Can you outsmart the hackers of tomorrow?

Strengthening Cybersecurity in Europe:
NIS 2 Directive, Vulnerability Management,
and Ransomware Readiness, AI is changing the cyber threats landscape.

Date: 16.06.2025

Atos EVIDEN

Agenda

Welcoming words by **Hristo Hristov, CEO of Eviden Bulgaria** and **Vessela Todorova-Mosettig, General manager of French-Bulgarian Chamber of Industry and Commerce**

<u>Topics:</u>

1. **The implications of the NIS 2 Directive for cybersecurity** – Stanimir Sotirov, Head of Cybersecurity in Eviden Bulgaria
2. **Importance of Vulnerability Management** - Stanimir Sotirov, Head of Cybersecurity in Eviden Bulgaria
3. **Implementation of the NIS Directive in the sector production, processing, Romania and Bulgaria** – Gergana Rakova, Chief expert in "Network and information security" Directorate at the Ministry of Digital Governance
4. **Project 101128086 « National Coordination Center » – Bulgaria** – Kalinka Boyanova, Chief expert in "Network and information security" Directorate at the Ministry of Digital Governance

Agenda

Coffee break and networking

Topics:

1. **Ransomware Readiness Assessment: A Critical Component** - Yavor Belitov, Service Line Manager in Eviden Bulgaria
2. **The Social Engineering Revolution: AI-Powered Deepfake & Cloning Attacks** – Martin Stoyanov, Big Data and AI Team Lead
3. **Conclusion** – Hristo Hristov, CEO of Eviden Bulgaria
4. Q&A, networking

Welcome to the Atos event

The implications of the NIS 2 Directive for cybersecurity

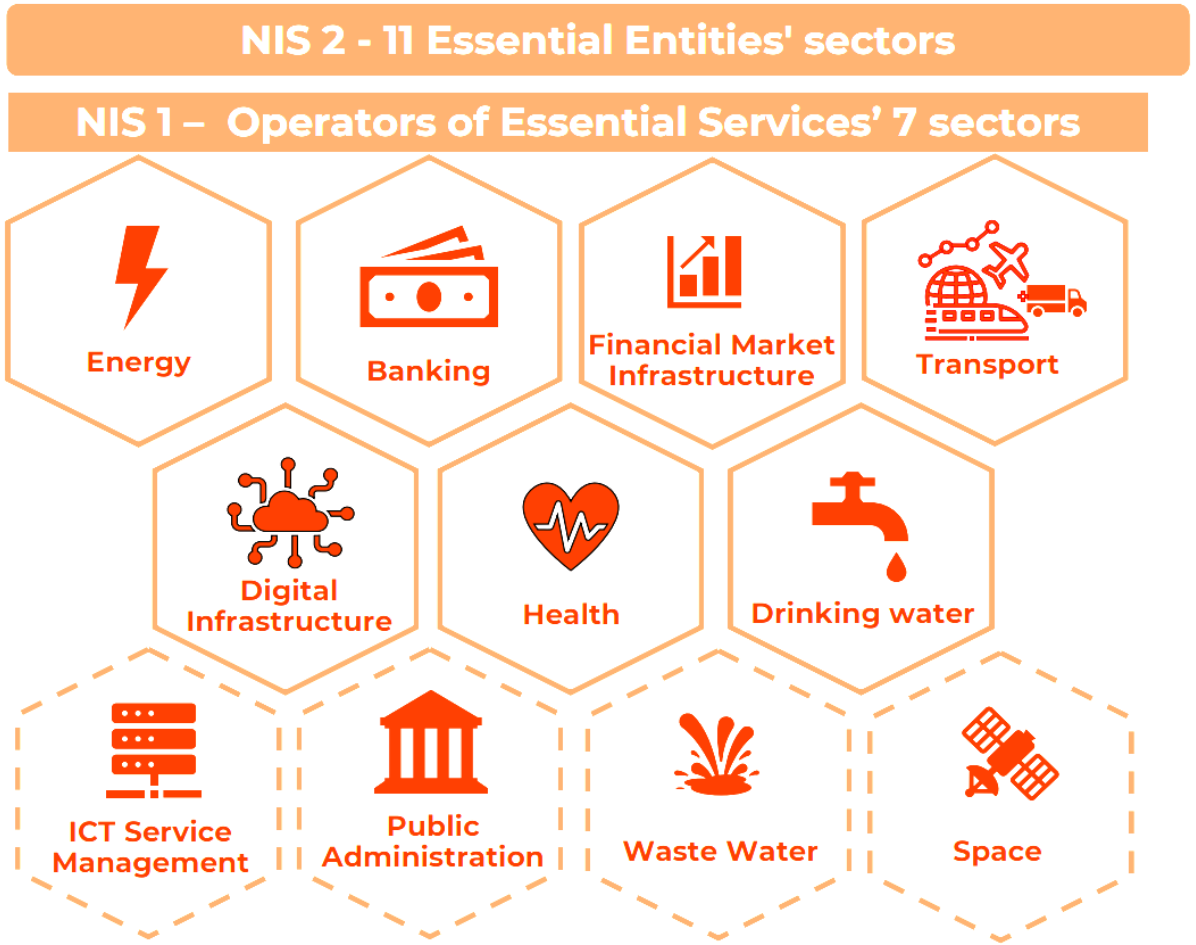
1. Veeam Survey results on NIS 2 Directive
2. Scope of NIS 2 Directive
3. NIS 2 Directive Penalties
4. NIS 2 Directive Highlights

