The European Cyber Security Organisation (ECSO), and in particular its Users Committee (UC), would like to better understand the operational needs of users/operators, the role of CISO’s, and the operational / strategic / business priorities of organisations when it comes to cybersecurity.

In collecting and analysing responses to the survey, it is the aim of ECSO to develop a short study able to inform CISO's/Boards, industry, and (national and European) policy makers on these important matters in order to, ultimately, enhance the cybersecurity of organisations (incl. their ability to respond to threats) and drive needed cybersecurity policies, regulations and use of resources for businesses and critical sectors.

To reach this goal, we will canvass CISO’s or equivalent, i.e. C-level experts working close to CISOs or in cybersecurity responsibility positions, through a holistic survey that will be shared across the Community (starting from ECSO's UC and broader membership), complemented with telephonic interviews or video meetings.
General / The work of a CISO

1 What is your job title?

2 Which sector do you represent (energy, finance, transport, healthcare, manufacturing, etc.)?

3 Do you have any cybersecurity certifications (i.e. CISSP, CISM, Security+, ISO 27001)? If so, which ones?

4 Does your organisation have a dedicated CISO position?
   If yes, mark N/A and skip to next question.
   If no, who is responsible for cybersecurity in your organisation?

5 In your opinion, what are the top 5 cybersecurity threats your organisation is facing?

6 What are the main challenges you face in implementing cybersecurity in/across your organisation?

7 Do you feel you have enough authority / Board level support to enforce cybersecurity policies within your organisation?

8 A CISO’s working lifecycle is said to revolve around Identify/Protect/Detect/Respond/Recover. Would you agree and how would you rank those in order of importance?

Board investment / Business continuity
1 Cybersecurity, beyond the technical challenges, brings up business-related and financial challenges (e.g. the costs of modernising the infrastructure). To what extent is cybersecurity considered crucial for business continuity in your organisation?

2 While executives may say cybersecurity is a priority, they need to follow through with strategic investments. In your opinion, what are the main reasons that Boards do not invest sufficiently in cybersecurity?

3 Executive Board perceptions can restrict cybersecurity effectiveness. If CISOs want to expand their influence and align cybersecurity with business priorities, they must “manage up” to Executive Boards and “manage across” to all employees.
To which extent do you agree with this statement? And how should such a business process be implemented?

4 When it comes to business continuity, we talk a lot about corporate social responsibility, business risk management strategy, insurance, protection of assets, etc. What do you think are the main disruptive aspects and financial impacts of cyberattacks on companies and Operators of Essential Services (OES)?

**Information sharing – Threat intelligence – Crisis management**

1 Geopolitics play a major role on security but policy developments in cybersecurity often happen behind closed doors, thus hiding the depth of security and the types of threats that need to be faced. How can we better share information and threats across sectors and countries? And how do we make such solutions visible to CISO’s in Europe?

2 Information sharing platforms such as MISP typically only share TLP amber or TLP green information at a technical level (e.g. IP addresses, file names, hashes, etc.). In your opinion, how can we better facilitate the sharing of information that is relevant for CISO’s (i.e. strategic, geopolitical, new hacking techniques)?

3 To what extent would you consider collaboration with law enforcement (local/national/Europol) useful for addressing the more pervasive and crime-relevant issues facing organisations? Do you know of any best practice cases of collaboration between CISO’s and law enforcement?
4 Does your organisation use cyber ranges or technical exercises to conduct simulated attacks or crises responses? Is the CISO involved in these activities?

Certification

1 How involved are you with certification in your organisation? In your opinion, what more needs to be done on this front?

2 Certification often needs to be balanced with agility. What is the most effective way to strike this balance?

3 Do you think that it would be useful to have a mandatory Code in place, i.e. to ensure cybersecurity posture and Corporate Social Responsibility in organisations (example of Canadian approach), and are penalties an effective way of ensuring that organisations implement such measures and apply remedies where needed?

Authentication

1 When it comes to authentication, a holistic approach is needed including the authentication of users, services, IoT, instances, computers, people, M2M (critical), and processes inside machines. The management of this process and the identification across services is also very important. Do you agree and how do you manage this inside your organisation?

Liability & Governance

1 It is often said that there is an absence of dialogue and trust between CISOs and their Boards. Even if legal liability is made compulsory for CISOs, Boards in most cases are not aware of it nor do they understand cybersecurity and its problems. As such, CISOs usually communicate their decisions to Boards without a discussion or dialogue to make them understand the why’s. What do you think could be put in place to better frame that way in which you report to your Board about risks (financial, digital, cybersecurity, etc.)?
A good governance structure is also needed for the evaluation of the risks and of the budget. GDPR brings the awareness to the Board, NIS makes reporting compulsory, but nothing is done for governance. There is no method of approval of a governance.

In general, a good governance structure has 3 pillars:

- Bring profits
- Optimise (not eliminate) the risks
- Optimise/manage the resources

A majority of companies put a lot of money, effort and energy into optimising/managing resources, some of them also tackle bring in profits, but in general, very few companies focus on optimising the risk. Many Boards think that by doing what CISOs tell them, they’re immune to any risk.

How do you think this governance issue could be best handled?

**European, Regulatory & Cross-sector aspects**

1. To what extent do you rely on the regulatory aspects and actions done at the European level for the protection of critical infrastructure and the implementation of the NIS Directive? What more can be done / what should be improved in your opinion?

2. In order to improve operational resilience, cross-border and cross-sector aspects need to be further optimised. How to fight cross-border and cross-sector fragmentation? What lessons can be learned from the more mature sectors in this area?

3. What are your criteria of choice for the procurement and use of cybersecurity solutions and services? (e.g. performance, costs, made in Europe, other)

4. How much is important for you to rely on certified or validated European solutions (c.f. sovereignty and autonomy issues) for a trusted management of your sensitive data?

**Additional Comments or Remarks**

1. Do not hesitate to let us know any other insights you might have: