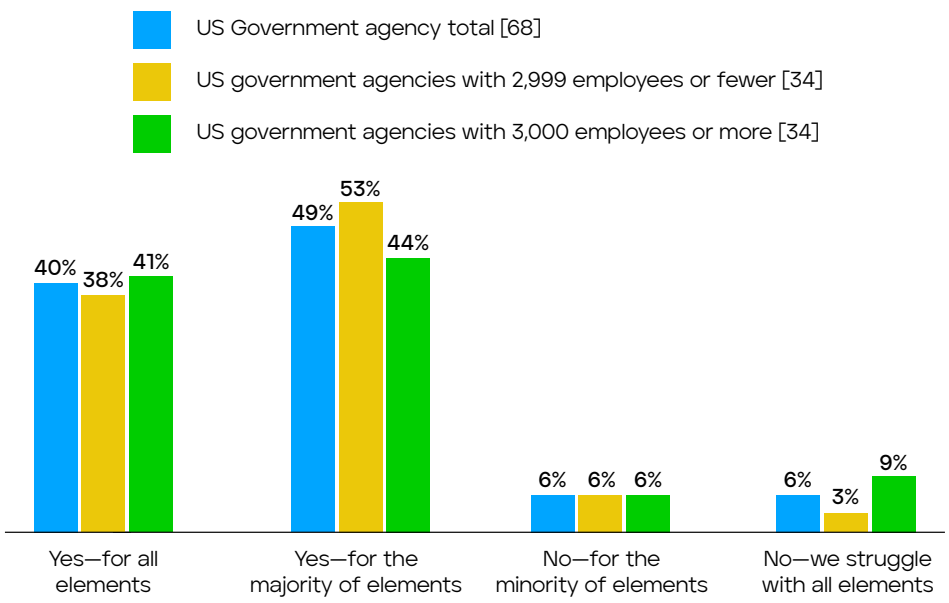


Figure 4: Do you believe that your organization has sufficient funding to fulfill the requirements of the EO? [base numbers in chart] asked to respondents in the US from government agencies, split by organization size

Echoing the earlier message that highlighted the importance of improving the security standards outlined for the development of software, 94% of respondents believe that cybersecurity standards for software development should be mandated by governments. While it is hoped that this would ensure consistency, the same proportion believe that there would be drawbacks such as government suggestions being too complex (47%) or expensive to implement (46%), and timelines being hard to adhere to (44%) - mirroring the concerns outlined for other elements of the EO.

94%

of respondents believe that cybersecurity standards for software development should be mandated by governments

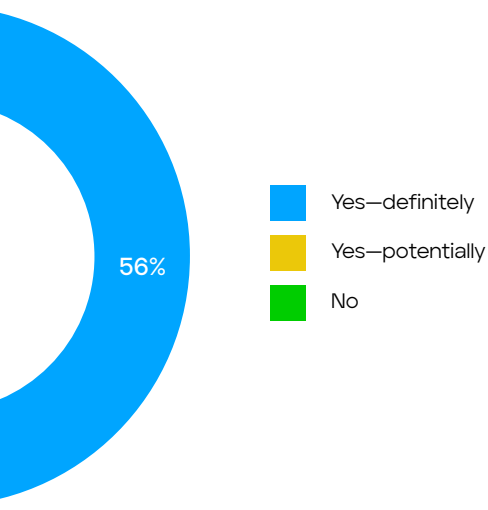


Figure 5: Do you believe that cybersecurity standards for software development should be mandated by governments? [900] omitting "Don't know"

While the overall aim of mandating software development and modernizing cybersecurity efforts is to minimize and limit cybersecurity incidents from occurring, there still is, and always will be some level of vulnerability and risk. When such incidents occur, it is just as important to analyze and understand what happened to make concrete recommendations for the inevitable next time. The US EO outlines the establishment of a Cybersecurity Safety Review Board, similar to the US National Transportation Safety Board, the former of which the vast majority (91%) of US respondents feel is necessary. While this is a popular suggestion, in practice, the level of oversight may be somewhat intrusive, with the EO stating that "the administration and private sector need to ask the hard questions" should an incident occur. However, improvement is front of mind, as 90% say that they would be comfortable with the level of oversight outlined. However, the finer details reveal an almost 50:50 split when thinking about who the board should focus on – 53% of respondents feel that it should only focus on government infrastructure, while 47% say that it should focus on either public sector and/or private sector infrastructure too. It is clear there may still be some logistics to be ironed out.

