Enhancing Cybersecurity and Digital Resilience in Europe

Executive Summary

Today we find ourselves at a crossroads for the Internet's future. On one hand, digital tools have never been more essential for people to access information, to connect with one another, to work, to learn. On the other hand, malicious cyber activity has grown more frequent and disruptive, costing European businesses billions of euros each year and fraying public trust in the digital ecosystem. Meanwhile, disagreements over Internet governance threaten to upend transatlantic digital commerce and security at a time when assertive challenges from authoritarian states demand cooperation among democracies.

The European Commission has responded through sweeping measures, such as the Cybersecurity Act, which empowered the EU Agency for Cybersecurity (ENISA) to drive improvements in the baseline security capabilities of EU institutions and Member States. For our part, we have been tracking cyber threats to European businesses and consumers for more than two decades, and work around the clock to uphold the trust and security on which a vibrant, inclusive European digital society depends.

In recent months, the war in Ukraine has offered the world a first glimpse of full-scale conflict in cyberspace. It has also underlined the importance of governments, civil society, and industry coming together to protect citizens and democratic institutions from online threats. Google, like many other companies, answered the call to help protect the Ukrainian people and their government.

This paper draws on the expertise of dozens of practitioners with decades of experience supporting European public and private sector organisations. It is intended to serve first and foremost as a resource for policymakers. It outlines Google's observations on strategic security trends and shares how our approach to "open security" can advance digital security and resilience in Europe.

We encourage the EU to embrace the following principles in guiding future cybersecurity legislation and regulation, just as they have guided our global security programme:

- The best security solutions enhance openness and interoperability, rather than limiting them
- Transparency is essential to protecting users from online threats
- Digital technologies must be secure by default
- Security must become more intelligent
- Public-private collaboration is essential to raising the security bar for all

Under President Ursula von der Leyen, the European Commission has advanced an ambitious digital agenda centred on economic transformation, digital inclusion, and shared prosperity underpinned by robust safety and security. Google shares these goals and values, and is committed to working with the EU, European Member States, and institutions such as ENISA as a trusted partner. To make this vision a reality, we recommend that the EU advance technology policies that put user protections first, promote innovation and technology modernisation, and explore new models of public-private partnership for collective defence.

We respectfully put forward seven **recommendations to the EU**, based on our experience in the cybersecurity space:

- Foster an ecosystem that promotes open security principles
- Invest in digital transformation to enhance ecosystem-wide security and resilience
- Engage industry and international partners to share intelligence and combat cybercrime
- Protect high-risk groups from malicious cyber activity
- Develop a “security impact assessment” for new regulations
- Partner with industry to expand access to security education and training resources
- Prioritise strong encryption over data location

I. Rapidly Changing Landscape

Rising cyber threats continue to erode trust in digital technologies. The pandemic, which accelerated digitisation trends in both the personal and professional settings, coincided with a rise in malicious cyber activities against European businesses and institutions, with attacks and the overall cost of remediating ransomware incidents doubling from 2020 to 2021. Despite this troubling outlook, we also see encouraging signs of cooperation and collaboration in building more secure and resilient societies. We want to highlight three noteworthy trends impacting cybersecurity in Europe.

