

# Cybercrime in the Age of AI

*Yugo Neumorni,  
President CIO Council*



# Yugo Neumorni

ContourGlobal, CIO

Advisory Board Member  
InCyber, France

Cargus, CIO

Chairman of EuroCIO

Hidroelectrica, CIO

CIO Council Romania  
President & founder

Vimetco, CIO

ISACA Romania  
President

Deloitte Central  
Europe, IT Manager

Deloitte Central Europe,  
IT Manager

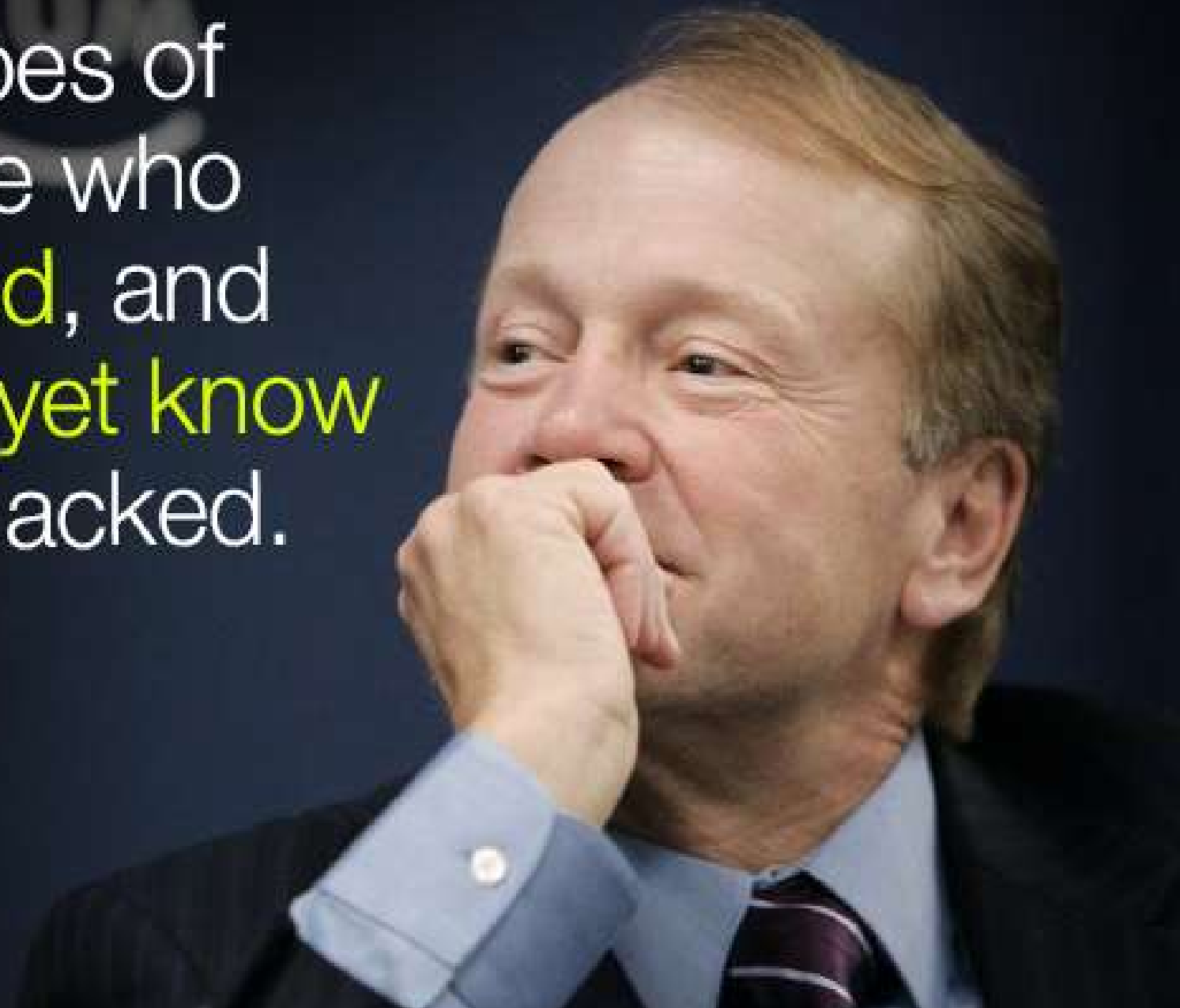
Having more than 30 years of experience in the IT industry, Yugo Neumorni is specialized in energy and manufacturing, complex digital transformation processes, IT systems redesign, cybersecurity and cyber-defense programs, data privacy and GDPR, ERP, BI and analytics projects, IT governance and COBIT framework.

He is speaker in IT international events, private investor and consultant for VC funds.

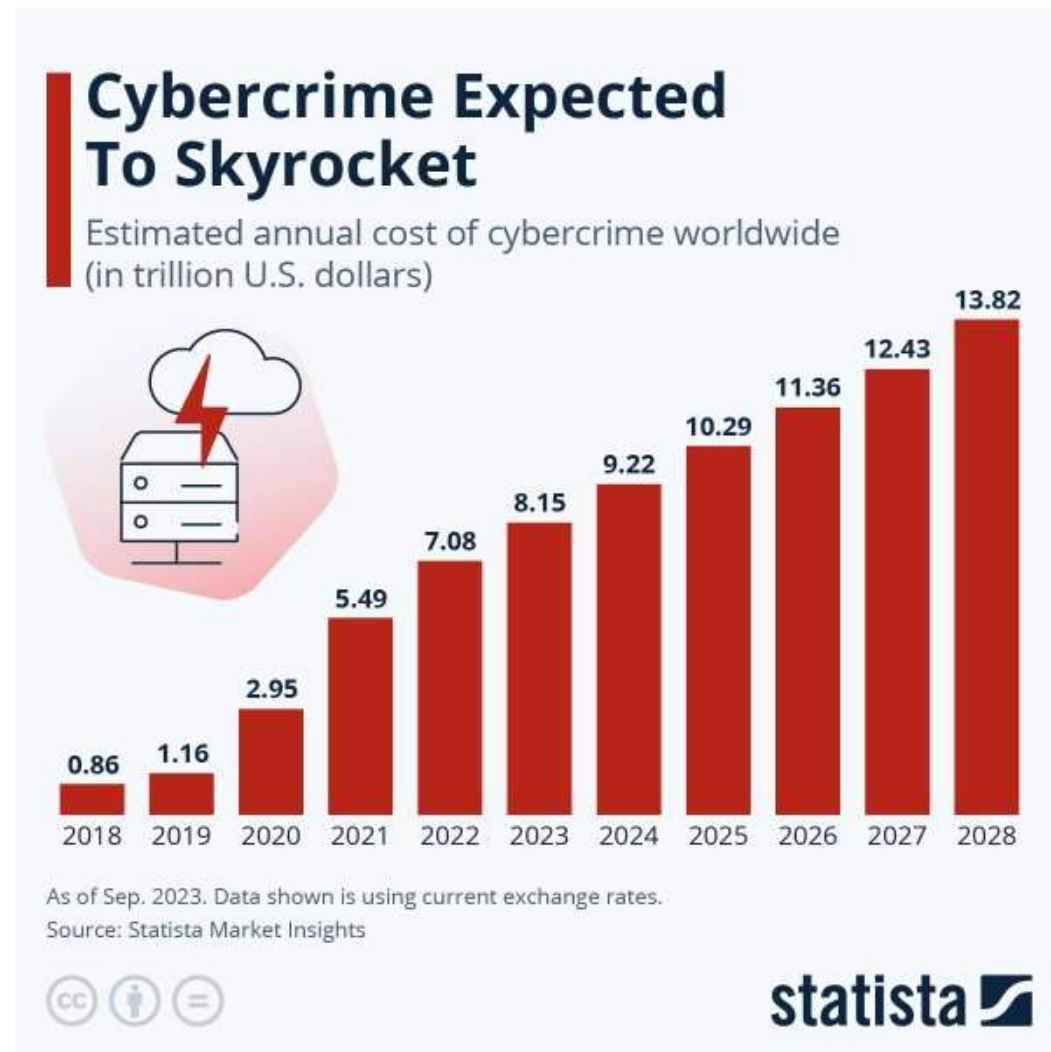
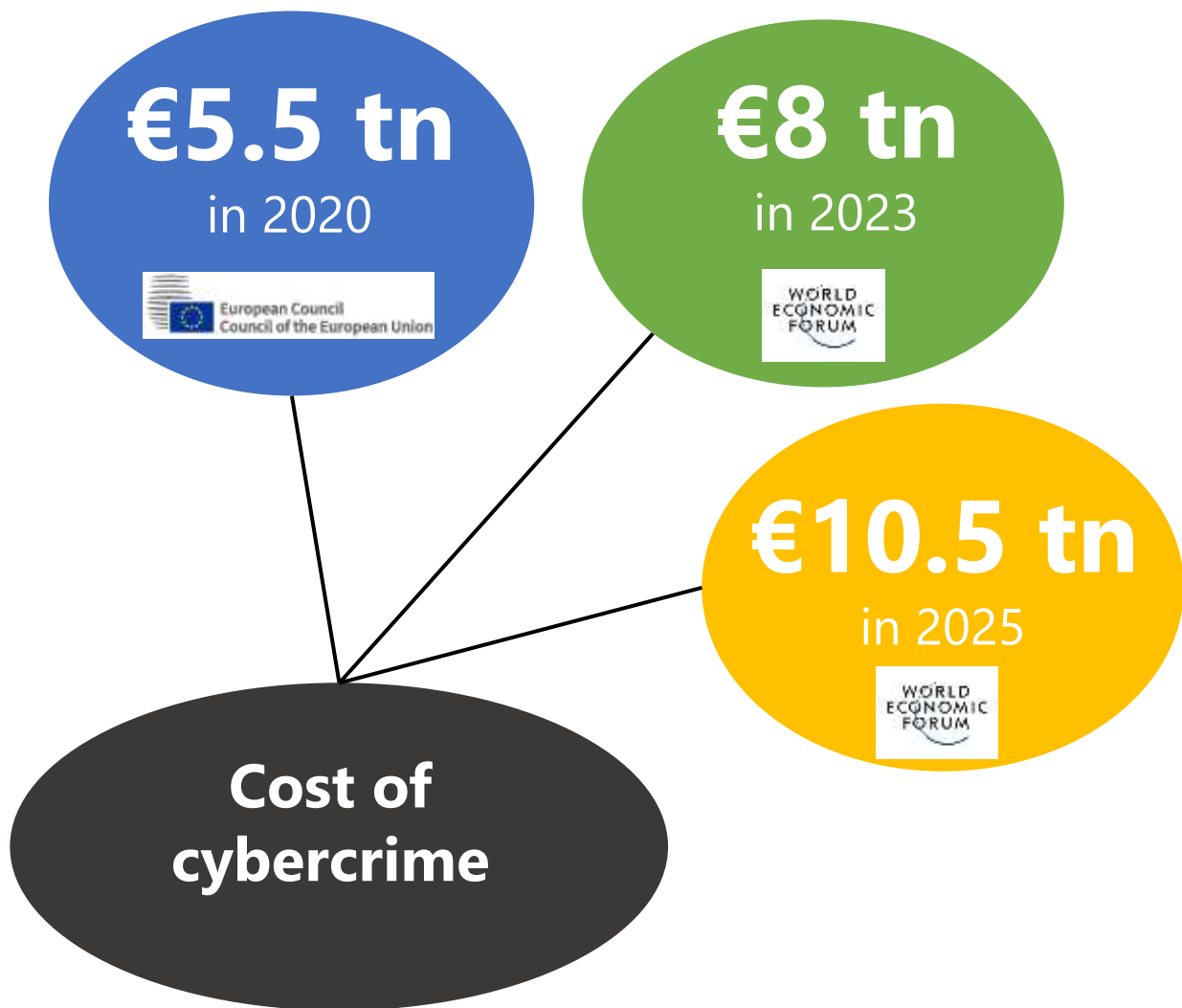


There are two types of companies: those who **have been hacked**, and those who **don't yet know** they have been hacked.

John Chambers  
Chief Executive Officer of Cisco



# Total costs of cybercrime globally



# Total costs of cybercrime globally



United States GDP

**\$25tn**



Germany GDP

**\$4.4tn**



France GDP

**\$3.03tn**



Cybercrime globally

**\$8.0tn**



Global GDP

**\$103tn**



Market capitalization

**\$3tn**



Market capitalization

**\$3tn**



# *Cybersecurity is a business*

	CAGR
Cybersecurity	- 8.5%
Energy	- 5%
EV Auto	- 23%
AI	- 28%
Food	- 1.68%

# IT Budgets

**Checkpoint Research** reported a **38%** increase of global cyber from 2022 to 2021 and with **48%** in utilities.

**Verizon** - the damages caused by an attack is quantified by Verizon between **5 to 15 mln USD**

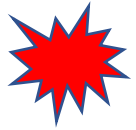


**Gartner** – Cybersecurity costs increase **11% YoY** and 12 – 15% YoY from the total IT budgets

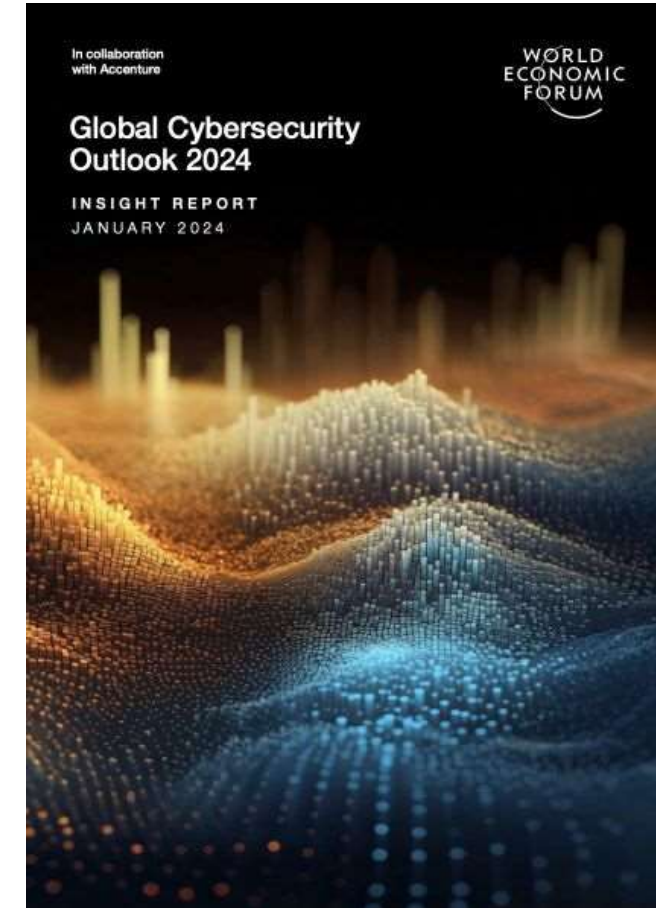
Cybersecurity costs estimated to **0.5 – 1% from total revenues** in average

**NIS2 Directive** brings 25% increase for companies to be enrolled on NIS2. 15% for companies that are already under NIS1 Directive. 13000 companies to be enrolled in Romania under NIS2.

# World Economic Forum. Global Cybersecurity Outlook 2024

*There is growing cyber inequity between organizations that are cyber resilient and those that are not.*




-  The number of organizations that maintain minimum viable cyber resilience is down 30%. While large organizations demonstrated remarkable gains in cyber resilience, SMEs showed a significant decline.
-  More than twice as many SMEs as the largest organizations say they lack the cyber resilience to meet their critical operational requirements.
-  90% of the 120 executives surveyed at the World Economic Forum's Annual Meeting on Cybersecurity said that urgent action is required to address this growing cyber inequity.

