



WITH YOU ALL THE WAY



Manos Manoli
I.T. Manager/Chief Info. Security Officer

csn
SHIPPING EVENTS

**7TH CSN CYPRUS
ICT CONFERENCE**

Intelligent Skies, Secure Seas:
The AI Impact on ICT

05 MAY 2026

My New CarKey



CYBERSECURITY & GEOPOLITICAL LANDSCAPES FORECAST



RANSOMWARE

Remains the most important cyber threat as new groups appear, and others like Lockbit are consolidated. We expect new extortion methods and dual ransomware attacks



MAJOR TAKEDOWNS

Law enforcement takedowns resulting in migrations to other platforms and recruiting of old integrants by other groups



0-DAYS AND SUPPLY CHAIN

The use of zero-day exploits and supply chain attacks to target a broad range of victims to continue or increase



MALWARE AS A SERVICE

MaaS providers to continue to refine their functionalities and provide services at a cheaper rate. New info stealer variants with enhanced features to avoid detection



ARTIFICIAL INTELLIGENCE

CTI researchers will likely uncover new ways AI is exploited in offensive operations. AI tools will likely pose new data privacy and confidentiality issue for companies



GEOPOLITICS

Geopolitics and elections are likely to be catalysts for the evolution of the cyber threat landscape in 2024.



CYBER INSURANCE

Policyholders are likely to face unprecedented challenge amid soaring insurance premiums



LOLBINS

Living-Off-the-Land Binaries and signed system drivers will likely circumvent more often security protocols and help privilege escalation



STATE SPONSORED GROUPS

Sophisticated groups will likely exploit edge devices more often

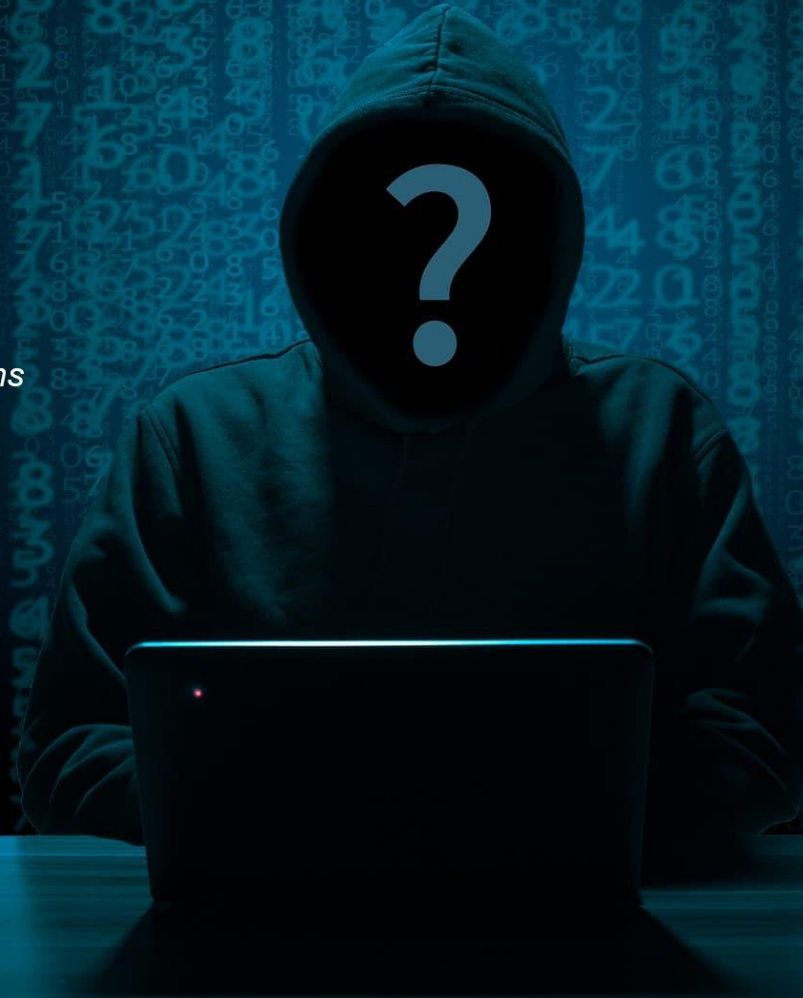


GLOBAL SHIPPING

Geopolitical instability and conflicts in Middle East will likely result in a surge in ocean freight rates