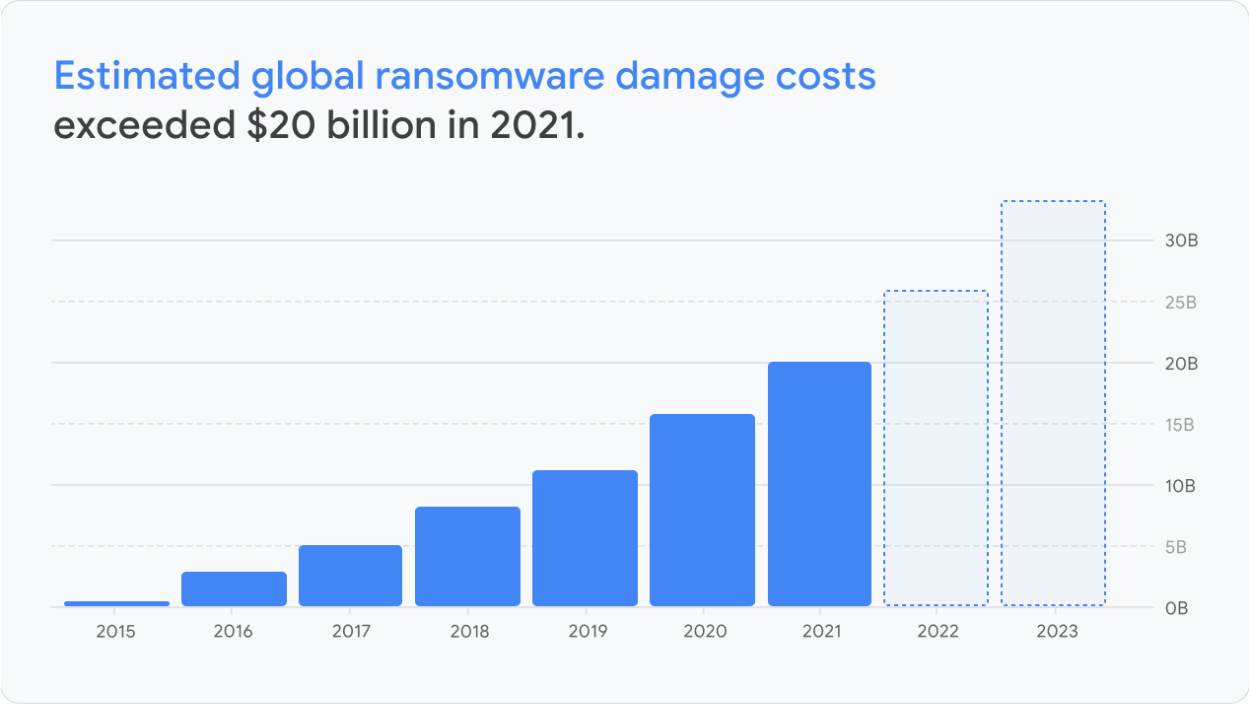
1.1 Strengthened collaboration in the light of the war in Ukraine

The war in Ukraine has demonstrated the extent to which software can be weaponized against everyday people and the public infrastructure they depend on. Russia-backed hacking and influence operations are not new to Google; we've been taking action against them for years. We are constantly disrupting campaigns targeting individuals and organisations in Ukraine as well as other activity from groups attributed to Russian and Belarus actors and notified law enforcement. Our Threat Analysis Group (TAG) has seen threat actors evolve their focus as the war continues. For example, we've seen some threat actors, including from China, shift to focus on Ukraine targets. We have also detected Russian threat actors targeting other Eastern European governments, military organisations, and NATO. A growing number of threat actors are using the war as a lure in phishing and malware campaigns. This includes state sponsored actors from China, Iran, North Korea and others.

The war in Ukraine is a tragedy for millions impacted or displaced by the fighting. But it has also illustrated what can be accomplished when governments, industry, and civil society come together in defence of shared values. The Ukraine conflict has shown that like-minded governments and civil society must work together in new ways to protect high-risk users and enhance digital resilience and redundancy.

1.2 The ransomware crisis persists

In 2020 and 2021, ENISA assessed ransomware as the "prime threat" to European businesses and organisations, which continues to pose serious risks. Attacks such as WannaCry and NotPetya caused billions of euros in damage, with much of that cost borne by European businesses and organisations. Ransomware cost global businesses an estimated $20 billion in 2021. Most concerning is the targeting of critical infrastructure – sectors such as healthcare, energy, and transportation – which could result in widespread disruptions to economic activity and social stability.



Source: Cybersecurity Ventures, June 2022

The ransomware crisis is exacerbated by deep reliance on a small number of legacy enterprise email providers and outdated security architectures that fail to prevent a single compromised machine from infecting entire networks. Addressing it is an urgent challenge. It will require systemic investments in digital transformation, zero trust architectures, and operating systems and devices that are secure by default. It will also take broader efforts to combat the ransomware epidemic through diplomacy, operational collaboration, and policy-making. Google welcomes the commitments and investments European governments have made to counter threats from ransomware, and we are eager to contribute to mitigating this pervasive challenge.

1.3 Rise of the "splinternet"

The war in Ukraine has accelerated worrying trends in Internet governance, as the digital divide between nations seems deeper than ever. The war has prompted calls for unprecedented sanctions affecting core Internet services like the Domain Name System and Certificate Authorities which would have severed Russia from core Internet connectivity. And it has accelerated steps taken by Russia and other authoritarian nations to aggressively surveil and control citizen behaviour online. But the schism is deeper than this: we are also seeing democratic governments developing policies that would threaten opportunity for millions of citizens. According to the OECD, Information Technology and Innovation Foundation, and others, Internet fragmentation policies are linked to a lower volume of trade, lower productivity, and higher prices for downstream industries that rely on digital technologies and the free flow of data. Internet fragmentation negatively impacts security as well, as it limits organisations and governments from tapping into the universal availability and resilience of global infrastructure while restricting situational awareness about global threats.

II. Driving European Resilience Through "Open Security"

To some, the concept of "open security" may seem a paradox. Throughout history, security in the physical world has been a privilege for those fortunate enough to live behind high walls and sturdy gates. In the days of the early Internet, organisations were beholden to a similar paradigm: corporate information security departments were tasked with protecting the perimeter, keeping user information and intellectual property inside the walled garden, and intruders out.

But as the Internet evolved, cracks in that approach became readily apparent. The proliferation of email phishing meant that it might take only a single misguided click to let attackers bypass the corporate firewalls. The rise of cloud computing further eroded organisational boundaries as the world's leading companies began tapping into rented computing power. More recently, the global COVID-19 pandemic forced organisations to adapt to their workforces doing their jobs remotely, outside the perimeter.

> Malware is the attack technique employed in 62% of supply chain attacks
>
> ENISA Threat Landscape for Supply Chain Attacks, Press Release, 2021

Over the last half-decade, disruptive attacks such as WannaCry and SolarWinds have proven a catalyst for businesses and governments to rethink our approach to cybersecurity at both the technical and political levels. Google had its own wakeup call more than a decade ago when we were the target of an advanced nation-state operation, now known as Operation Aurora. In the aftermath of the attack, we dismantled our existing security model piece by piece and embraced a new approach built on open principles, secure-by-default products, zero trust architecture, collaborative partnerships, and investment to push the frontiers of information security at global scale.

Where others promise security through digital walls and moats, data localisation, or closed ecosystems, open security acknowledges that information is only useful when it is accessible. The role of information security is therefore to ensure that information is available to those authorised to possess it – no matter where they are – and *only* to those authorised to possess it. Security based on open principles necessarily takes ingenuity. But it is achievable for public and private sector organisations of all sizes around the world.

We encourage the EU to embrace the following principles in guiding future cybersecurity legislation and regulation, just as they have guided our global security programme:

The best security solutions enhance openness and interoperability, rather than limiting them. The growing need to accommodate an increasingly global, remote workforce and enable the adoption of hybrid and multi-cloud environments will require security practitioners to look beyond perimeter defence models. In the aftermath of Operation Aurora, Google was faced with a similar challenge: how could we enhance our security while preserving the openness required to organise the world's information and make it universally accessible and useful? Our answer was to pioneer the zero trust model and scale it across our global network. In a zero trust model, all users, devices, and applications are continuously vetted for security risks and access to information is earned. With a zero trust model in place, businesses and governments can apply consistent protections across users and workloads, regardless of whether they're working from a corporate office or at home, or whether they're running in the cloud or an on-site data centre.

Transparency is essential to protecting users from online threats. Greater scrutiny by thousands of eyes produces digital products and services that are more secure, more reliable, and more trustworthy. Google is a proud believer in the open source software movement and a key contributor to open source security projects, such as SLSA. At the same time, it's essential to uphold shared transparency principles to ensure that organisations can responsibly disclose information about product vulnerabilities so that they can be patched, or about threats to public safety or democratic processes without compromising privacy protections.