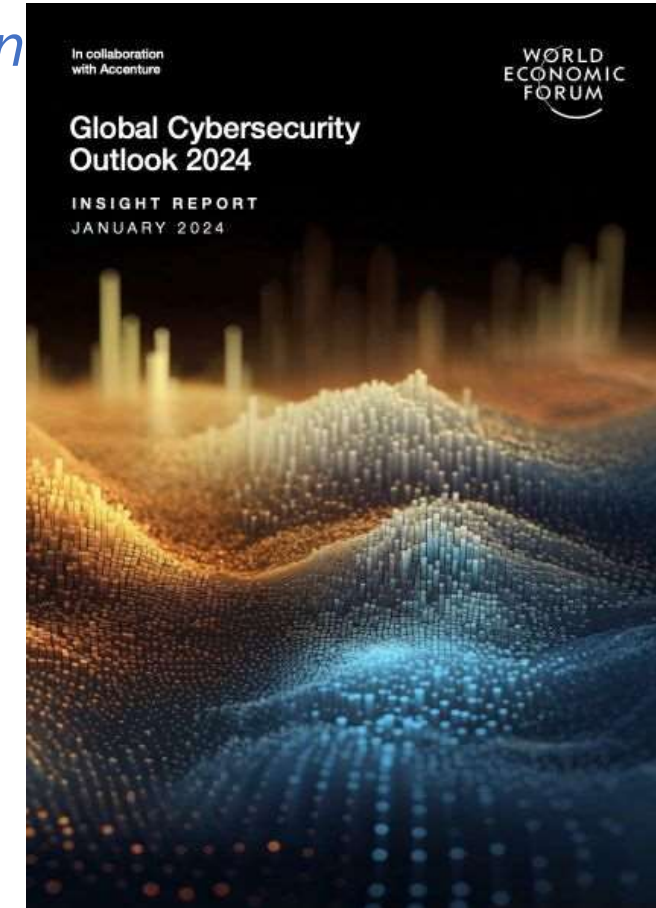




# World Economic Forum. Global Cybersecurity Outlook 2024





*Alignment between cyber and business is becoming more common*

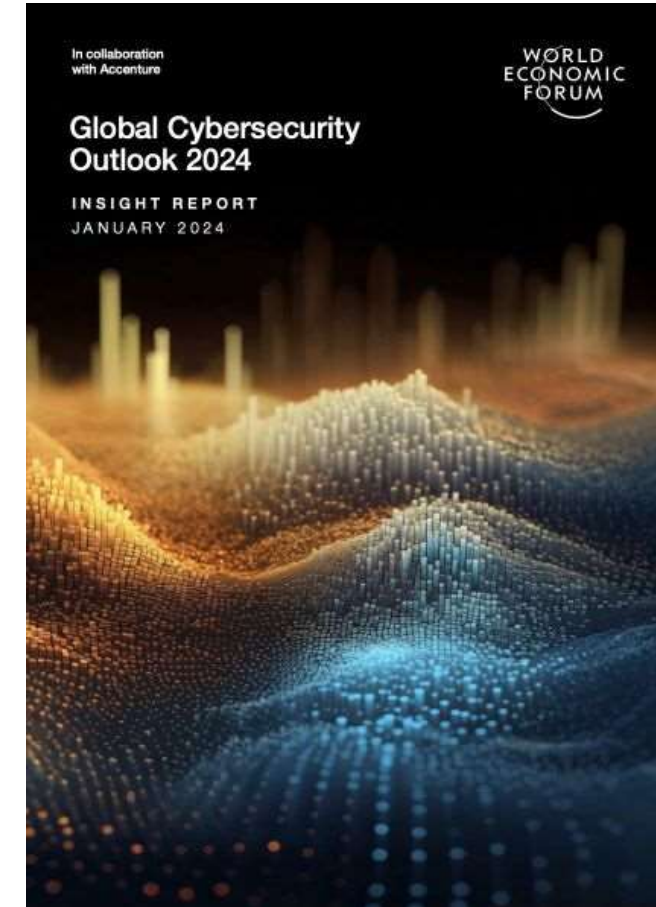
-  **29% of organizations** reported that they had been **materially affected** by a cyber incident in the past 12 months
-  **The largest organizations say that the highest barrier to cyber resilience is transforming legacy technology and processes**
-  There is a clear **link** between **cyber resilience** and **CEO engagement**. This year, 93% of respondents that consider their organizations to be leaders and innovators in cyber resilience trust their CEO to speak externally about their cyber risk. Of organizations that are not cyber resilient, only 23% trust their CEO's ability to speak about their cyber risk.



# World Economic Forum. Global Cybersecurity Outlook 2024

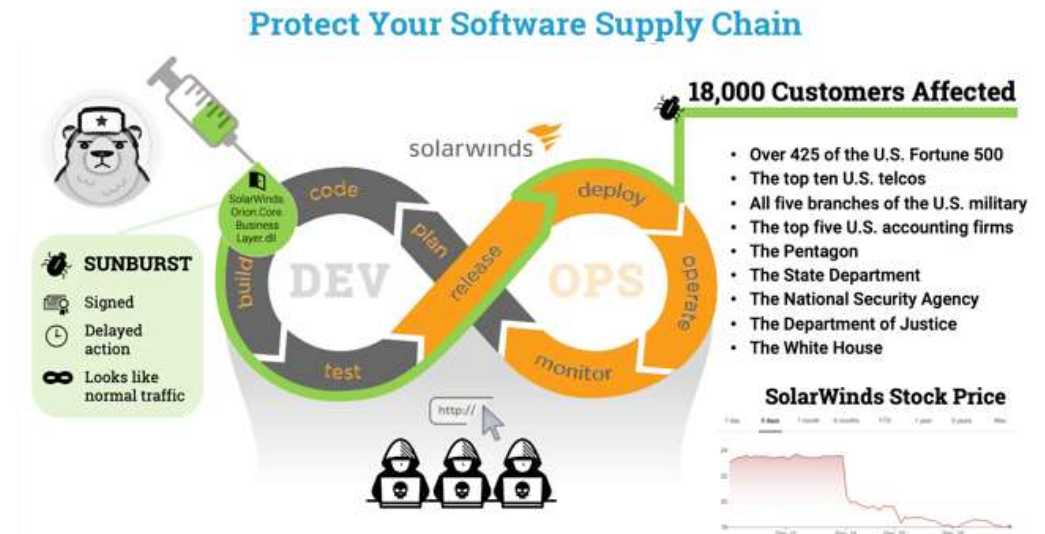
*Cyber ecosystem risk is becoming more problematic.*

-  **41%** of the organizations that suffered a **material incident** in the past 12 months say it was caused by a third party.
-  **54% of organizations** have an insufficient **understanding** of cyber vulnerabilities in their **supply chain**.
-  Even 64% of executives who believe that their organization's cyber resilience meets its minimum requirements to operate say they still have an inadequate understanding of their supply-chain cyber vulnerabilities.
-  60% of executives agree that cyber and privacy regulations effectively reduce risk in their organization's ecosystem – up 21% since 2022.



# SolarWinds attack - 2021

- highly sophisticated Russian Intelligence group has compromised the SolarWinds Orion platform infecting directly into the SolarWinds DevOps. the package was signed with a valid certificate
- 18,000 customers affected downloading the patches, opening a backdoor to the attackers
- Attackers penetrated and manipulated SolarWinds 9 months before, malware deployment estimated to December 2019
- Orion it is connected everywhere – from switches and routers, to firewalls, virtualization infrastructure, Active Directory, storage management tools and more
- US agencies, DHS, the Department of Energy, the National Nuclear Security Administration, and the Treasury — were attacked. Also private companies, like Microsoft, Cisco, Intel, and Deloitte
- This could lead access to OT / SCADA / Industrial Control System networks



- What if operating systems (Windows) supply chain will be hacked?
- What if the hardware firmware of critical equipment is hacked?



**IBM**

*It takes 277 days on average to identify and contain a breach: 207 days to identify and 70 days to contain.*

<https://blog.adolus.com/blog/three-things-the-solarwinds-supply-chain-attack-can-teach-us>



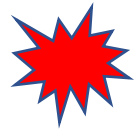

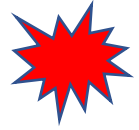
# Ukrainian power grid attack

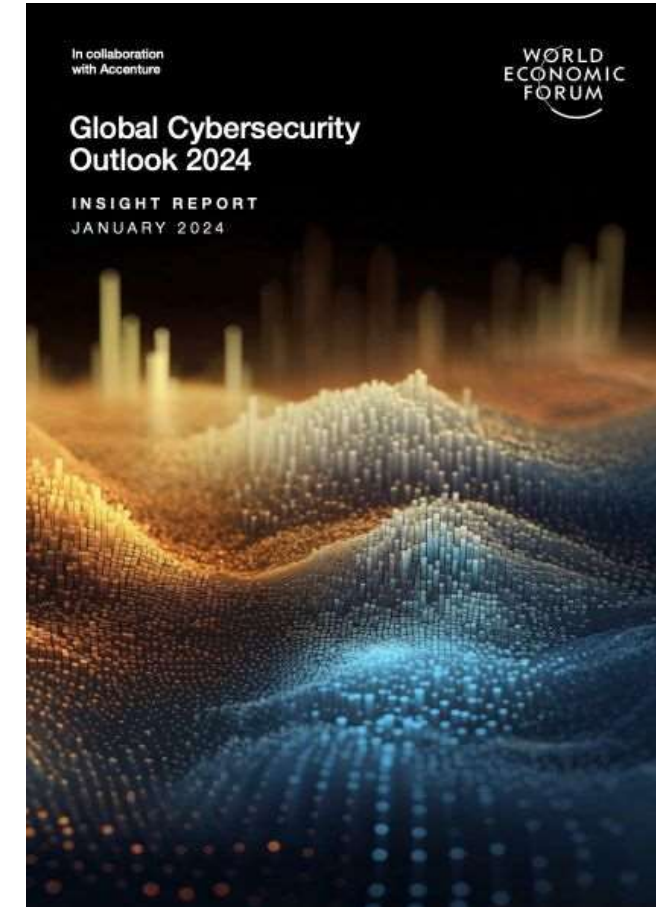
- 225,000 people were left without power for 6 hours on Dec 23, 2015, in Ukraine.
- Spear-phishing schemes, malware, and manipulation of long-known Microsoft Office macro vulnerabilities. Collected the credentials to gain access to SCADA systems
- Co-opting remote terminal units within SCADA systems to issue "open" commands to specific breakers at substations
- Severing communications by targeting firmware in serial-to-Ethernet devices
- Installing and running a modified KillDisk program that deleted information on what was occurring while making recovery reboots nearly impossible
- Shutting down uninterruptible power supplies at control centers
- Executing a large denial-of-service attack on utility call centers that prevented customers from reporting outages
- Spear phishing is a targeted email that appears to be from a known business or individual



# World Economic Forum. Global Cybersecurity Outlook 2024

The cyber-skills and talent shortage continues to widen at an alarming rate.