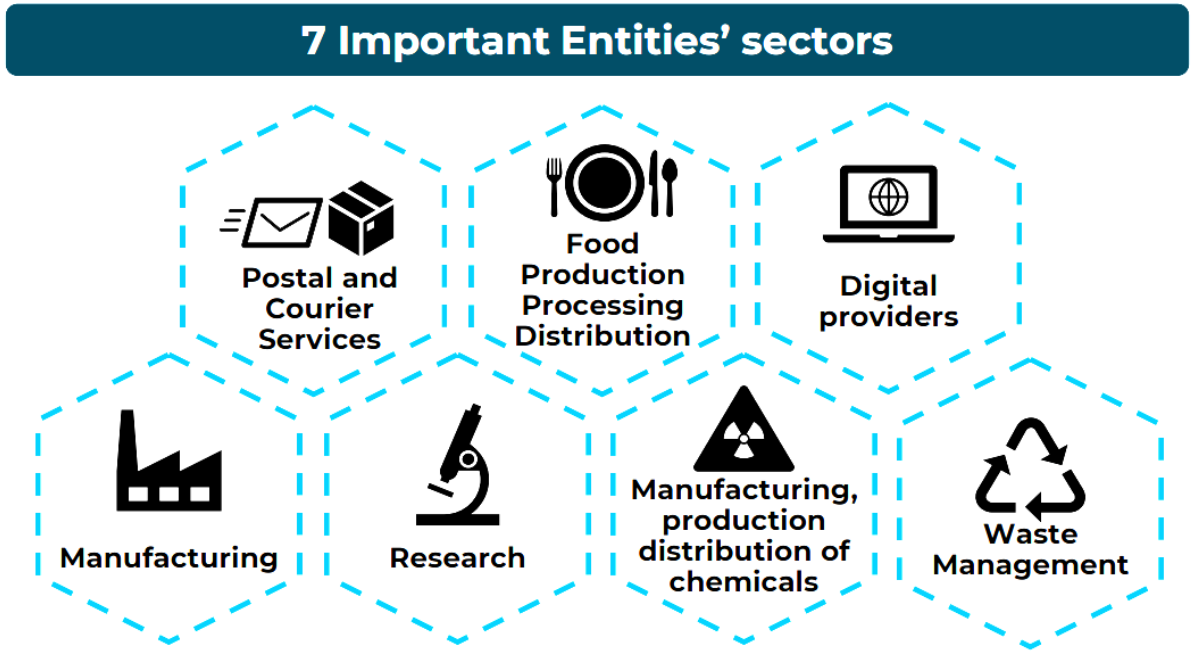
Veeam Survey results on NIS 2 Directive

90% of EMEA Businesses Faced Cybersecurity Incidents that NIS2 Could Have Prevented, Veeam Survey Reveals

Approximately 80% of businesses are confident in adhering to NIS2, yet 66% will miss the compliance deadline

Scope of NIS 2 Directive (160.000 entities in EU)