Digital technologies must be secure by default. Open security requires that organisations focus on the fundamentals of software development and embed security at every stage of the product life cycle, from design through deployment. Users should be confident that the data they entrust to their devices, browsers, or cloud platforms remains safe with minimal manual configuration on their part. State-of-the-art security should be seamless, ubiquitous, and seemingly invisible. For example, Google embeds strong ransomware protections in its devices, operating systems, and platforms like Workspace. ***There has never been a reported successful ransomware attack against a ChromeOS device.***

Security must become more intelligent. The global demand for digital security is fast outpacing the supply of trained security professionals. Governments, businesses, and universities must develop common strategies to expand security education and training to close this gap. At the same time, businesses and governments should modernise their approach to security operations to take advantage of automation to free up analysts for higher order tasks and artificial intelligence to respond to threats at machine speed.

Public-private collaboration is essential to raising the security bar for all. Governments have an unprecedented opportunity to strengthen security through agenda-setting, public investments in technology modernisation, and policies that motivate security-conscious behaviours. At the same time, technology companies have the opportunity to advance ecosystem-wide improvements in security through implementing essential features, such as 2-step verification, at global scale and through democratising advanced security tools, such as

zero trust architecture or advanced DDoS protections, for users and organisations of all sizes. Public-private partnerships will prove essential to our collective efforts to push the frontiers of security, including the development and implementation of post-quantum cryptography. That's why in 2021 Google pledged to invest $10 billion to raise the global cybersecurity bar in partnership with governments, universities, and nonprofits.

Underpinning Google's approach to open security are thousands of the world's leading experts and practitioners. Immediately following Operation Aurora, we established teams such as the Threat Analysis Group (TAG), which monitors and blocks sophisticated threats, and Project Zero, which scours the Internet for undiscovered "0-day" vulnerabilities. In 2021 we created Google Cybersecurity Action Team (GCAT) to guide global businesses and governments along the path to secure digital transformation. And in 2022 we welcomed the addition of Mandiant, an industry leader in cyber threat reporting, incident response and cybersecurity advisory services to help us reinvent enterprise security.

Google is also investing in security and privacy protections for Europeans on Europe's terms. We listened to our users and to policymakers, and made it our priority to make Europe the home of our security engineering efforts worldwide. In 2019 we launched our first Google Safety Engineering Centre (GSEC) in Munich to co-locate hundreds of engineers and foster co-creation of Google security and privacy tools, such as Google Password Manager and Google Security Check-up. In 2023 we will unveil a European centre for cybersecurity and malware research in Málaga, to help businesses and governments better understand evolving cyber threats and protect their customers and citizens. Our centre in Málaga will be key to Google's local and regional cybersecurity partnerships for years to come. In addition, Google Cloud is partnering with European companies like T-Systems, Thales, and Indra-Minsait to offer trusted cloud solutions that meet our customers' digital sovereignty requirements.

Images from GSEC Munich

III. Recommendations for the EU

The scale of the cybersecurity challenge requires bold solutions and new public-private partnerships. Given these challenges, we recommend that the EU focuses on a few key issue areas.

3.1 Foster an ecosystem that promotes open security principles

The Internet was built on a foundation of multi-stakeholder governance, openness and interoperability, which created the conditions for one of the greatest expansions of opportunity and productivity in history. Disrupting this model would pose profound risks to businesses, institutions and ordinary users across the European ecosystem — not least to their security. A fragmented Internet is fundamentally less secure, because it makes it more prohibitively difficult to raise global security baselines through open standards and best practices. As one example, web browser companies like Google coordinated to drive up the global percentage of encrypted web traffic from less than 50% in 2014 to well over 90% today. This industry-led effort makes eavesdropping on users' web browsing far more challenging, an advancement in privacy that would have been next to impossible in a fragmented ecosystem.

The principles of openness and transparency support security in other ways, too. Well-managed open source projects benefit from greater engagement and auditing of codebases to find flaws. Transparent sharing of information about threats and vulnerabilities ensures that the largest possible audience can benefit. And open, interoperable systems enable organisations to rapidly adopt the best security practices and technologies, regardless of source. Open technologies foster greater innovation, lower barriers to entry, and are better for security because they enable more parties to work on shared security issues. There are four policy areas where the EU can help promote these values while enhancing security:

Open Internet principles: We encourage the EU and its Member States to embrace digital transformation built on open principles: trust, resilience, and solidarity in the face of threats to shared values, as an alternative to policies that would further fragment the Internet along national boundaries. We welcomed the announcement of the Transatlantic Data Protection Framework and the launch of the Declaration for the Future of the Internet, signed by 61 countries including many EU members, as critical steps in renewing trust. We stand ready to work with policymakers on both sides of the Atlantic to advance policies that protect users and their data, promote common standards, harmonise regulatory requirements, enhance interoperability and data portability, and prevent discrimination in digital trade.

