ECS

EUROPEAN CYBER SECURITY ORGANISATION

SEPTEMBER EDITION
AWARENESS CALENDAR

Organisational resilience

Awareness Calendar CYBERSECURITY

This calendar will feature a different topic each month to spread awareness of key aspects of cybersecurity and showcase ECSO Members’ and Partners' solutions and services in the relevant areas to potential users.

The monthly themes for 2022 are planned as follows:

- January – Cybersecurity certification
- February – Internet of Things
- March – Gender diversity in cyber
- April – Artificial Intelligence
- May – Cyber ranges & range-enabled services
- June – Cybersecurity for verticals
- July – Social engineering
- August – Privacy & data security
- September – Organisational resilience
- October – Cyber hygiene & readiness
- November – Cloud computing
- December – Threat & vulnerability management

DID YOU KNOW?

- Information and communication technology (ICT) products and services create opportunities for EU economies and societies. However, when everything is connected, a cybersecurity incident can affect an entire system, disrupting economic and social activities. This is why the European Commission presented the EU Cyber Resilience Act on the 15 September 2022, introducing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products and ancillary services. Find all you need to know here and how it will work in practice here.

- In addition, Cyber ranges can also be used to test and improve an organisation's resilience. Overall, cyber resilience applies to any process, system, business and organisation where there is a reliance on IT, OT, IoT which pretty much covers the majority of organisations in a nation, including critical infrastructures. In the context of cyber resilience, cyber exercises provide opportunities for organisations to demonstrate critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their critical information, services, and assets. More information can be found in ECSO's paper Understanding Cyber Ranges: From Hype to Reality.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

RESOURCES FROM OUR MEMBERS

(ISC)² offerings for organisational resilience in cybersecurity

(ISC)² offers a number of webinars and professional development courses related to resilience in cybersecurity.

Supply Chain Security: Planes, Trains, Trucks and Ships Webinar is available for purchase. In this webinar, leading cybersecurity experts explore solutions that answer the most critical challenges facing your regional market. Earn 1.5 CPE Credits for each webinar you attend.

Building Cyber Resilience in a Cloudy World. To cope with the changing business models such as remote working, organisations moved to the cloud much faster than anticipated. The paradigms are countless.

Incident Management: Preparation and Response. Learn how to determine that an event has become an incident, quickly and effectively respond to eliminate the immediate threat. Develop strategies and solutions to ensure similar incidents don’t plague your organisation in the future. Free for members and available for purchase for non-members. Earn 5 CPE Credits.

economie

FPS Economy, S.M.E.s, Self-employed and Energy

CENTRE FOR CYBER SECURITY BELGIUM

supports the organisational resilience of SMEs

The Belgian Federal Public Service (FPS) Economy has launched a call for projects concerning the strengthening of the organisational resilience of Belgian SMEs. The selected projects should raise awareness and encourage SMEs to act regarding the importance of having a clear view of their cybersecurity situation and their capabilities to prevent and react to cyber-incidents as an organisation.

Through this call for projects, SMEs should be able to:

- create and maintain a complete inventory of their IT assets and valuable information.
- be aware of the value of the data which they have and the potential risks that are linked to it.
- have all the basic procedures necessary for proper protection.

Four other calls are also made to increase technical measures, training and access to skills, professional support as well as specific projects for local traders and women entrepreneurs. Project leaders should submit their project proposal by the 31st October 2022. READ MORE.

Protection and prevention

CYBER SECURITY
AGENCY OF
CATALONIA

The Agency performs its protection function for the Government of Catalonia mainly by providing cyberthreat detection and mitigation services.

Prevention is essential to ensuring the sustainability of a protection model against threats and cyberattacks based on maturity rather than on reaction as the sole response mechanism. In this respect, the Cybersecurity Agency of Catalonia performs a preventive function in many areas, such as secure design in the development of solutions and services for the Government of Catalonia; assessment of the level of cybersecurity of the Government of Catalonia's ICT providers; digital identity management, and cyberthreat risk analysis.

Resilience in the context of cybersecurity refers to the ability of assets to withstand and recover from disasters or service failures. For this reason, the Cybersecurity Agency of Catalonia devotes part of its efforts and capabilities to determining resilience levels in contingency situations caused by cyberattacks. It does so by carrying out disaster recovery simulations and tests, as well as by writing up contingency and operational plans for situations.

READ MORE.