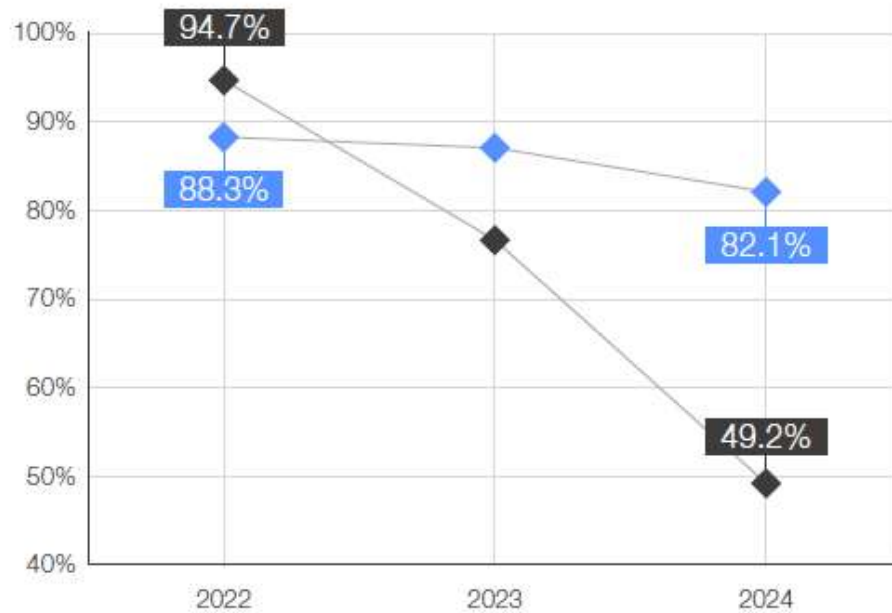
-  Half of the smallest organizations by revenue say they either do not have or are unsure as to whether they have the skills they need to meet their cyber objectives.
-  Only 15% of all organizations are optimistic that cyber skills and education will significantly improve in the next two years.
-  52% of public organizations state that a lack of resources and skills is their biggest challenge when designing for cyber resilience.



# World Economic Forum. Global Cybersecurity Outlook 2024

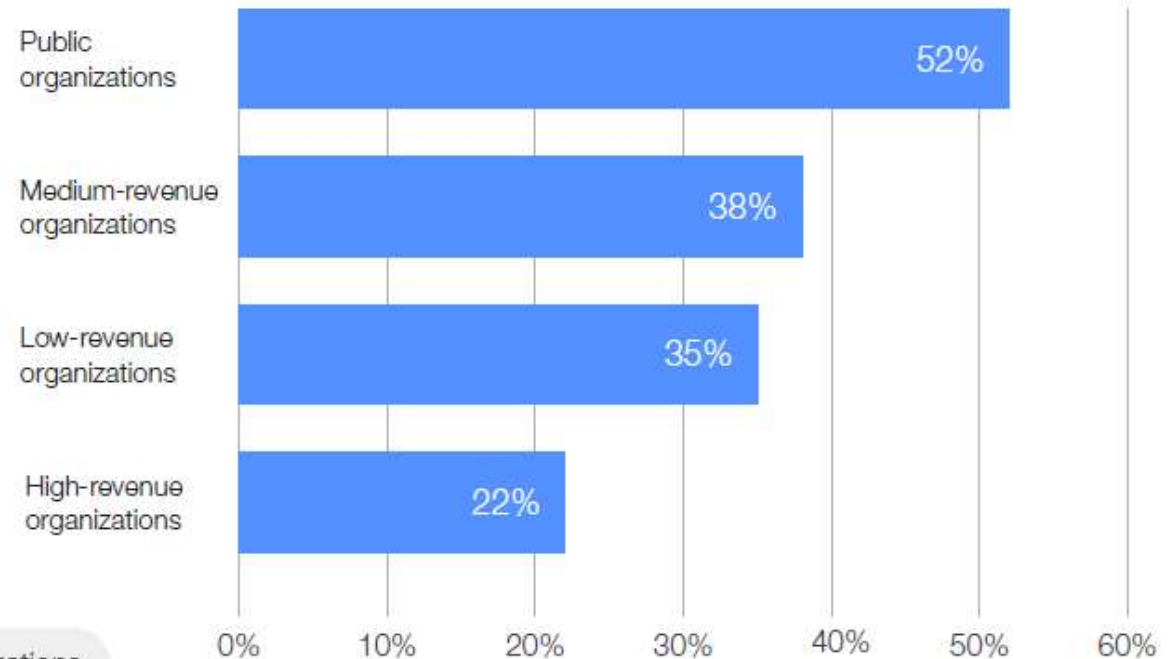
## The cyber skills and talent shortage continues to widen at an alarming rate

Does your organization have the skills needed to respond to and recover from a cyberattack?