Open mobile ecosystems: Consumers do not have to choose between open mobile ecosystems and security, and we think the security argument in favour of closed systems that lock out competitors is overblown. As the EU implements the Digital Markets Act, we encourage the EU to develop an approach that balances the need for security with the ability to give consumers choice in the marketplace. We would welcome an open exchange on this topic that is backed by data on real mobile security threats.

Open cloud: Cloud services should be designed to maximise the portability of data and applications between multiple cloud service providers and on-premises environments. This will help to maximise customer choice and minimise vendor lock-in concerns. We urge the EU to codify a preference for open, interoperable, hybrid, and multi-cloud arrangements in EU public procurement frameworks. We encourage the EU to examine proposed regulations that would impose barriers to market entry by foreign providers and to continue to shine a light on problematic licensing practices that limit European businesses' choice in cloud partners.

Open source security: The disclosure and response to the Log4Shell vulnerability underscored the need to better understand systemic dependencies on open source software, and develop new approaches to promote and advance security in the open source ecosystem. Google is a strong supporter of the open source software community and is making investments to raise the level of open source security globally.[1] We encourage the EU to partner with industry to identify the open source projects public and private sector organisations rely on most and invest in ecosystem-wide risk mitigations. We also encourage the Commission and EU bodies like ENISA to leverage public procurement guidelines to drive implementation of best practices in secure software development, the use of software integrity frameworks like SLSA, and the adoption of modern software tools and architectures.

3.2 Invest in digital transformation to enhance ecosystem-wide security and resilience

Recent attacks on Microsoft Exchange, SolarWinds, Kaseya, and others demonstrate that overreliance on outdated technology infrastructures and devices that are difficult to patch and maintain puts European organisations at greater risk of cyber espionage and extortion. The problem is particularly acute for small and mid-sized organisations that are often constrained from investing in the latest cybersecurity tools or competing for scarce talent in light of the uneven economic recovery.

With digital ecosystems increasingly interconnected and only as secure as their weakest link, there are few better ways to raise the security baseline of the common market than to incentivise technology modernisation through secure-by-default technologies and cloud services. Google strongly supports the Commission's Digital Decade target of reaching 75% adoption of modern cloud services, big data, and AI by 2030, and its use of the Recovery and Resilience Facility (RRF) as a springboard for new investments in digital transformation.

Partnering with cloud service providers like Google Cloud can enable European organisations to access superior vulnerability management, security tools, and expertise than most can achieve on their own. Google Cloud's defence-in-depth security model centres on custom-built microchips and hardware, encryption at-rest and in-transit, true zero trust architecture, and resilience delivered by more than 30 cloud regions worldwide. Google Cloud is also certified as compliant with dozens of European and international security standards and regulations.

[1] We've pledged $100 million to support the Open Source Security Foundation (OpenSSF) to develop collaborative solutions to open source security challenges. We launched a new team to speed security resources to high-priority projects and new tools to give our partners and customers access to the same secure open source tools and libraries our own engineers use to build secure applications.

Along with modern cloud services, adopting secure-by-default devices, operating systems, and email platforms can enhance Europe's resilience to threats like ransomware. Google's Chrome OS, which powers Chromebooks, is a cloud-first platform that provides protection against ransomware by default. There has never been a reported successful ransomware attack against a Chrome OS device.

The Google Cybersecurity Action Team (GCAT) is committed to working with European policymakers to share our experience and expertise in secure digital transformation. We stand ready to partner with European government bodies, enterprises, and organisations to leverage the NIS2 Directive, along with the RRF, as catalysts for technology modernisation and significant improvements in baseline security.

3.3 Engage industry and international partners to share intelligence and combat cybercrime

The recent surge in ransomware attacks against European organisations, and concerns about possible spillover from the cyber conflict between Russia and Ukraine, have underscored the need for closer threat intelligence sharing and joint incident response planning between governments and industry. To support this effort, Google is committed to sustaining and deepening its cyber threat information sharing partnerships with EU government bodies. We regularly publish threat intelligence resources through channels such as the Threat Analysis Group's blog, quarterly Threat Horizons reports from Google Cloud, and regular Malware Trends reports from VirusTotal. Google's VirusTotal platform enables security researchers and practitioners in Europe and around the world to share information and expertise on the malware ecosystem, free of charge.

> Google delivered over 50K government-backed attack warnings in 2021.
>
> Source: Threat Analysis Group.

We are excited to incorporate Mandiant, and its dynamic cyber defence, threat intelligence, and incident response services, into Google Cloud's core security offerings to EU governments. Mandiant's industry-leading team of security and intelligence professionals supports enterprises and governments in more than 80 countries worldwide. Together, Google Cloud and Mandiant will deliver a wide range of end-to-end security operations offerings with even greater capabilities to support EU customers across their cloud and on-premise environments.

Google will remain an active participant in public-private threat information exchanges and closed-door briefings with EU policymakers and technical experts. Our security teams will continue to partner closely with Computer Emergency Response Teams (CERT) throughout the EU to warn government bodies about threats we observe. We are also exploring ways to be more engaged in sector-specific forums such as the EU Cloud Information Sharing and Analysis Centre (ISAC) overseen by ENISA. We will continue to make our cybersecurity executives and our security teams available and accessible to brief EU bodies on cybersecurity threats, to provide testimony before EU rulemaking bodies, and to participate in joint preparedness exercises in partnership with bodies such as ENISA, CERT-EU, and the European Cybercrime Centre (EC3).

But information sharing alone is insufficient to combat modern threats. The EU should consider ways to enhance cooperation on the development of advanced technologies to disrupt threats. For example, Google is a leader in applying artificial intelligence (AI) to security. Embedding AI and machine learning into our products to keep users safe from ransomware and other threats by detecting and blocking 99.9% of all spam and phishing attempts. As the European Union pursues complementary goals of enhancing cybersecurity and making the EU a world-class hub for human-centric trustworthy AI, we would welcome greater dialogue to explore areas of cooperation and collaboration.

3.4 Protect high-risk groups from malicious cyber activity

We are concerned by a rise in digital repression, including attacks on important civil society actors – like human rights workers, electoral organisations, and journalists – on which an inclusive digital society depends. This trend is fueled in large part by the commercial surveillance industry, which enables the proliferation of dangerous hacking tools, arming those that would not be able to develop these capabilities in-house. Use of these tools is growing, fueled by demand from governments. Seven of the nine zero-day vulnerabilities our Threat Analysis Group (TAG) discovered in 2021 fall into this category: developed by commercial providers and sold to and used by government-backed actors. TAG is actively tracking more than 30 vendors with varying levels of sophistication and public exposure selling exploits or surveillance capabilities to government-backed actors. We have reported on users in several European nations who have been targeted by these capabilities.

While this challenge requires a global response, the EU can take a leading role in building norms around use of these tools and policy frameworks to control them. We applaud the European Parliament for taking on this pressing issue, and would encourage the EU to consider policy approaches to address harms from this industry. Urgent action needed to 1) implement transparency and disclosure mechanisms, 2) consider export controls for vendors located in the European Union to limit their spread to authoritarian regimes, and 3) implement an avenue of redress for people who have been victimised by these technologies.

In addition to our work shining a light on these threats, Google has made it a priority to build free cybersecurity tools to protect high-risk users and organisations. These tools have been critically helpful to users and organisations impacted by the War in Ukraine. For instance, in March Google expanded eligibility for Project Shield, a free protection against DDoS attacks, so that independent news sites, nongovernmental organisations, embassies and government

institutions in proximity to the conflict, including the Ukrainian government, could continue to offer their crucial services. Today, Project Shield protects hundreds of organisations worldwide, including 200 in Ukraine alone. Google's Advanced Protection Program (APP), which offers our highest form of account security, is protecting hundreds of high-risk users on the ground in Ukraine from surveillance and intimidation.[2]

We would welcome the opportunity to partner with EU institutions and other relevant organisations to provide security awareness training and offer free security resources to Members of the EU Parliament and their campaigns ahead of the 2024 European elections, just as we have done for the 2021 German election and the 2022 French election.