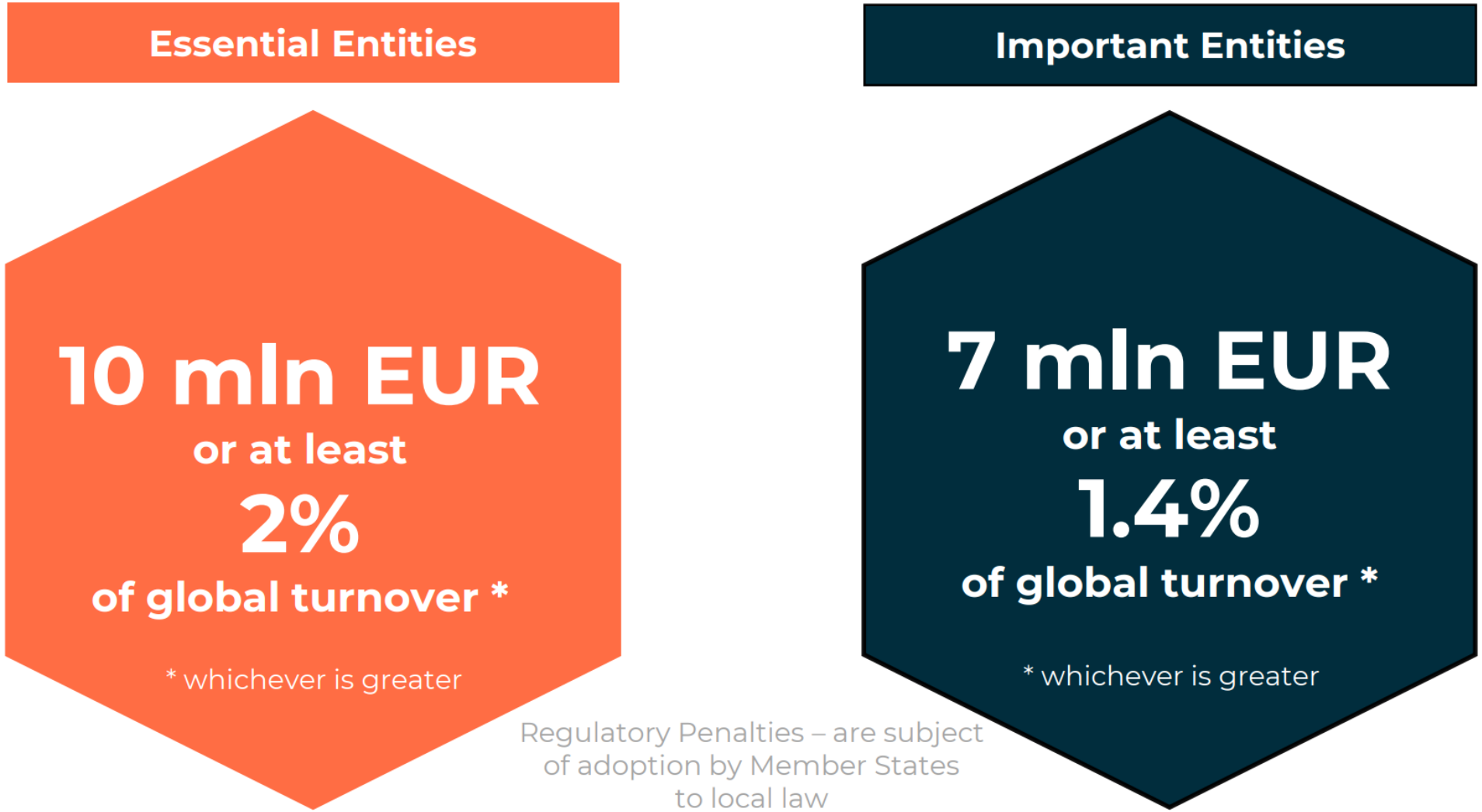




NIS 1 Directive Operators of Essential Entities became Essential Entities in NIS-2
NIS 2 Directive – Newly added Essential Entities, apart from those included in NIS-1 Directive

New group of Important Entities in NIS-2 Directive

NIS 2 Directive Penalties



Regulatory Penalties – are subject of adoption by Member States to local law

NIS 2 Directive Highlights

- The security requirements are covering both IT and OT infrastructure
- Senior management, including CEOs are personally accountable for the cybersecurity practices of their organizations
- CEOs must ensure that adequate measures are in place to manage and mitigate cybersecurity risks
- Cyber Security Incidents reporting – within 24 hours for initial warning, within 72 hours for Incident notification
- Change Management is additional requirement for Bulgaria
- Bulgaria is expected to transpose the NIS 2 security requirements into Bulgarian legislation in June 2025 (expecting final/second vote of the law in the Bulgarian Parliament)

The importance of Vulnerability Management

1. Why it is essential to have a Vulnerability Management program?

2. Vulnerability Management Lifecycle

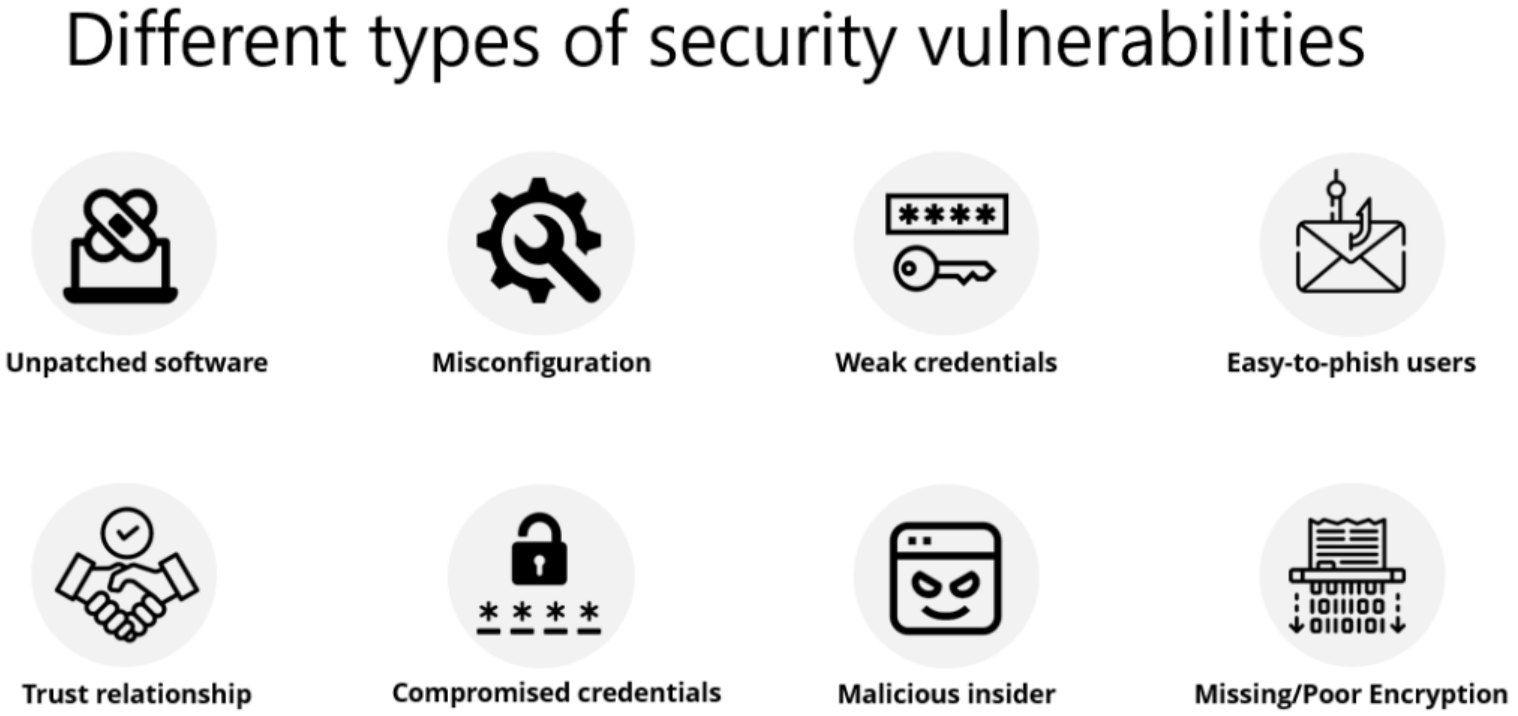
3. Is the risk of Cyber Threats real?

Why it is essential to have a Vulnerability Management program?

1. Vulnerabilities are considered a Major Cybersecurity Risk

2. Evolving T

3. Protects E



Vulnerability Management Lifecycle

Is the risk of Cyber Threats real?

