ECSO
EUROPEAN CYBER SECURITY ORGANISATION

ECSO BAROMETER 2020: "CYBERSECURITY IN LIGHT OF COVID-19"

Report on the results of surveys with ECSO members and the cybersecurity community

Executive Summary

From March to May 2020, the European Cyber Security Organisation (ECSO) conducted surveys with its members and the cybersecurity community (large companies, RTO's/universities, regions/clusters, SME's, public administrations, EU institutions/agencies, users/operators, and associations) in order to better understand the impact of the COVID-19 pandemic on the activity of cybersecurity stakeholders during the crisis period, as well as their expected challenges post-crisis.

Here are the 7 key takeaways from the results of those surveys:

- From a cybersecurity standpoint, an increase in fraud, cybercrime and cyber attacks has been the top concern for organisations during the pandemic.
- Many organisations are concerned that they will have a lack of understanding of how the market has changed and evolved (for their organisation's business, activity, etc) once the current health crisis is over.
- The cybersecurity community believes that stronger public funding for research and innovation and a shorter cycle from research to innovation to cope with potential new disruptive challenges are fundamental aspects needed to recover activities after the COVID-19 crisis.
- There is a need for research & innovation across all areas of cybersecurity but the cybersecurity community considers infrastructure resilience and data & AI (including privacy) as particularly pertinent priorities to be tackled by Horizon Europe (HE) and the Digital Europe Programme (DEP).
- Artificial Intelligence, 5G & future communications network, and IoT are the key technological areas which will have a drastic impact on the future.
- The public services, e-government, and digital citizenship sector was indicated as the most relevant sector to suffer cyber threats due to digital transformation, with public administrations facing challenges with the sudden and complete shift to remote and online working. Critical infrastructures remain a priority when it comes to the prevalence of cyber attacks and ensuring cyber resilience, with a significant increase in cyber attacks experienced by the healthcare and financial sectors during the crisis.
- Advocacy, awareness, cyber resilience measures, visibility for solutions, and investment, capacity-building & competitiveness are the main pillars of needs expressed by the cybersecurity community during & after the COVID-19 crisis.

In light of these results, the report concludes with a set of recommendations centred around investing in Europe & fostering strategic public-private partnerships, leveraging European assets & increasing R&I funding, boosting European competitiveness, and placing cybersecurity at the heart of Europe's digital sovereignty.

Introduction

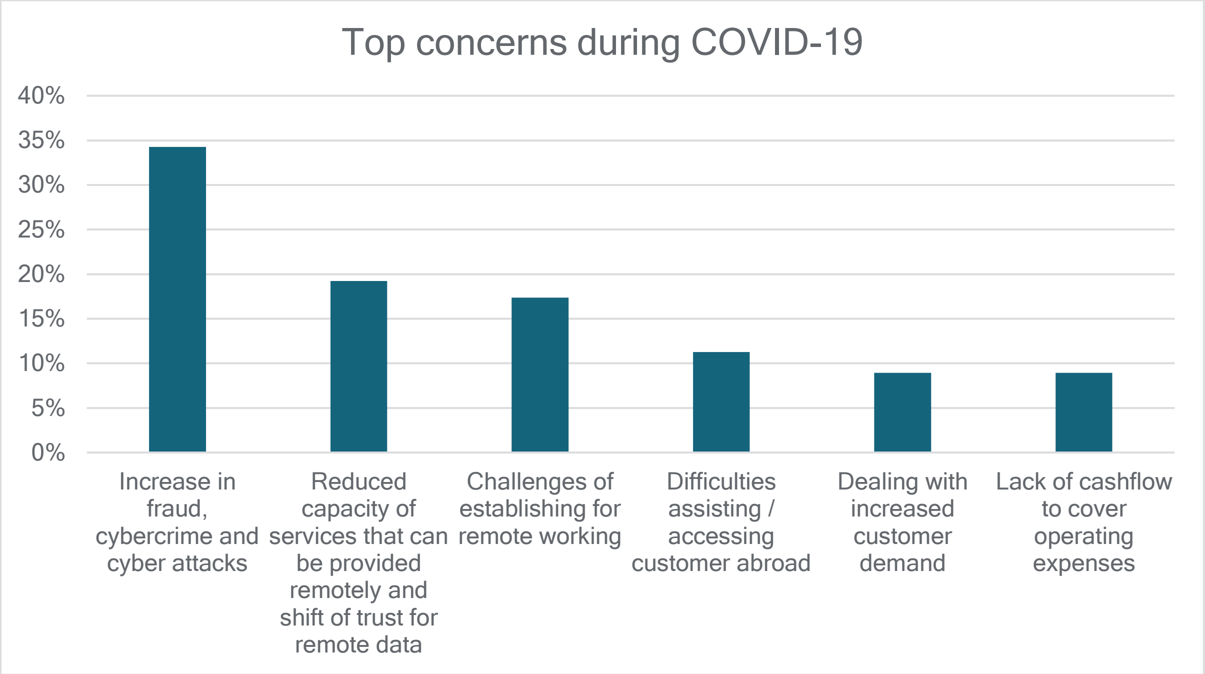
Across Europe, intensive efforts have been made to combat the global spread and effects of the coronavirus (COVID-19) pandemic with various measures to support public health systems, safeguard the economy and ensure public order and safety. At the same time, the outbreak has created an even more fertile ground for cybercrime, threatening the safety of citizens and businesses in a challenging operational and financial environment. As businesses and citizens increasingly rely on digital solutions, the nature of the threat is also changing, with cybercriminals exploiting fear, uncertainty and unprecedented situations. This crisis is a reminder of how crucial our digital ecosystem is to our economy, citizens, and political life. It is the invisible yet crucial foundation of today's world, upon which we rely to communicate. But the pandemic has also shown us how important it is to ensure the protection and resilience of the digital ecosystem across the entire value chain. In these challenging times, cybersecurity must be considered as an essential instrument to ensure the secure and coordinated implementation of global financial, political and sanitary contingency plans, as well as of the safety of citizens.