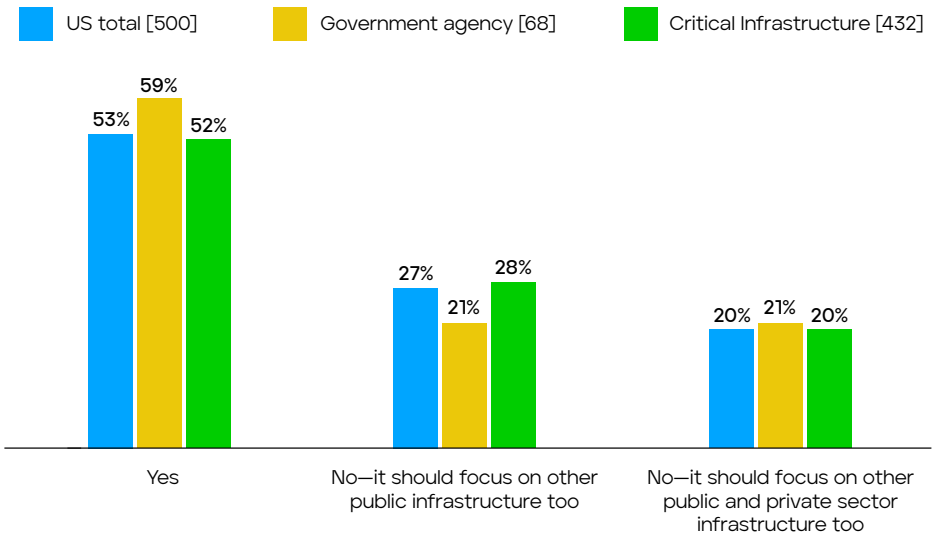


Figure 6: Do you feel that the Cybersecurity Safety Board (or similar) should focus only on government infrastructure? [base numbers in chart] split by respondent type within the US, omitting some answer options

Despite there being areas requiring further alignment, respondents from the US are optimistic that the EO will have a positive impact on cybersecurity. Supporting this, 96% feel that it will result in at least a low level of improvement (97% for those in critical infrastructure, 90% for those in government agencies). When exploring opinions across different regions, levels of confidence are similar, as 89% of those in APAC and 87% in Europe feel that formalized, government-led initiatives will lead to improved protection against cyberthreats.

96%

feel that the EO will result in at least a low level of improvement

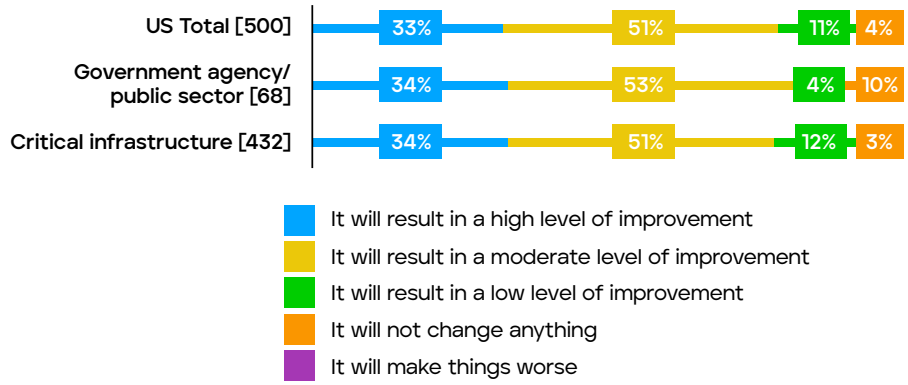


Figure 7: To what extent do you feel that the EO will change how well government agencies and other organizations are protected and defended against cyberthreats? [base numbers in chart] split by respondent type within the US, omitting some answer options

The reception of the US EO is generally positive with many indicating that they are confident in the improvements that it will bring to protecting against cyber incidents. These confidence levels extend globally when exploring views on government-led initiatives, and so it may be that other nations replicate a similar order to secure their cybersecurity postures as well. However, there are challenges which center on funding and meeting deadlines, and while some have the appropriate funding to meet the demands of the EO, it is important that the government appropriates additional funding to ensure a real improvement is made in its cybersecurity capabilities.

It is also important that the cybersecurity products being implemented are being developed securely, and so further mandates would be welcome. However intrusive these levels of oversight may feel, organizations suggest that they would be comfortable with this, if it introduces improvements and further protection. This positive outlook is an encouraging sign for governments, however, there are some doubts, as 89% feel that the EO will not be able to solve all current cybersecurity issues - there will still be gaps of which malicious actors can take advantage. Overall, however, the EO is perceived as an important step in the right direction.