3.5 Develop a "security impact assessment" for new regulations

We applaud the Commission's draft Declaration on Digital Rights and Principles, which seeks to codify a right to safety and security for all EU citizens. We would like this norm to be protected and, in fact, written into law. At Google, every product and service needs to undergo rigorous threat modelling from the design phase onward. We would like to advocate a similar mindset in public policy that takes security into account at every step in the legislative or regulatory process in order to guarantee digital security for all.

European leaders should consider adopting a "security impact assessment" mechanism for all new tech regulations in the EU. Just as the EU performs an assessment of the economic, social, and environmental impacts of new initiatives, the same level of diligence should be performed to ensure new policies do not undermine European citizens' security and privacy.

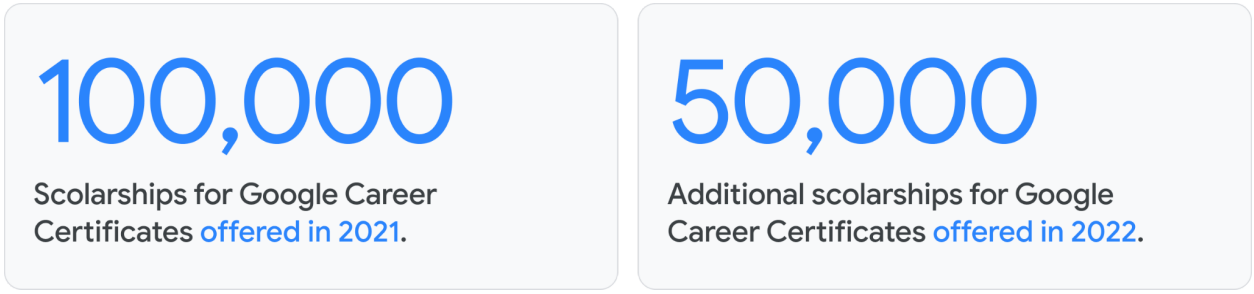
3.6 Partner with industry to expand access to security education and training resources

As the latest ENISA report on the cyber workforce makes clear, the European Union is facing a critical lack of resources to address the scale of the cybersecurity challenge. The digitisation of Europe, combined with the growing understanding of the need to invest in security, have led to a demand for skilled cyber practitioners that far outpaces supply. According to the latest Digital Economy and Social Index data, 55% of enterprises find it challenging to fill ICT roles. A

[2] To date, we have not observed a single APP user be successfully compromised via phishing since the inception of the programme.

better use of secure digital infrastructure and automation coupled with cyber skills can provide a robust response to increasing cyber attacks. We encourage the EU institutions to continue to invest in cybersecurity-focused digital skills.

Digital skilling initiatives are at the forefront of Google's commitment to invest $10 billion over five years to strengthen global cybersecurity. In collaboration with the EU's Pact for Skills, in 2021 we announced our goal of providing 100,000 scholarships for Google Career Certificates in IT and data analytics for job seekers in Europe, the Middle East, and North Africa. In 2022 we're offering an additional 50,000 scholarships in EMEA. This year Google partnered with Spanish organisations including BBVA, CEPYME, and INCIBE to offer free security training for hundreds of Spanish small and mid-sized businesses. We'd like to explore opportunities to partner with ENISA and other EU organisations to expand training for small businesses and offer specialised cloud computing and cloud security training to expand access to critical skill sets and improve cyber resilience.



3.7 Prioritise strong encryption over data location

In recent years, European Member States have advanced numerous proposals that seek to achieve data protection through the localisation of data within set geographical boundaries. Even when well-intentioned, data localisation policies can curtail the economic benefits of cross-border collaboration and innovation, while raising processing and storage costs for EU businesses and organisations. They also fail to recognize how the ability to transfer data across borders can actually support policy objectives in the protection of privacy, security, and regulatory compliance. For example, in the financial services industry, the ability to transfer and analyse data in real-time across borders is necessary to combat financial fraud, money laundering, or other illicit financial transactions. Security operations tools that monitor traffic patterns, identify anomalies, and divert potential threats depend on global access to real-time data.