To further explore the effects of the COVID-19 crisis, from March to May 2020, ECSO conducted surveys internally with members as well as externally with the community through webinar polls in order to better understand the impact of the COVID-19 pandemic on the activity of cybersecurity stakeholders during the crisis period, as well as their expected challenges post-crisis. The results are taken from an internal survey of ECSO members as well as polls conducted during the first two webinars of the ECSO Webinar Series 'Cyber Resilience during and after COVID-19" (on Digital Europe and the Horizon Europe Programme) which had over 340 participants combined. Respondents came from all categories of cybersecurity stakeholders in Europe: RTO's/universities, regions/clusters, SME's, Large Companies (users and providers), public administrations, EU institutions/agencies, users/operators, and associations.

The following report provides a summary of the results of these surveys and offers recommendations to the European community for cybersecurity in light of the COVID-19 crisis.

Results

Top concerns for organisation's activity during the COVID-19 pandemic



34% of respondents listed 'Increase in fraud, cybercrime and cyber attacks' as their top concern for their organisation's activity during the pandemic. This is unsurprising considering the fact that we have seen a significant increase in cyber attacks of varying nature during the COVID-19 crisis.

The heightened concern of cyber attacks has surely also been propagated by the fact that the pandemic forced everyone into remote working and to go digital in all aspects of life. With increased activity online comes an increased risk of exposure to cyber attacks. Criminals have more entry points than ever before as everything which is connected to a network is a target.

Several reports from Europol[1] show that criminals took advantage of the virus proliferation very quickly and are abusing the demand that people have for information and supplies. Europol has observed that:

- There has been an increase in cyber attacks as cybercriminals have sought to exploit an increasing number of attack vectors as telework has become the norm and allowed connections to their organisations' systems. One of main examples of this is when the Czech Republic reported a cyberattack on Brno University Hospital which forced the hospital to shut down its entire IT network, postpone urgent surgical interventions, and re-route new acute patients to a nearby hospital.

[1] STAYING SAFE DURING COVID-19: WHAT YOU NEED TO KNOW (2020), https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know

- Criminals have used the COVID-19 crisis to carry out social engineering attacks, namely phishing emails through spam campaigns and more targeted attempts such as business email compromise (BEC).
- There has been a prevalence of phishing campaigns that distribute malware via malicious links and attachments and execute malware and ransomware attacks aiming to profit from the global health crisis.
- Fraud schemes have been used to target citizens, businesses and public organisations through bogus websites, fake apps, fake investment opportunities, and money muling. They also expect several new or adapted fraud schemes to emerge over the coming weeks as fraudsters will attempt to further capitalise on the current situation.