Section III: Partnership

While the US EO aims to protect the nation against persistent and increasingly malicious actors, further attempts could be made to improve and enhance cybersecurity efforts. For example, critical infrastructure and government agencies must have a strong working partnership to see real success. It is certainly clear that there is room for improvement when thinking about this as almost all respondents (99.7%) believe that there are areas where greater support is needed from their country's government, such as:

99.7%
believe there are areas where greater support is needed from their country's government

- For all respondents' organizations - A combination of incident notification and liability protection to facilitate sharing of attack data between impacted organizations, government partners and industry audiences (43%)
- For those in US government agencies or critical infrastructure organizations – Improved guidance on best practices (46% and 44% respectively)

Casting the focus on the first point; when thinking about information sharing and incident reporting, historically government agencies have required access to information, but are less willing to share it, introducing friction between those entities and critical infrastructure organizations. This could be for several reasons such as contractual obligations, or concerns around privacy or data security incidents. Supporting this notion, 98% feel that there is at least a little room for improvement when thinking about the data shared by relevant organizations with the government, and vice versa, 98% feel that there is room for improvement when thinking about the data shared by the government to relevant organizations.

98%
feel there is room for improvement in the data shared by the government to relevant organizations

When thinking about potential data sharing improvements, these center on the quality (59%), relevance (50%), ease of access to (50%) and speed of the data being shared (46%), with the latter being a greater concern for those in the US (50%) compared to their European (43%) and APAC (42%) counterparts.

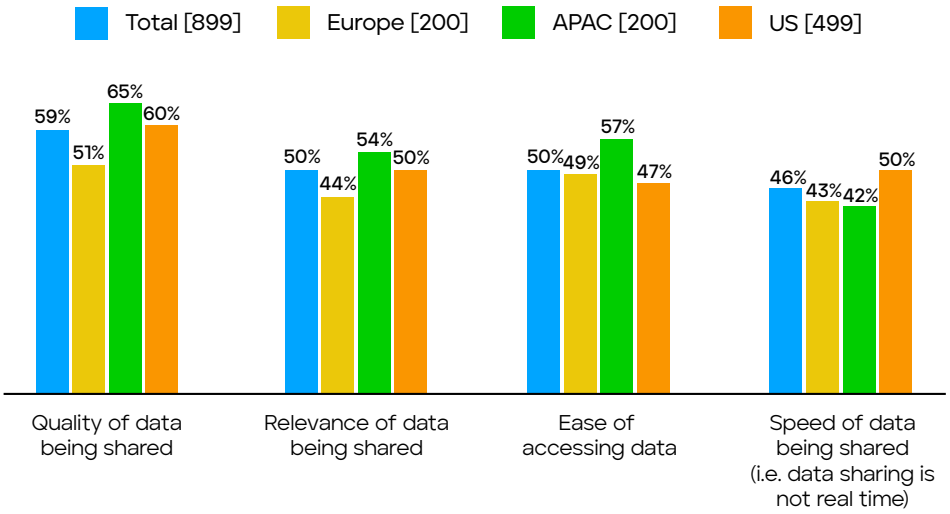


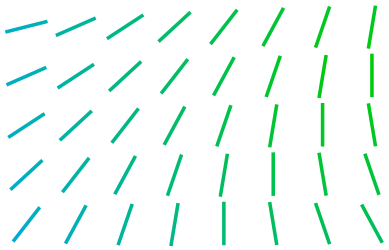
Figure 8: In which areas related to data sharing are improvements needed most? [base numbers in chart] asked to respondents who said there is "room for improvement" for statements in the context of information/data sharing, split by region, omitting some answer options

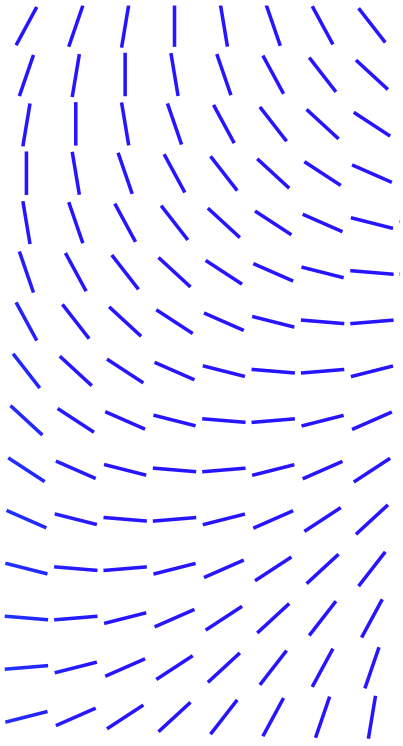
Further to this, there are improvements that could be made when thinking about the types of data which would be most useful and relevant for the government to share with critical infrastructure organizations, those being:

