ECIS European Committee for Interoperable Systems

ECIS White Paper

1 October 2019

The importance of openness and interoperability in cybersecurity and cloud services

1. Introduction

The European Committee for Interoperable Systems ("**ECIS**") is an international, non-profit association of information technology companies founded in 1989 which endeavours to promote a favourable environment for interoperable ICT solutions. For three decades ECIS has actively represented its members on issues relating to interoperability and competition before European, international and national fora, including the EU institutions and WIPO (*e.g.*, the Microsoft case). ECIS' members include both large and small information and communications technology hardware and software providers, including IBM, McAfee, Opera, Oracle, and Red Hat.

One of the flagship initiatives of the Europe 2020 strategy has been to give a prominent role to improved standard-setting in the ICT sector to ensure interoperability between ICT applications, services and products with a view to combating lock-in and reducing fragmentation of the digital single market while simultaneously promoting innovation and competition. ECIS plays an important role in advising European authorities on such matters relating to the implementation of standardisation policy in the ICT field.

Since its inception, ECIS has been a champion not only of the open source model, but also of interoperability, beginning with its involvement in helping to formulate the interoperability provisions of the 1991 Software Directive[1]. More recently, ECIS activities have been focused on interoperability for cloud and cybersecurity products and services.

As a pioneer in relation to the subjects of openness and interoperability, ECIS members believe they are well-placed to: (i) provide constructive input on issues arising in the context of EU initiatives on openness and interoperability (such as cybersecurity and cloud services) during this upcoming five-year EU mandate; and (ii) share and present this white paper to industry to spur constructive discussion with all stakeholders on the issues discussed herein.

The concepts of openness and interoperability in the context of cybersecurity and cloud services are nuanced and require careful consideration when applying them in public policy. Nevertheless, the growth of cloud and cybersecurity deployment places mounting pressure on vendors to offer superior levels of interoperability. ECIS members maintain that openness and interoperability between and amongst IT systems architectures - based on a strong model of collaboration between partners - is at the heart of best-in-class, pro-competitive multi-cloud and cybersecurity products and services. Such collaboration unlocks both digital transformation and emerging technologies. Indeed, programming languages on the world wide web to connect, say, a web browser to a web page would be impossible without open standards defining

[1] 91/250/EEC repealed by 2009/24/EC

interoperability. Interoperability is a cornerstone of the ICT industry and has been defined as "the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged."[2]

The ability of individuals and businesses to move data or applications from one platform to another goes to the heart of the objectives of ECIS, which has long been advocating interoperability based on open standards and open interfaces to avoid lock-in and promote competition on the merits. In today's networked ICT environments, devices do not function purely on their own, but must interact with other software and devices. A device that cannot interoperate with the other products with which consumers expect it to interoperate is of limited value. It is interoperability that drives competition on the merits, based on innovation and investment. Therefore, *any* restriction or limitation on the free flow of data due to an absence of interoperability will stifle innovation, limit the value of the products and services in question, and ultimately strangle the full potential of Europe's digital single market.

The ability of different cybersecurity and cloud services to interoperate empowers consumers and organisations to choose from amongst them. It is precisely for this reason that interoperable products must compete with one another, and it is this competition that has driven innovation in the software industry. This approach is currently the most effective to ensure that customers are not 'locked in' to proprietary technologies that do not work with one another or do not allow for change and adaptation as markets and technologies evolve.

It is worth noting the interesting shift which has emerged over the past few years; that is, the movement of developers from a proprietary to an open-source model. The adoption of open-source software has accelerated in recent times[3], across companies of all sizes and all industry verticals, and is used in the delivery of cloud services by the majority of cloud providers. This is likely to be the result of businesses moving to more agile operations and therefore becoming more comfortable with open-source technologies and practices.

As discussed below, it is clear that interoperability is crucial in realising the full value of cloud computing. Having a standardised definition for the mechanisms that are used for independent systems to exchange data has enabled numerous technologies to thrive. Although there are already countless standards defined for specific technologies used in cloud offerings, leading standards organisations and consortia/fora are taking steps to better define standards across multiple cloud services enterprises in areas such as security, management and status monitoring, so that interoperability can help cloud solutions evolve and reach their full potential.

In relation to cybersecurity, a lack of interoperability and cyber intelligence-sharing across information systems can have serious consequences, including, for example, the limitation of response capability against cyber (or even larger scale) terrorist attacks. Interoperability is therefore critical for successful threat intelligence in any organisation as it allows for: (i) the sharing and receiving of cyber-threat intelligence within, and also beyond, the company's boundaries; (ii) the rapid detection of, and preparedness of cybersecurity experts to, respond to

[2] ISO/IEC17788:2014, 3.1.5.

[3] More enterprise open-source software and less proprietary software within next 24 months, according to Red Hat's 2019 report: https://www.redhat.com/en/enterprise-open-source-report/2019

imminent attacks; and (iii) the potential for a range of capabilities through specific frameworks (such as STIX™ discussed below) to collaborate on threat analysis, and automate threat exchange, detection and response. Interoperability enables cybersecurity communities to communicate using a common language which, in turn, aids in a better understanding of cyber-attacks.

This white paper explores how such interoperability has clear benefits for enterprise, consumer and government markets as they deploy cloud services and cybersecurity solutions and seek to protect against existing and prospective threats.

As industry moves towards enhanced interoperability in this space, cloud deployment and cyber resilience become more efficient and cost-effective. Over time, such interoperable architectures are easier to maintain than IT environments built of disparate parts, and as their use and application becomes more widespread, they will contribute to closing the skills gap as these systems will require less manual intervention.

In the cybersecurity environment, early adopters of new cybersecurity solutions see immediate benefits from their investments, but as more organisations deploy the new products, cybercriminals have greater incentives to develop countermeasures. In reality, cyber-defence capabilities become less effective over time as attackers develop countermeasures to evade or neutralise them, so organisations benefit most by adopting and deploying cybersecurity solutions as early as possible.[4]

In such an environment, organisations that utilise open and interoperable cybersecurity solutions and architectures are able to incorporate new innovative solutions and integrate them into their IT environments more rapidly with the benefits that come with early adoption. In this year of European Parliament elections and the renewal of the EU College of Commissioners, ECIS's mission is entirely consistent with:

- the objectives expressed by the Heads of State and Heads of Government at the Tallinn Digital Summit in September 2017, when they called for the Union to become: "*a global leader in cybersecurity by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free, safer and law-governed internet";*
- the Tallinn eGovernment declaration pledged governments to: *"make more use of open source solutions and/or open standards when (re)building ICT systems and solutions (among other things, to avoid vendor lock-ins), including those developed and/or promoted by EU programmes for interoperability and standardisation";* and
- the EU's digital strategy (November 2018) provided yet more direction for governments to increase the adoption of open-source by stating *"Open-source solutions will be preferred when equivalent in functionalities, total cost and cybersecurity."*

[4] *See*: https://www.mcafee.com/enterprise/en-us/assets/fact-sheets/fs-maximizing-threat-defense-effectiveness.pdf

2. ECIS' perspective

Interoperability of cloud and cybersecurity services is achieved through a variety of ways by ECIS members[5]. What they have in common is a belief in designing technology to an open standard, on an open platform and with published and publicly available interfaces accessible by customers in order to reduce the risk of vendor lock-in. We observe these features in several solutions being deployed.

A) Enabling the sharing of cybersecurity data, including threat intelligence and insights into observed threats

Security is awash with complexity. Sophisticated attacks are increasing, and for many years too many cybersecurity products have operated in isolation, all against a background of scarcity in human resources to address these challenges. Improving cyber-defence capabilities using cutting-edge threat intelligence is therefore a priority for every public and private sector organisation.

Sharing cybersecurity data leads to several outcomes: (i) improving detection and investigations in security operations, (ii) improving endpoint or network protection (with KPIs), or (iii) measuring an organisation's capability to defend against and deter fast-evolving hostile techniques.

Sharing cybersecurity data with other organisations for security purposes - including other service providers, information sharing and analysis organisations from the public and private sectors, and computer emergency response teams - can help those organisations mitigate vulnerabilities that compromise the confidentiality of personal information, avoid exposures that can lead to accidental breach of personal information, and help prepare for suspected or known malicious actors.

When embarking upon a programme to share cybersecurity data, an open standards-based approach needs to be strongly considered for several reasons, including enabling robust ecosystems, avoiding vendor lock-in, and ensuring that interoperability is assured for the long term.

Thankfully, a number of international standards have recently been created within the industry to enable collaboration and the sharing of cybersecurity data more efficiently. These standards are currently at various stages of industry adoption; however, all are gaining significant momentum in the space, and many ECIS members are involved in their development.

B) Current international open standards

- **STIX™ / TAXII™** – STIX™ 2 (Structured Threat Intelligence Expression) and TAXII™ 2 (Trusted Automated eXchange of Intelligence Information) are JSON-based industry standards for sharing cyber-threat intelligence information between and amongst governments, threat intelligence vendors, ISAOs, cybersecurity product developers, enterprises, and end-

[5] *See*: http://www.ecis.eu/library/

users. STIX™ 2 and TAXII™ 2 are developed by the OASIS Cyber Threat Intelligence Technical Committee.[6]

- **OpenC2** – Open Command and Control is a concise and extensible language to enable machine-to-machine communications for purposes of command and control of cyber-defence components, subsystems and/or systems in a manner that is agnostic of the underlying products, technologies, transport mechanisms or other aspects of the implementation. OpenC2 is developed by the OASIS OpenC2 Technical Committee.[7]
- **CACAO** - Collaborative Automated Course of Action Operations (CACAO) is an effort to create a standardised language and associated protocols to capture and automate a collection of coordinated cybersecurity actions and responses, called a Course of Action (COA) Project. CACAO is a newly proposed working group within the IETF.

C) Standards emerging from open-source communities

A number of ECIS members are making considerable strides in the area of sharing and collaborating on cybersecurity data.

One example, is that of the Open DXL project developed by McAfee, which encourages vendors to break down the walls that separate its cybersecurity products.[8]

Open DXL enables security devices to share both threat intelligence and orchestrate security operations quickly and securely. A growing number of security companies are actively connecting and sharing threat intelligence feeds using the DXL ecosystem. This approach also brings to life ECIS members' commitment to working collaboratively and in public and private partnerships to build tools that are robust enough to deter and ultimately defeat cyber-attackers.

The philosophy is to make the threat intelligence communications messaging framework available to all, so that the community of cyber companies can develop a rich set of competing products. The approach is also supported by over 130 Security Innovation Alliance (SIA) partners supporting implementation and adoption of a common messaging language, including other ECIS members.

An open and interoperable exchange of threat intelligence data meets EU objectives of securing data privacy, enhancing resiliency, improving digital trade and data flows, and enhancing European cloud adoption. Equally, open architectures of this type enable both cooperation and competition between cybersecurity vendors as they help them integrate and interoperate, and can help advance the development of smaller cybersecurity enterprises.

[6] *See*: https://oasis-open.github.io/cti-documentation/

[7] *See*: https://openc2.org/

[8] *See*: https://www.mcafee.com/enterprise/en-us/assets/faqs/faq-data-exchange-layer.pdf

D) Enabling Interoperability

Having so many products in the cybersecurity and cloud security marketplace is driving complexity and forcing organisations to focus disproportionately on infrastructure maintenance rather than designing and implementing security outcomes. In such an environment, there is a greater risk of false positives as overall visibility of the threat landscape is compromised, resulting in breaches to the endpoint and cloud environment.

In this context, interoperable threat management platforms are key to ensuring a properly integrated and comprehensive approach to cyber risk management, data security, and data privacy needs. ECIS members are active in this area, with different methods and tools which promote interoperability. Examples of this include (i) orchestration platforms that provide a single pane of glass for the user of multiple third-party solutions, (ii) cloud platforms that federate security data, which allow for rich cross-platform cybersecurity analytics use cases, and (iii) threat intelligence analytics tools that provide for more rapid response.

E) Enabling digital transformation

Organisations are transforming through technology faster than ever, whether by adopting the cloud, enabling employees to use their own devices, driving the use of IoT to transform the way they engage with customers, partners and/or employees, or all of these. Hence, we are seeing a geometric increase in the number of cloud services that are available as SMEs, enterprises, and governments invest in a multitude of cloud environments that enable greater collaboration - allowing teams to communicate in real time, efficiently share information, collaborate on documents and access information. **This explosion in complexity means that organisations bear greater risk than ever as these technologies have expanded the attack surface.** Increasingly, sophisticated adversaries are targeting European government and enterprise cloud infrastructure, seeking to 'weaponise' cloud services and take over their functioning with malicious intent.