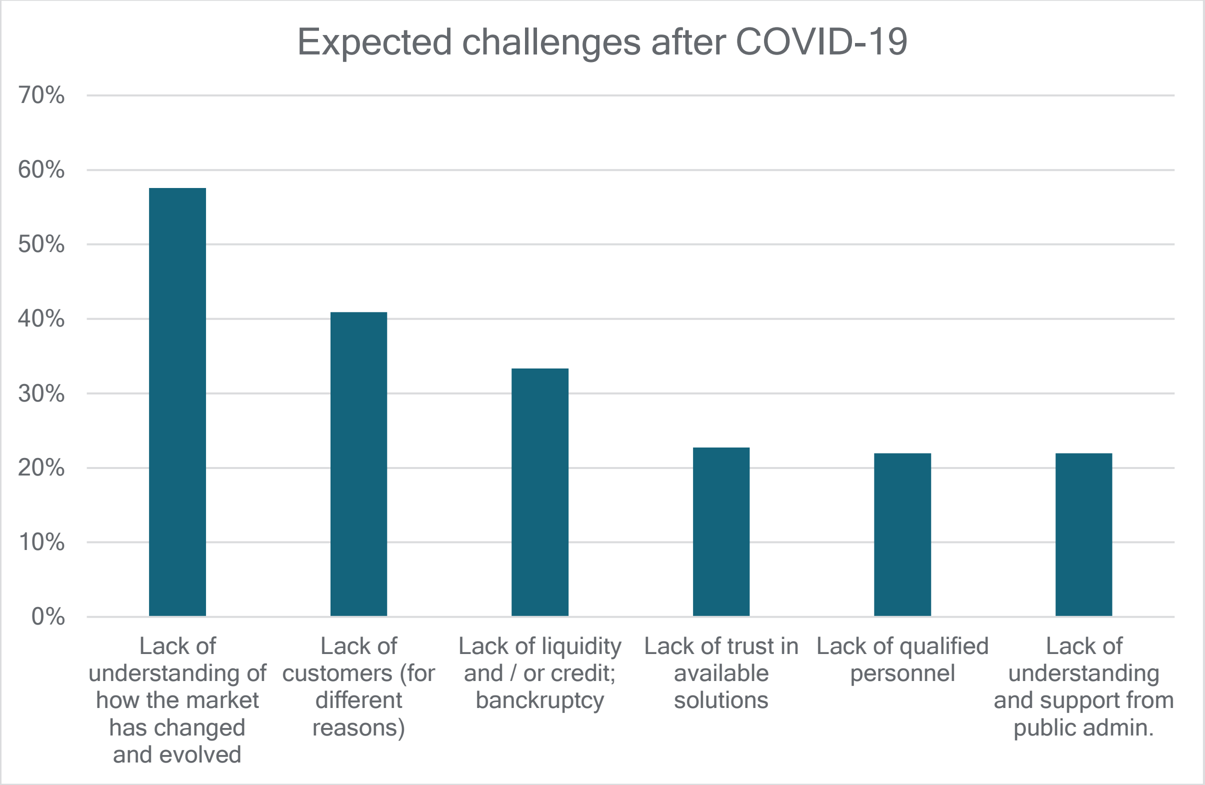
The financial sector is still the main target of phishing attacks while the healthcare sector is particularly affected by ransomware attacks. It is no surprise then that there has been an increased focus on these two sectors during the crisis and we could expect this to continue, along with calls for increased cyber resilience of critical infrastructures in general, after the crisis.

The other main concerns indicated by respondents were 'Reduced capacity of services that can be provided remotely and shift of trust for remote data' (19%) and 'Challenges of establishing guidelines for remote working' (17%) which demonstrates that challenges related to remote working have been at the forefront of people's minds, with organisations needing to act swiftly to manage the need to go completely online and remote during the pandemic. This has resulted in several observed trends & challenges:

- Increased Internet traffic.
- Increased reliance on secure remote access technologies (including VPN – Virtual Private Networks) which employees are not always familiar with and with potentially sensitive links between professional and personal computers and associated devices (e.g., personal printers).
- Increased use of smartphones (including access to secure mobile applications) for remote conferences, exchange of documents etc.
- Increased attack surface as more individuals work from home and part of the internal company network could be reachable from outside.
- Increased need to help SMEs protect their ICT infrastructures.
- Increased need to raise awareness on cyber threats during the COVID-19 crisis which have sought to take advantage of the pervasive shift to remote working (phishing, fraud, videoconferencing, etc.).

IT and cybersecurity, despite remaining operational during the COVID-19 crisis, could be seen as a secondary priority compared to other economic emergencies and could therefore face budget cuts to facilitate the recovery of major economic sectors paralysed by the crisis (transport, tourism, large part of industrial manufacturing, etc.). Yet, we should not forget that cybersecurity is and will be a support to economy recovery with its strong market growth. It is thus essential to urgently address ways to improve the resilience of digital processes, supply chains and critical infrastructures at local / regional, national and European level in the short and medium / long term.