Data localisation requirements can also undermine security and resilience by preventing European organisations from scaling resources to combat DDoS attacks or failing over their data to more secure locations when threatened by a natural disaster or armed conflict. For example, the Ukrainian government reversed previous policies requiring data localisation when the Russian invasion threatened its physical data infrastructure – instead seeking other mechanisms to advance resilience, including use of cloud capabilities for data storage.

Strong encryption and customer control of encryption keys are superior means of protecting sensitive data than are requirements mandating where data is physically located. Customer-managed encryption tools, pioneered by Google Cloud, give European organisations unprecedented control over their data – including the ability to block cloud providers from decrypting their data for any reason – without sacrificing the universal availability and resilience that global infrastructure affords. We encourage the EU to promote data protection through strong encryption rather than data localisation, and invite the EU to learn more about Google's implementation of encryption tools.

IV. Conclusion

Confronted by shared digital security challenges, Google is committed to partnering with the EU, ENISA, and other EU bodies to raise the security bar for all European businesses, organisations, and Internet users. We stand ready to support the secure digital transformation of thousands of European businesses, to defend European businesses and Internet users from ransomware and commercial surveillance, to partner with European authorities to combat sophisticated threats, to equip the next generation of cybersecurity professionals with the training they need to make an impact in their field, and to work with policymakers to implement policies that put user protections first and promote security-conscious behaviours by businesses and users.

APPENDIX - Key Regulatory Files

A.1 Cyber Resilience Act (CRA)

We support the EU's intention to drive improved security in the product ecosystem. We encourage the EU to aim for maximum global harmonisation on security standards for devices and services, which will ensure compliance is manageable for small manufacturers. Google is a leader in producing secure-by-default software and hardware, and we would welcome the opportunity to partner with the Commission to share our expertise and help build consensus for a common sense approach.

A.2 EU Cloud Services Scheme (EUCS)

Google supports the EU's efforts to create a security labelling scheme for cloud services and its efforts to harmonise regulations across the common market. We also support France's efforts to implement its SecNum Cloud certification, which contains strict sovereignty provisions that respond to its unique domestic context. We are concerned, however, that efforts to implement corresponding sovereignty provisions – such as an EU headquarters requirement and strict data localisation measures – on an EU-wide basis through the EUCS "High" level certification will: 1) create trade-offs for effective cybersecurity by removing capabilities to analyse threat trends on a global basis and maximise data infrastructure resilience; 2. limit choice of cloud provider for European businesses and organisations or create disincentives for those organisations to attain state of the art cybersecurity; and 3) further delay adoption of innovative cloud capabilities by European public sector agencies and regulated industries. A pan-European, cross-sector scheme such as EUCS should reflect the broadest possible consensus and include only those measures that align with the technology and procurement needs of all Member States.

A.3 NIS2 Directive

Google supports the revised NIS2 Directive, which will contribute to European cyber resilience. One area of concern that has received relatively little attention is the oversight challenge NIS2 poses for national cybersecurity regulatory agencies. In some cases, NIS2 will multiply the number of entities an agency must oversee and protect by 10x or more without comparable increases in funding or headcount. Growing resource gaps may challenge governments' ability to prepare for or respond to cyber incidents. They may also force agencies to triage resources in favour of the largest or most critical entities, and away from small and mid-sized entities who need assistance most.

A.4 eIDAS

We endorse the EU's objective to encourage electronic identification, authentication and website certification throughout the EU. These are necessary components of modern digital societies. In order to gain users' trust, the eID proposal (eIDAS) must ensure the highest level of security. In this context, we'd like to point out that technical experts, including Internet pioneers like Vint Cerf, have continually raised concerns about Article 45 of the proposal . As written, eIDAS would circumvent established browser policies and security protocols that have been working for many years to protect people browsing across websites. This is a prime example of digital sovereignty objectives being in conflict with multi-stakeholder governance

for security protocols that keep EU citizens safe online. Efforts to subvert browser authentication policies have been attempted by authoritarian regimes to spy on their citizens' web browsing. The EU's actions here could unintentionally fuel this global trend, which would make European citizens less safe online. Google stands ready to share its technical expertise on how to best provide the highest level of security in the context of eIDAS. We look forward to engaging with the EU on this point.