- Cyber Magazine

  News & Articles | Magazines | Reports & Whitepapers

  Cybersecurity breaches at Orange and NTT Communications expose mobile infrastructure weaknesses, as direct exploitation rises by 74% across telecoms

- Orc

  -

  -

  -

About us

26
operating countries
(including non consolidated countries)

291 million
customers worldwide

at December 2024

127,000
employees

€40.3 billion
in revenue

Orange in the world

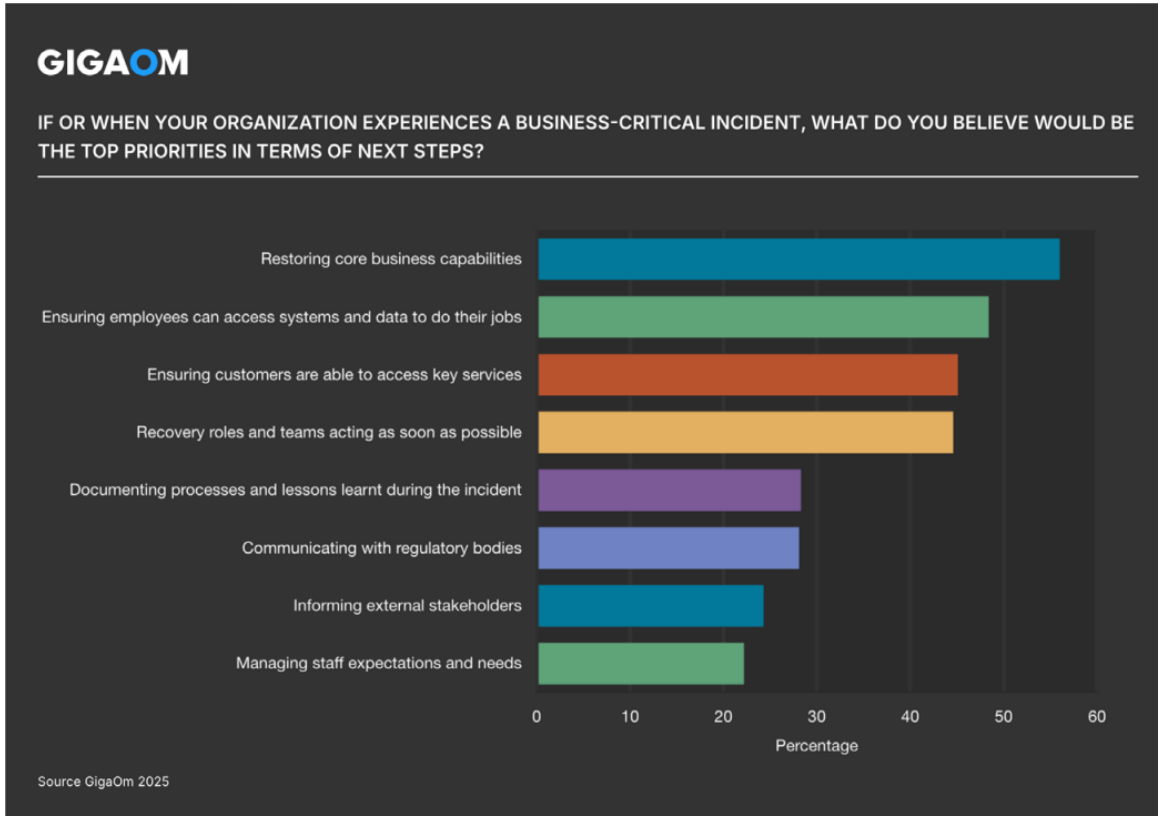
Orange share price

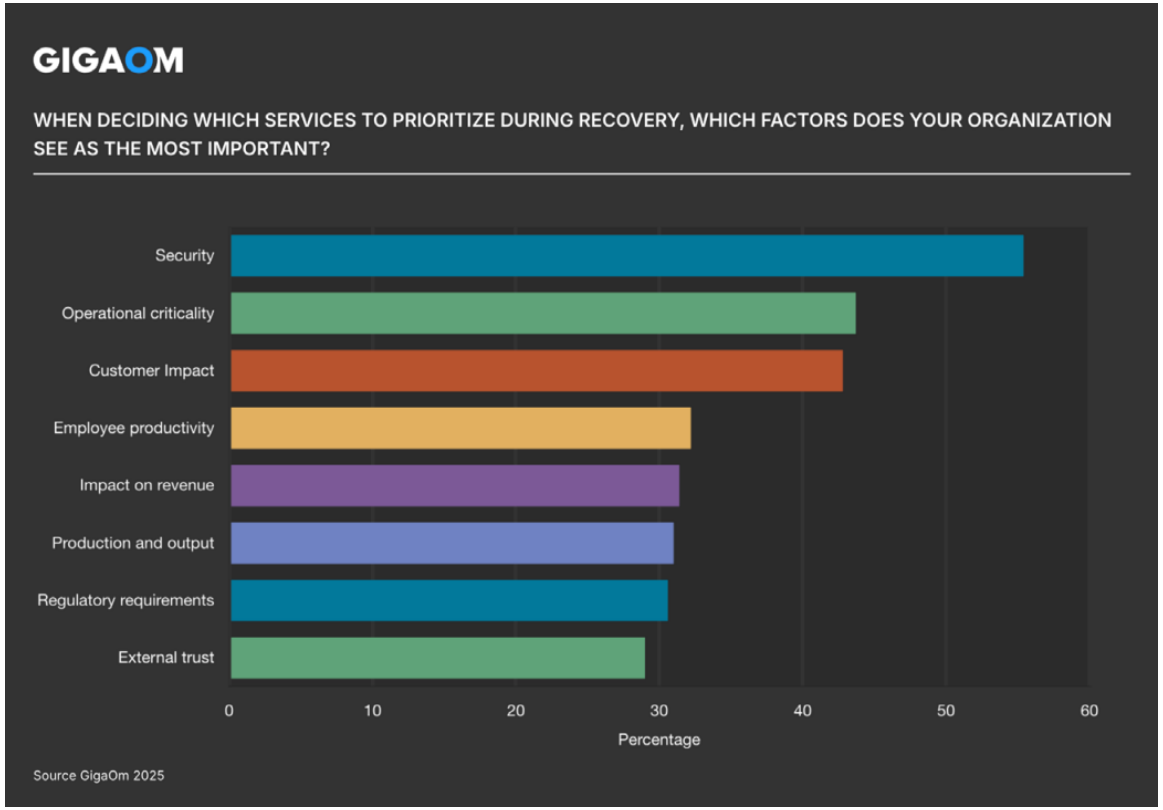
Ransomware Readiness Assessment

1. The Gap
2. Planning
3. Testing your plan
4. Preparedness Assessment

The Gap

Neither side was wrong – we need to build a bridge between the two





Source: Commvault report "Minimum Viable Recovery: Closing the Recovery Gap"

Planning

Key Questions (that are commonly missed)

- When do we trigger the recovery plan and procedures?
- Who can take the decision to activate the plan?
- How to achieve the maximum possible degree of automated decision making?
- What is the order of restoration? Is the order of restoration agreed with the business stakeholders?
- "Clean Infrastructure" vs "Existing infrastructure"

Testing your plan

Key Challenges

- Do we ever test complete IT landscape recovery from cyber incident? Do we execute only the mandatory restore tests required for the annual audit?