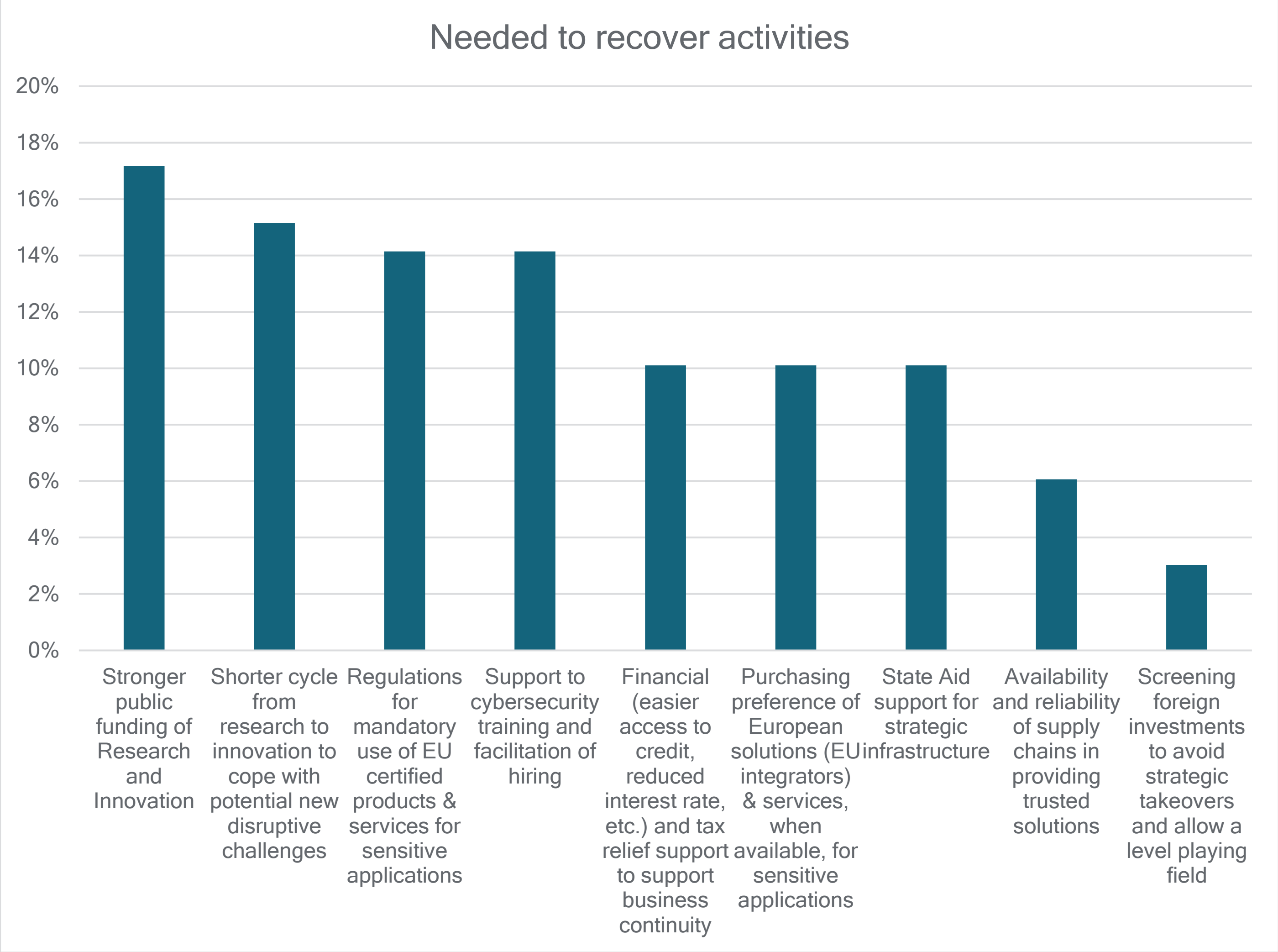
Expected challenges (for organisation's business, activity, etc) once the current health crisis is over



58% of respondents listed 'Lack of understanding of how the market has changed and evolved' as their top expected challenge (for their organisation's business, activity, etc) once the current health crisis is over. With an insufficient understanding of how the market has evolved comes uncertainties with regards to how one's business has been or will be affected. Most cybersecurity organisations will not have considered the potential impact of a global pandemic in their business continuity and incident response plans but these must be reviewed and consider the effect of a pandemic such as COVID-19 on the market, business, and critical elements of the supply chain, with cybersecurity at the heart of this.

While some organisations will experience a decrease in investment in new digital processes and the security needed to improve resilience because of the crisis, there could also be an opportunity to generate revenue by leveraging digitalisation and industry innovation to create increased automation, faster detection and response, and an accelerated transition into cloud-based services.
As cybersecurity is a market composed by many different technologies applied to many different applications, digitalisation and industry innovation should be brought forward with a specific approach for cooperation with the private sector for market aspects and stronger synergies for public-private investments and procurements.