Cyber Group Pattern Shift

1. *Script Individuals*
2. *Cyber Crime Groups*
3. *Cyber Crime Organisations*
4. *Insider Threats*
5. *State Government Groups*



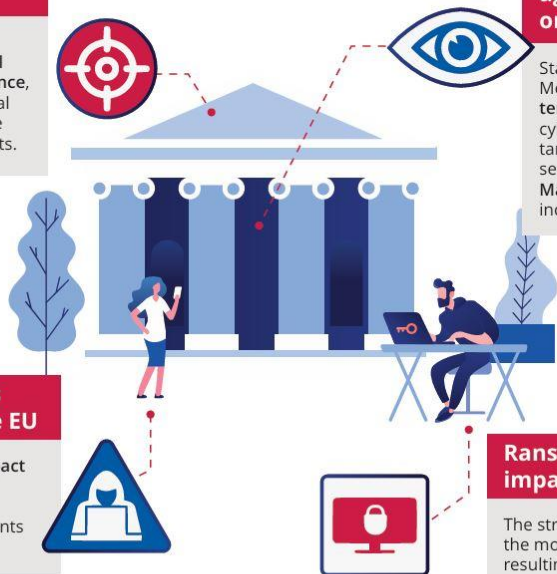
1. *Cyber Crime Groups*
2. *Cyber Crime Organisations*
3. *State Government Groups*
4. *Insider Threats*
5. *Script Individuals*



Threat Overview

Top 5 targeted sectors in the EU

These reportedly include public administration, transport, digital infrastructure and services, finance, and manufacturing, with essential entities representing 53.7% of the total number of recorded incidents.



State-aligned operations against EU Member States organisations persist

State-aligned activities against EU Member States continued at a steady tempo, with state-nexus cyberespionage activities notably targeting the public administration sector, and Foreign Information Manipulation and Interference (FIMI) increasingly targeting EU audiences.

Hacktivism dominates incident volume in the EU

It was mainly driven by low-impact DDoS campaigns targeting EU Member States' organisations' websites, with only 2% of incidents leading to service disruption.

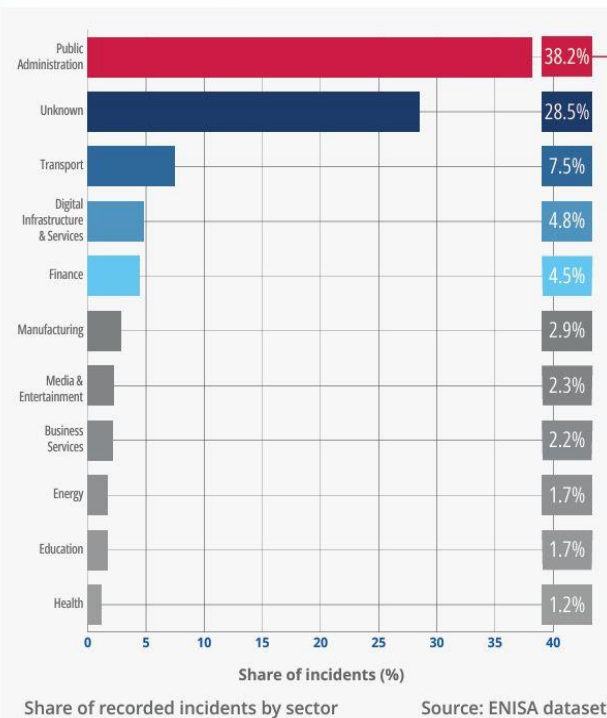
Ransomware remains the most impactful threat in the EU

The strains Akira and SafePay were among the most deployed, with a few incidents resulting in service disruptions.

02



Sectorial overview



38.2% Public Administration

Public Administration was identified as the most targeted sector in the EU (38.5%), dominated by low-impact DDoS (94.8%), with ransomware particularly affecting municipalities.



The transport sector came in second (7.5%), with most reported incidents pertaining to air and logistics, with a particular focus on targeting the maritime sector displayed by state-nexus intrusion sets.



While reportedly less targeted (2.2%), digital infrastructure and services in the EU, including Digital Services Providers remain high-value targets, particularly in the frame of incidents leveraging cyber dependencies used as launchpads for follow-up attacks.