Cybersecurity: resilience must be designed

Cybersecurity, on a global level, is experiencing one of the moments of greatest interest, both because technological progress is constantly increasing and because the level of risk is high. Cyber-resilience is the ability of an organisation to better manage its business during a data breach or cyber-attack, in order to ensure the availability of the entire ICT system.
The question to ask is: Do cybersecurity teams have recovery plans in place in the event of a breach, but can critical business processes be kept active during a hacker attack?
Currently, the lack of specific technical skills constitutes the main obstacle to face cybersecurity, so that organisational efforts must be aimed at implementing effective and efficient Business Continuity, Risk Management and Disaster Recovery plans. The ability to resist an attack is a prerogative that can guarantee the survival of an organisation; in this Exprivia Cybersecurity offers various services: READ MORE.

JYVSECTEC by jamk

jamk | University of Applied Sciences

Cyber arena based cyber exercises as a tool for improving organisational resilience

Cyber arenas are beyond cyber ranges. Cyber arenas are safe, highly realistic, complex, large-scale training and learning environments, which include several domain and business specific cyber-physical systems. Businesses and organisations can safely and cost effectively evaluate and reflect their business continuity plans and improve their organisational resilience through cyber exercises based on the cyber arena. For businesses and organisations of various maturity levels cyber arenas offer several kinds of cybersecurity exercises and trainings. For instance, in productised exercises with a baseline that shows evidence of an occurred cyber-attack, supported by a technical coach, an organisation can track traces of cybersecurity incident from the technical controls and follow the organisation's playbook for responding to incidents. In tailored live-fire exercises, a simulated threat actor (red team) performs realistic tactics, techniques, and procedures (TTP) against the organisation. From the organisation's perspective, the threat actor aims to undermine the organisation's business and brands. READ MORE.

LEONARDO

Leonardo cyber resilience for your organisation

Leonardo supports customers in anticipating, countering and containing critical situations arising from physical or virtual threats such as cyber-attacks, natural disasters and physical security breaches. Our Cyber Security & Resilience and Secure Digitalisation offering portfolio guarantee adequate cyber security and resilience measures through services and platforms that can be natively integrated and tailored to the specific needs of each customer.

- Cyber Resilience & Consulting (Security Strategy & Governance, Risk Assessment & Management, Crisis Management, Cyber Resilient Architecture Design & Build)
- Cyber & Security Academy
- Cyber Security Assessment Laboratory (Compliance and Common Criteria Certifications)
- Managed Security Services (Real Time Security Monitoring, Cyber Threat Intelligence, Vulnerability Assessment, Penetration Testing, Incident Response)
- Business Continuity & Disaster Recovery Services
- Cyber Platforms (Cyber Trainer, Cyber Range, Cyber Information Superiority, Cyber Situational Awareness System)

READ MORE: Cyber Game Award Ceremony, Leonardo launches Cyber Information Superiority

Cyber resilience as a responsibility and when to invest in red teaming

Smaller organisations often do not consider themselves worthy of an attack or feel they cannot afford to equip themselves with the correct level of security. They should analyse, however, whether a successful attack on them can lead to breaches of their partners and customers. As WithSecure argues here, organisations should consider cyber resilience their responsibility and a crucial element of trust in collaboration. At the same time, investments in cybersecurity require careful analysis and planning. While red team engagements seem to be growing in popularity, WithSecure discusses here when those can be an effective and efficient choice and when other activities should be considered first.

RESOURCES FROM THE COMMUNITY

Cyber resilience: things to know

HWG

A Cyber Security Company

Over the past year and a half (that of the pandemic), the word resilience - the ability of a system to withstand any negative event and return to functioning as it did before the event - has had a lot of media exposure and has been declined in different keys. Not least the digital one, with the parallel emergence of the concept of cyber resilience. READ MORE.

itrainsec

Manage crises responsibly through organisational resilience

An organisation that is resilient is able to handle any situation or problem that comes its way. It is able to sense change as it emerges, and takes action to minimise any risk. An organisation that is not, will not thrive under adverse circumstances, and is more likely to fall behind, or even close its doors in times of uncertainty. Find out how building organisational resilience can help your company manage crises responsively and effectively. READ MORE.

THANK YOU

for your time!

The Cybersecurity Awareness Calendar
is an initiative launched by:
European Cyber Security Organisation (ECSO)
29, rue Ducale
1000 - Brussels

company/ecso-cyber-security

@ecso_eu

www.ecs-org.eu

secretariat@ecs-org.eu