What would be needed to recover activities once the current health crisis is over



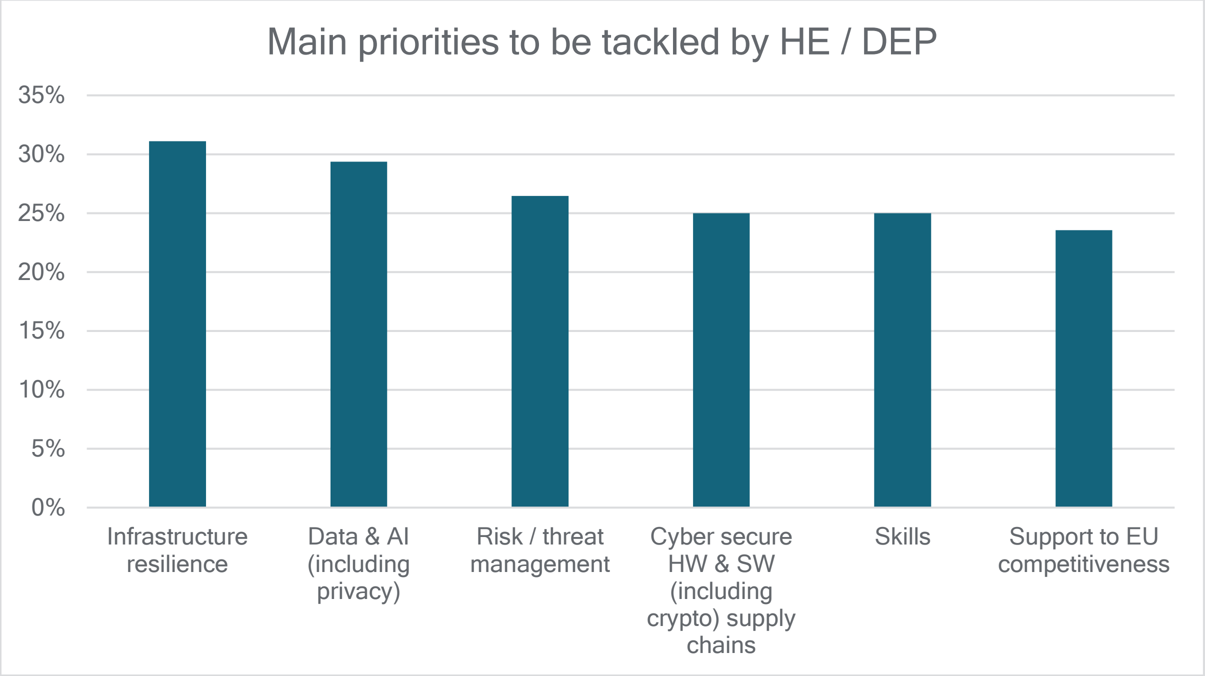
‘Stronger public funding of Research and Innovation’ (17%) and ‘Shorter cycle from research to innovation to cope with potential new disruptive challenges’ (15%) were the top answers for what would be needed to recover activities once the current health crisis is over. This was closely followed by ‘Regulations for mandatory use of EU certified products & services for sensitive applications’ (14%) and ‘Support to cybersecurity training and facilitation of hiring’ (14%).

There is an urgent need to re-define priorities for R&I (Horizon Europe) and DEP (or other EU funds) in light of the post-COVID society and market evolutions. There could be concerns that with the slowing down of the economy there would be possible cuts in R&I funding in the next years. Yet, the European Commission’s recent proposal[2] for a Next Generation EU recovery package clearly shows the willingness to boost investment in R&I as a direct response to the effects of the COVID-19 crisis.

[2] Europe's moment: Repair and prepare for the next generation (2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_940

The European Commission’s proposal recognises the need for increased investment in Horizon Europe (HE) and the Digital Europe Programme (DEP) and has reflected this in its new reinforced Multi-Financial Framework (MFF) 2021-2027 proposal (total proposed: 1.100 Bn€). Horizon Europe will in the end probably get more funding than expected in the initial proposal while the Digital Europe Programme (a new programme for the next Multi-Financial Framework) will enable the financing of projects in cybersecurity, AI, quantum technologies, etc.