03



IMAGE: VENTI VIEWS/PHOTOMOSH

Ransomware attack on maritime software impacts 1,000 ships

Malware

Briefs

BRIEFS

Barracuda Networks issue added to CISA vulnerability list

'Real-world experience' informs new Pentagon cyber strategy

Lender OneMain fined \$4.25 million for cybersecurity lapses

Iran-linked hackers Agrius deploying new ransomware against Israeli orgs

Health insurer says patients' information was stolen in ransomware attack

US sanctions North Korean entities involved in cyberattacks and IT worker fraud

Cryptomining group traced to Indonesia uses compromised AWS accounts |

Spying campaign targets Ukraine, Israel, India, Kazakhstan and others, cyber agency says

FBI warns about fake job ads from cyber traffickers

Lloyd's List: Θύμα κυβερνοεπίθεσης μία στις πέντε ναυτιλιακές την τελευταία τριετία

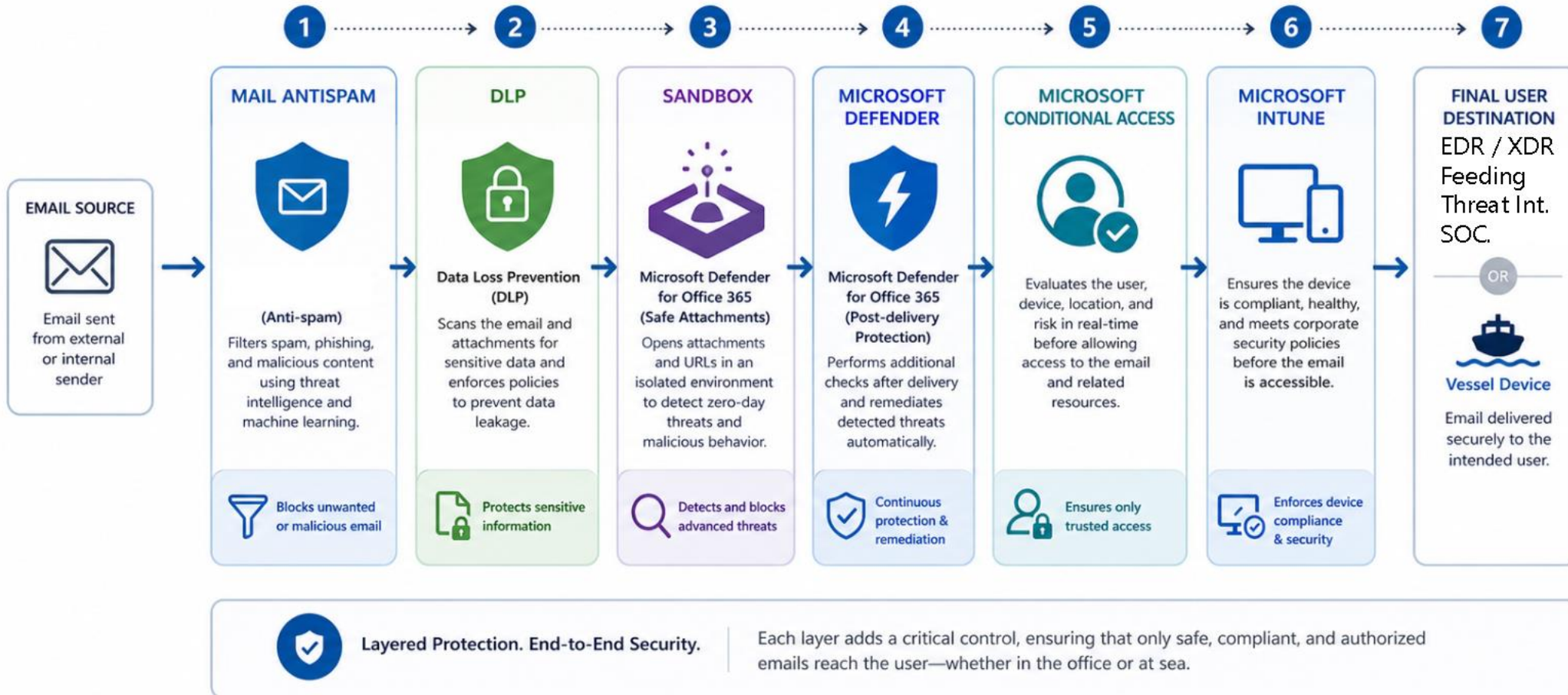
Ήδη θύματα είναι γνωστά ονόματα όπως Maersk, Cosco, CMA CGM, MSC, Clarksons, DNV, το Tokyo MOU και ο Διεθνής Ναυτιλιακός Οργανισμός (IMO) σύμφωνα με έρευνα της Lloyd's List