- Are we sure that backups would be intact? Are we sure we can recover it all?
- Are we sure we know how to agree on recovery point?
- Do we have all the right parties onboarded in this procedure? Are they aware of our procedures and their role?
- Are we sure we have the proper timing in the plan?

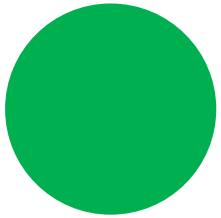
The Goal of the Ransomware Preparedness Assessment

- IT Systems recovery is an IT task

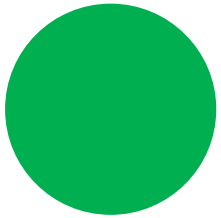
- Recovery plan is created by IT team only

- Recovery plans and procedures exist

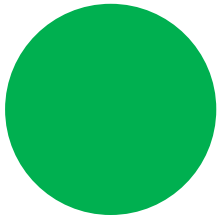
- We can recover from a ransomware event



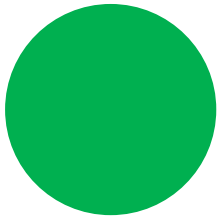
- IT Systems recovery is a Business Continuity matter owned by IT



- Recovery plan creation is moderated by IT in collaboration with business stakeholders



- Recovery plans and procedures exist, are tested and amended regularly



- We can recover our systems in order of criticality within predictable timing


Number 2: we chose a very open dialogue around this.
From day 1 we were on Twitter telling about what had happened,
and we have spent enormous resources on helping other companies.
I think that is an important point to make.

Thank you!

Date: 16.06.2025