Main priorities to be tackled by HE and DEP

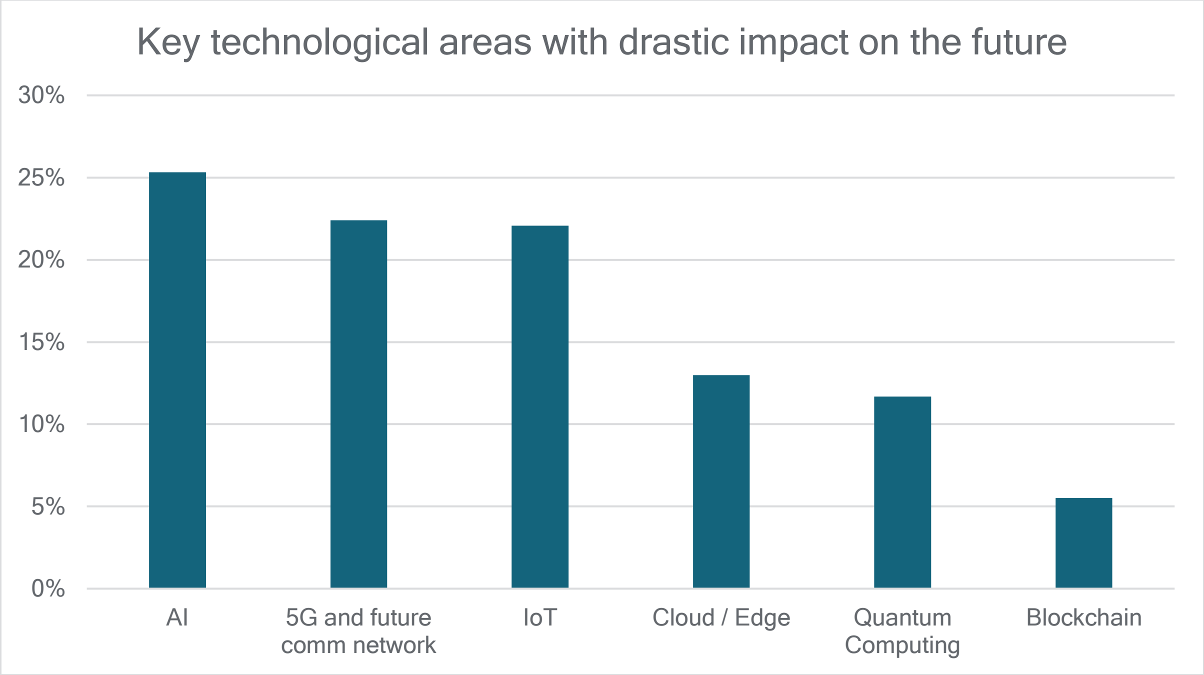


The main priority to be tackled by Horizon Europe (HE) and the Digital Europe Programme (DEP) as indicated by respondents was 'Infrastructure resilience' (31%), which was closely followed by 'Data & AI (including privacy)' (29%), but the values for all answers were quite close. This clearly demonstrates that the appetite and need for R&I across cybersecurity topics is stronger than ever.

The Digital Europe Programme (DEP) will likely focus on a higher digital recovery after the pandemic and this is likely to be reflected in the new Multiannual Financial Framework (MFF), with a higher budget redistributed to support the digital recovery. In Europe, R&I is a strong asset and we have a pool of knowledge that is recognised worldwide. Policy makers should therefore be able to leverage on these existing assets to meet current and future challenges.

When it comes to infrastructure resilience, there is a need to increase investments on commonly redefined and agreed priorities for sensitive / strategic applications and critical infrastructures through "close to market" projects with a high TRL (Technology Readiness Level), supported by procurement policies. This should be coupled with reinforced measures to ensure that operators of essential services can maintain and make their IT infrastructure resilient and dependable in times of high demand and crisis. This should also be considered for the coming review of the Network and Information Security (NIS) Directive, in close consultation with the NIS Cooperation Group.

Key technological areas that will have a drastic impact for the future



25% of respondents indicated ‘Artificial Intelligence’ as the key technological area which will have a drastic impact on the future, closely followed by ‘5G and future comm network’ (22%) and ‘IoT’ (22%).