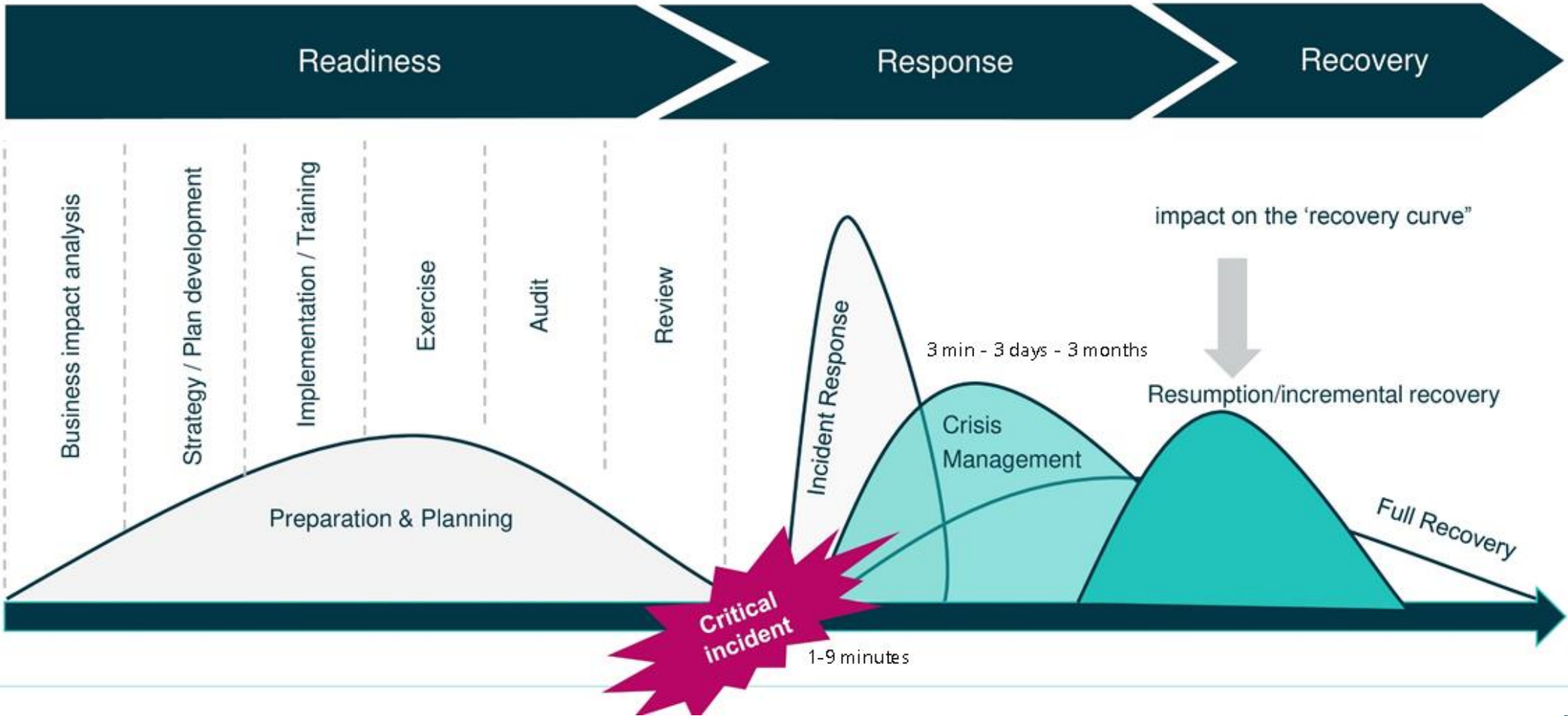
Advertisement

Email Security Journey – From Source to User

Multiple layers of Microsoft security technologies work together to protect every email before it reaches the end user.



▶ Managing cyber incidents in a time



WELCOME ABOARD!

Marlow Navigation Co. Ltd.

13 Alexandrias Street, 3013

P.O. Box 57077, CY-3720

Limassol, Cyprus

Tel: +357 25 882 588

info@marlowgroup.com

www.marlow-navigation.com