ECIS members are addressing this new threat by **building security into products, services, and supply chains, together with providing security solutions**, while governments play a key role in advancing cybersecurity best practices. Above all, government and enterprise digital transformation must be underpinned by confidence that data loss prevention, threat protection and active perimeter monitoring are all in place and have best-in-class resilience.

A second way in which ECIS members are addressing these digital transformation risks is via the **promotion of open cloud security architectures.** Open and interoperable cloud security architectures provide quick and comprehensive means to achieving higher security standards in governments and enterprises, enhancing the pace of digitalisation and increasing competitiveness as the market responds to open standards. ECIS members strongly advocate an open and interoperable approach that allows customers to integrate cloud SAAS services without building a bespoke integration or writing code. Such an approach is enabled **by providing open API for cloud security services**, so that any service provider or partner can build API connectors to secure any cloud services and enforce the same set of security policies across all cloud services. This open approach - in which APIs are published - drives interoperability across the many cloud services available on the market today and allows new cloud services to be adopted securely; thereby reducing the costs of product integration and increasing operational efficiency, whilst reducing the risk of data privacy violations.

3. Enhancing openness and interoperability - Recommendations for EU cybersecurity and cloud policy

ECIS believes that the development of **open and interoperable architectures and solutions should have greater prominence in European Union cybersecurity and cloud policy**, so that governments and enterprises can interact and work together across borders to manage global threats without friction.

An interoperable approach brings benefits to companies that deploy cybersecurity and cloud security solutions, and can help ensure that they do not need to make multiple products for varying requirements in each market, or build to country-specific standards. Interoperability can also benefit government and enterprises in that they benefit from a secure digital infrastructure.

To achieve enhanced openness and interoperability, ECIS would encourage the European Commission, Cybersecurity Agency (formerly ENISA), CERTs and national cybersecurity authorities to use the following baseline principles:

- Ensure implementation of the European legislation to date (*e.g.,* the NIS directive and the EU Cybersecurity Act) building on the model of a multi-stakeholder, public-private partnership approach to cybersecurity standards and policies, a process that is open, participatory, risk-based and transparent. This would provide all stakeholders with a meaningful opportunity to review drafts, offer comments, and understand how competing viewpoints are factored into the resulting document. Cybersecurity is a shared responsibility – neither governments nor companies can address it alone;
- Europe's future cybersecurity framework policies should use widely adopted, industry-led practices and standards that are developed in open, voluntary, consensus-based processes such as the ISO/IEC 27000 family of information security management systems standards and other tools. These provide a common language to better help organisations comprehend, communicate and manage cybersecurity risks (such as the U.S. NIST Cybersecurity Framework);
- Wherever practicable, European cybersecurity standardisation efforts to promote interoperability should be based on restriction-free intellectual property (consistent with unencumbered open standards driving the internet/software world). These would be voluntary and incentivised by market forces to ensure flexibility so as to adapt responses to a dynamic threat environment; and
- Where regulators are developing mandatory requirements to protect critical systems under the EU's NIS directive, ECIS would encourage their development using process-oriented, standards-based mechanisms for cyber risk-management[9].

[9] *See*: https://www.cybersecuritycoalition.org/cybernextdc2017-whitepaper

This approach to policy will improve effective implementation as governments, enterprises and cloud and security vendors are encouraged to work collaboratively, which will, in turn, lead to greater adoption and better outcomes not generally achieved by a top-down regulatory approach.

In closing, we encourage the European Commission, Cybersecurity Agency (formerly ENISA), CERTs, and CSIRTs to work together in partnership with ECIS members to make the vision of a truly open and interoperable cybersecurity and cloud ecosystem become a reality. Such an ecosystem - based on open international standards – would harness the benefits of competition and innovation whilst ensuring that innovative solutions work effectively together through a system based on collaboration. We remain at your disposition should further information be required, or a follow-up engagement arranged, to further discuss the details and importance of this matter during the next five-year EU mandate.