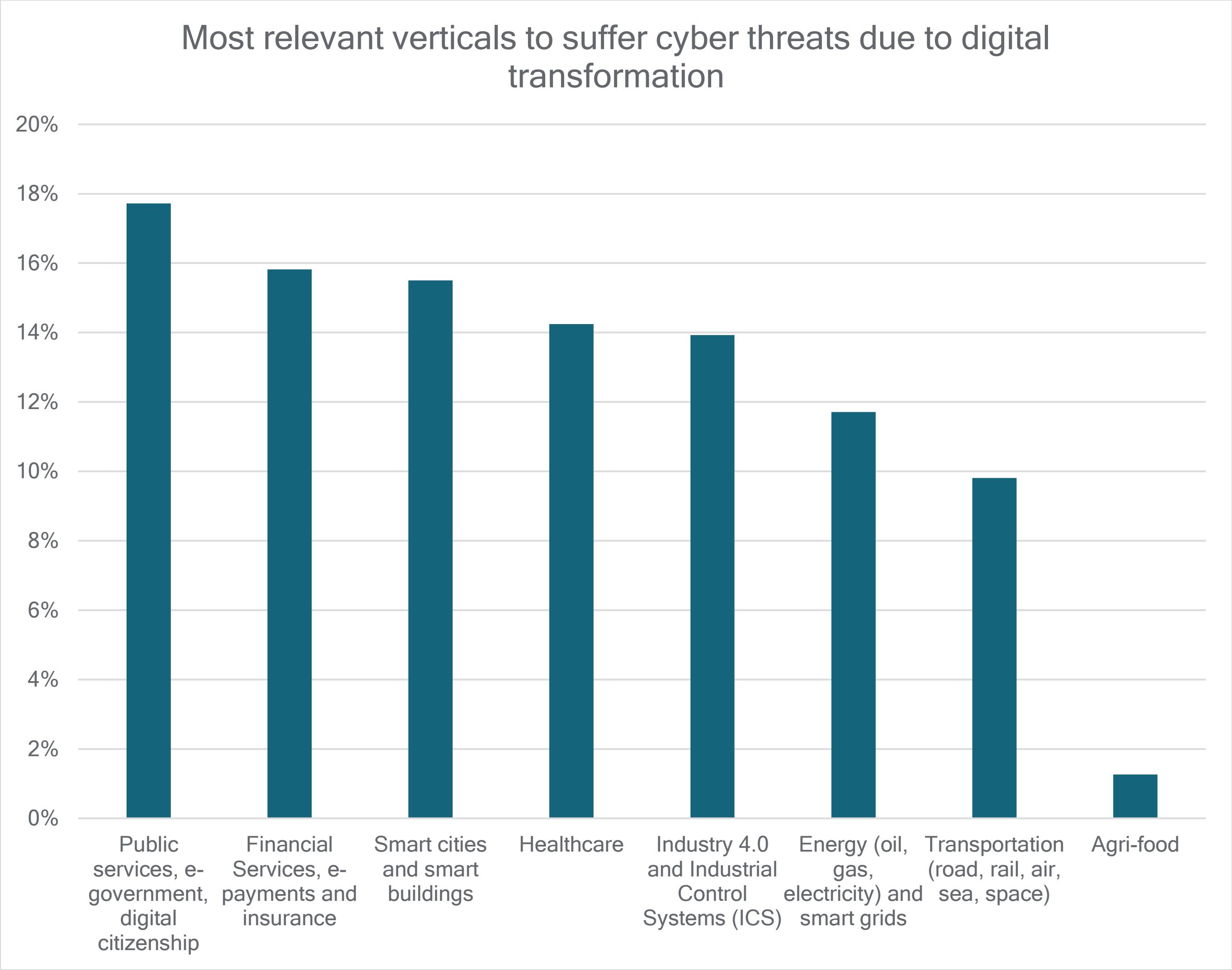
In the post crisis period, there will be an increased use of IT solutions to, inter alia, speed up the recovery of manufacturing. To facilitate the recovery from this crisis in Europe in particular, we could expect accelerated digitalisation (more than anticipated in the pre-COVID era) in Industry 4.0 of IoT, Artificial Intelligence, 5G, Cloud & Edge computing, blockchain, high performance computing, automated decision making and management of large amounts of data. It is important to note that cybersecurity is the “glue” linking all these technologies and their use in the different applications / verticals. The use of new technologies will help address specific needs, but it will also further increase the attack surface: applications should be adequately protected against evolving threats by the “cybersecurity glue”. Investment and capacity-building (i.e. through key technology strategic partnerships) will be key here.

The European Commission’s Next Generation EU proposal is a step in the right direction as it looks to harness the full potential of the EU budget and allocate €8.2 billion toward the Digital Europe Programme (DEP), involving investments in supercomputing, artificial intelligence and cybersecurity. This includes:

- Investing in more and better connectivity, especially in the rapid deployment of 5G networks.
- A stronger industrial and technological presence in strategic sectors, including artificial intelligence, cybersecurity, supercomputing and cloud.
- Building a real data economy as a motor for innovation and job creation.
- Increased cyber resilience.

The responses to our survey clearly indicate support from the cybersecurity community for the European Commission’s proposal to be approved as AI, 5G, and IoT are at the forefront of disruptive technologies that will impact but also drive the future European cybersecurity market, research and policy area.

Most relevant verticals to suffer cyber threats due to digital transformation



18% of our respondents indicated ‘Public services, e-government, digital citizenship’ as the most relevant sector to suffer cyber threats due to digital transformation, closely followed by ‘Financial services, e-payments, and insurance’ (16%) and ‘Smart cities and smart buildings’ (16%). It should be noted that other sectors, with the exception of ‘Agri-food’, followed closely as relevant sectors in this regard.

If we look at it in the context of the COVID-19 crisis, it is clear that public administrations have been particularly affected with significant difficulties in managing remote working and an increase in cyber attacks. It should also be noted that public administrations represented a much bigger percentage of our respondents than users/operators. One could therefore expect less emphasis on operational issues linked to the main critical infrastructures in the responses. Yet, these essential and strategic sectors will be even more important post-COVID-19 as efforts will be needed to increase the cyber resilience of our critical infrastructures and supply chain, and this is crucially also highlighted as a priority in the Next Generation EU proposal.

The financial sector is of course particularly vulnerable to cyber attacks (especially phishing) and fraud, and it is a sector that is consistently flagged as a priority by the cybersecurity community as the continuation of services (e.g. online banking) and maintaining the reputation and integrity of banks is of paramount importance to ensuring cyber resilience and the smooth running of the economy. Smart cities and smart buildings are not usually indicated as a priority in our discussions with the community, at least not as a standalone sector, but rather it is highlighted for the pervasiveness of IoT and its importance for the increased digitalisation of society and cities. This, along with its impact on all other sectors of the economy, surely explains its rating here.