- Data that is known about different crime groups (48%)
- Data about cyber-attack campaigns in progress (47%)
- Data about common cybersecurity weaknesses in organizations (47%)
- Data about different attack vectors used (46%).

While the aforementioned types of data would be extremely helpful to private sector organizations, it is vital that the previous improvements (around quality, relevance, ease, and speed etc.) are considered too so that the data being shared is not only of good quality but is also shared in a timely manner so that it can be acted on quickly and confidently. Time is of the essence when acting against cyberthreats and criminals.

Overall, it is quite clear that there is room for improvement when casting the spotlight on the relationship between critical infrastructure and government agencies. A strong partnership between public and private sectors is vital in ensuring visibility and understanding of cyber-attacks targeting both groups, as well as improving cybersecurity as a whole for many nations across the globe.



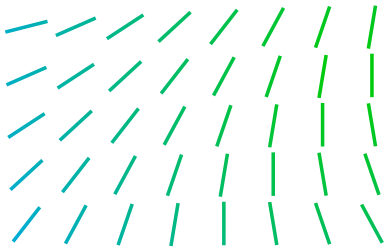


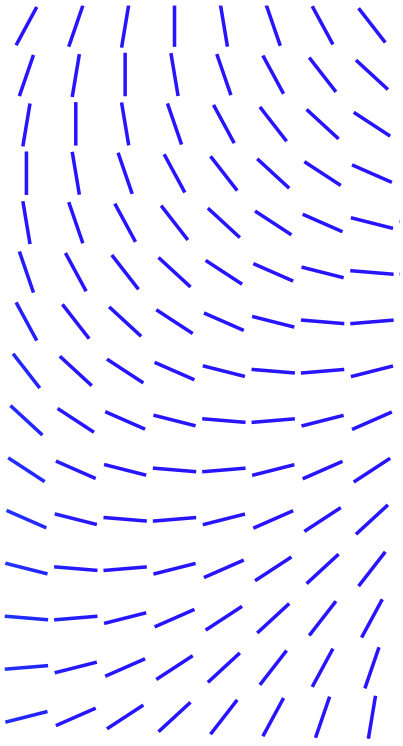
Conclusion:

Organizations are and will always be vulnerable to the ever-growing cyber-threat landscape that continues to become more sophisticated. To protect themselves, they must adopt more modern cybersecurity solutions to minimize the risks they continue to face. For those in the US, the recent EO may have acted as a catalyst to begin these modernization efforts, while for other nations across the globe the recent remote working requirement is likely to have introduced a further need for increased protection.

The broad elements and expectations of the EO are welcomed by many surveyed respondents from both critical infrastructure organizations and government agencies, and it is hoped that it will raise standards and improve responses to cyber incidents across the nation. Across other markets where an EO does not exist, there are high confidence levels in similar government-led initiatives, and so this may be the start of many more to come.

While these initiatives are imperative in seeing improvements in the protection of the evolving attack surface, it is also important to recognize that there are other areas that pose opportunities for progress. From data sharing to inconsistent playbooks, there are barriers that must be overcome to improve the relationship between the government and critical infrastructure institutions. Combined with government-led initiatives such as the US EO, organizations can confidently say that they are making significant progress to effectively thwart the threats of cyber adversaries.





Methodology:

Trellix commissioned independent market research agency Vanson Bourne to conduct the research upon which this whitepaper is based. Nine hundred security professionals from organizations with 500 or more employees, across several markets were surveyed from both government agencies (federal government and armed forces) and critical infrastructure organizations (local and provincial government, government critical infrastructure, private critical infrastructure), split in the following ways:

Region	Government agencies	Critical infrastructure	Total
Americas (US)	68	432	900
Europe (UK, Germany, France)	24	176	
APAC (India, Australia, Japan)	31	169	

All interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

About Trellix:

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers. More at https://trellix.com.

About Vanson Bourne:

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their 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.