Cybersecurity needs & requirements will increase as the digital transformation of our critical infrastructures and society accelerates. The COVID-19 crisis has been a massive booster for digital transformation but it has also increased our exposure to vulnerabilities and threats. More than ever, we need trusted solutions and ones that we master in Europe so we can ensure that our future is digital and secure. This crisis has shown the need for an increased autonomy in critical sectors and the recovery of digital sovereignty. Long term sovereignty and resilience of the EU and its Member States should be recovered in the cybersecurity sector, and cyber sovereignty should be one of the main driving objectives for future investments. The cybersecurity industry must be recognised as a vital sector for Europe and its countries and it could be part of those “critical infrastructures” that need to be developed, supported and preserved.

Supporting the cybersecurity community during COVID-19: main needs expressed

Advocacy

Build technological partnerships
Organise events, networking

Awareness

Inform citizens on cyber risk
Fake news, disinformation

Cyber resilience

Information sharing and strategic intelligence
Risk mitigation
Focus on sectoral needs
Early warning

Investment, capacity-building & competitiveness

Match offer and demand
Provide information on funding and consortia building

Solutions

Showcase industry security & privacy solutions

Supporting the cybersecurity community after COVID-19: main needs expressed

Advocacy

Advocate for a reliable, safe and secure European IT backbone

Awareness

Raise awareness on cyber threats, especially in the healthcare sector

Give visibility to the impact produced during the crisis as a consequence of ineffective cybersecurity measures

Develop a post-crisis comms strategy

Cyber resilience

Collect lessons learned

Report on needs of sectors

Investment, capacity-building & competitiveness

Match offer and demand

Facilitate consortia building

Develop a public and private co-investment mechanism to boost development, competitiveness and business.

Solutions

Provide solutions that uphold security and privacy

Provide solutions for weakened supply chains

Information on remote working solutions

Recommendations

As we look to strengthen the cyber resilience of our infrastructures and keep up with the accelerated digital transformation of our economy & society, we have an opportunity to make Europe a leader in the cybersecurity industry but we need proper funding, investment, and access to market to achieve this. In light of the results of the surveys conducted with ECSO members and the community on cybersecurity needs during and after COVID-19, we offer the following recommendations to steer investments, public-private cooperation, and technologies in cybersecurity in Europe in the years to come:

Invest in Europe & foster strategic partnerships

- Increase investments on commonly redefined and agreed priorities for sensitive / strategic applications and critical infrastructures through "close to market" projects with high TRL (Technology Readiness Level), supported by procurement policies.
- Reinforce measures to ensure that operators of essential services can maintain and make their IT infrastructure resilient and dependable in times of high demand and crisis.
- Support the accelerated digitalisation in Industry 4.0 of IoT, Artificial Intelligence, 5G, cloud & edge computing, blockchain, high performance computing, automated decision making and management of large amounts of data, i.e. through strategic partnerships.
- Invest in cybersecurity on a massive scale (e.g. venture capital, public-private co-investment) as it represents the "glue" linking all technologies and their use in the different applications / verticals. The use of new technologies will help address specific needs, but it will also further increase the attack surface: applications should therefore be adequately protected against evolving threats.

Leverage European assets & increase R&I funding

- Re-define priorities and increase funding for R&I (Horizon Europe) and DEP (or other EU funds) in light of the post-COVID society and market evolutions.
- Ensure that research funding covers the full spectrum of the cybersecurity industrial ecosystem, from infrastructure resilience, data & privacy, and risk/threat management, to skills and support to EU competitiveness. It is only by ensuring that R&I underpins the needs of the entire value & supply chain that we will be able to boost the cybersecurity market, innovation, and job creation in Europe.
- Leverage on Europe's strongest assets and showcase European cybersecurity champions in research, drivers of industrial innovation, and data & privacy ambassadors on a global scale.

Boost European competitiveness

- Engage the cybersecurity industry to support the economic recovery with its strong market growth.
- Address ways to improve the resilience of digital processes, supply chains and critical infrastructures at local / regional, national and European level in the short and medium / long term.
- Develop a specific approach to consolidate the European cybersecurity market (linking technologies and applications) in closer cooperation with the private sector for market aspects and stronger synergies for public-private investments and procurements.

Place cybersecurity at the heart of Europe’s digital sovereignty

- Invest in trusted solutions and ones that we master in Europe so we can ensure that our future is digital and secure.
- Increase autonomy in critical / vital sectors and recover the long-term sovereignty and resilience of the EU and its Member States.
- Make cyber sovereignty one of the main driving objectives for future investments.
- Recognise the cybersecurity industry as a vital sector for Europe and its countries and make it part of our “critical infrastructures” that need to be developed, supported and preserved.

For more, read the ECSO recommendations on cybersecurity in light of the COVID-19 crisis.