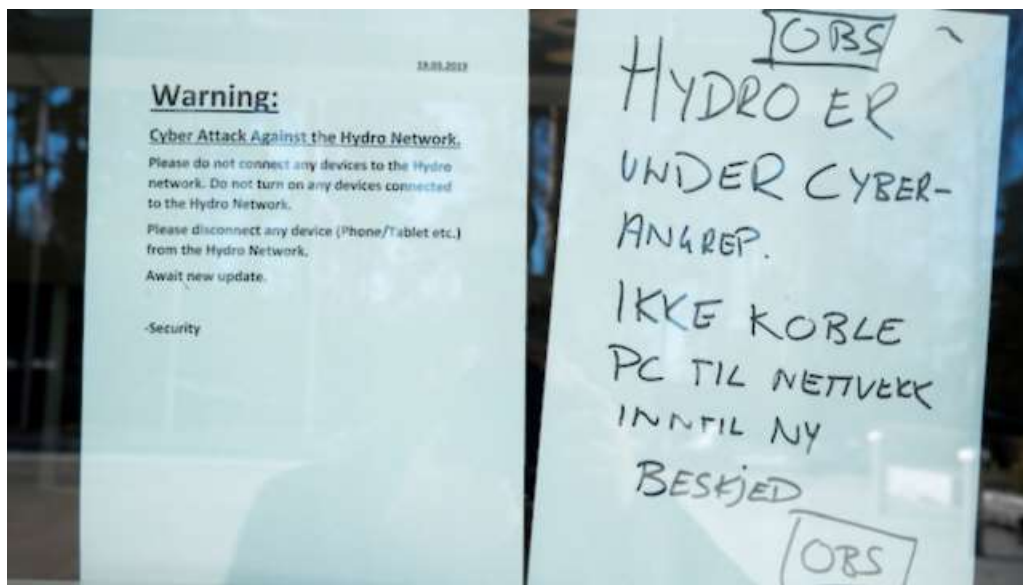
● Low-revenue organizations ● Medium- and high-revenue organizations

Are resources or skills gaps the biggest challenge for your organization when designing for cyber resilience?



# Norsk Hydro held hostage by a ransomware attack

- 22,000 computers affected
- 170 sites in 40 countries
- 35.000 employees back to pen and paper
- Norsk operated on manual
- Norsk restored from backups



## Workshop:

- To pay or not to pay?
- Where do I get Bitcoins?
- Where is my backup?
- Was backup affected?
- IS there a DRP plan for ransomware situations?
- What is the first service restored? Active Directory? ERP?
- Do we need additional hardware? Where do we get from?



# World Economic Forum. Global Cybersecurity Outlook 2024

## Emerging technology will exacerbate long-standing challenges related to cyber resilience

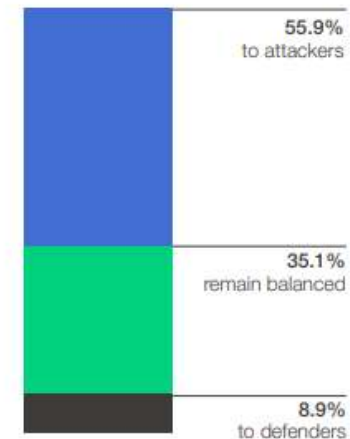
As organizations race to adopt new technologies, such as generative artificial intelligence (AI), a basic understanding is needed of the immediate, mid-term and long-term implications of these technologies for their cyber-resilience posture.

Fewer than one in 10 respondents believe that in the next two years generative AI will give the advantage to defenders over attackers.>

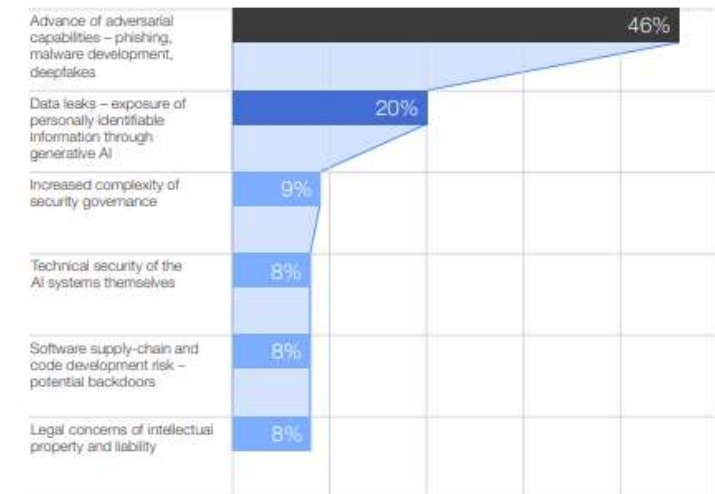
Approximately half of executives say that advances in adversarial capabilities (phishing, malware, deepfakes) present the most concerning impact of generative AI on cyber

### Emerging technologies will exacerbate long-standing challenges related to cyber resilience

In the next two years, will generative AI provide overall cyber advantage to attackers or defenders?



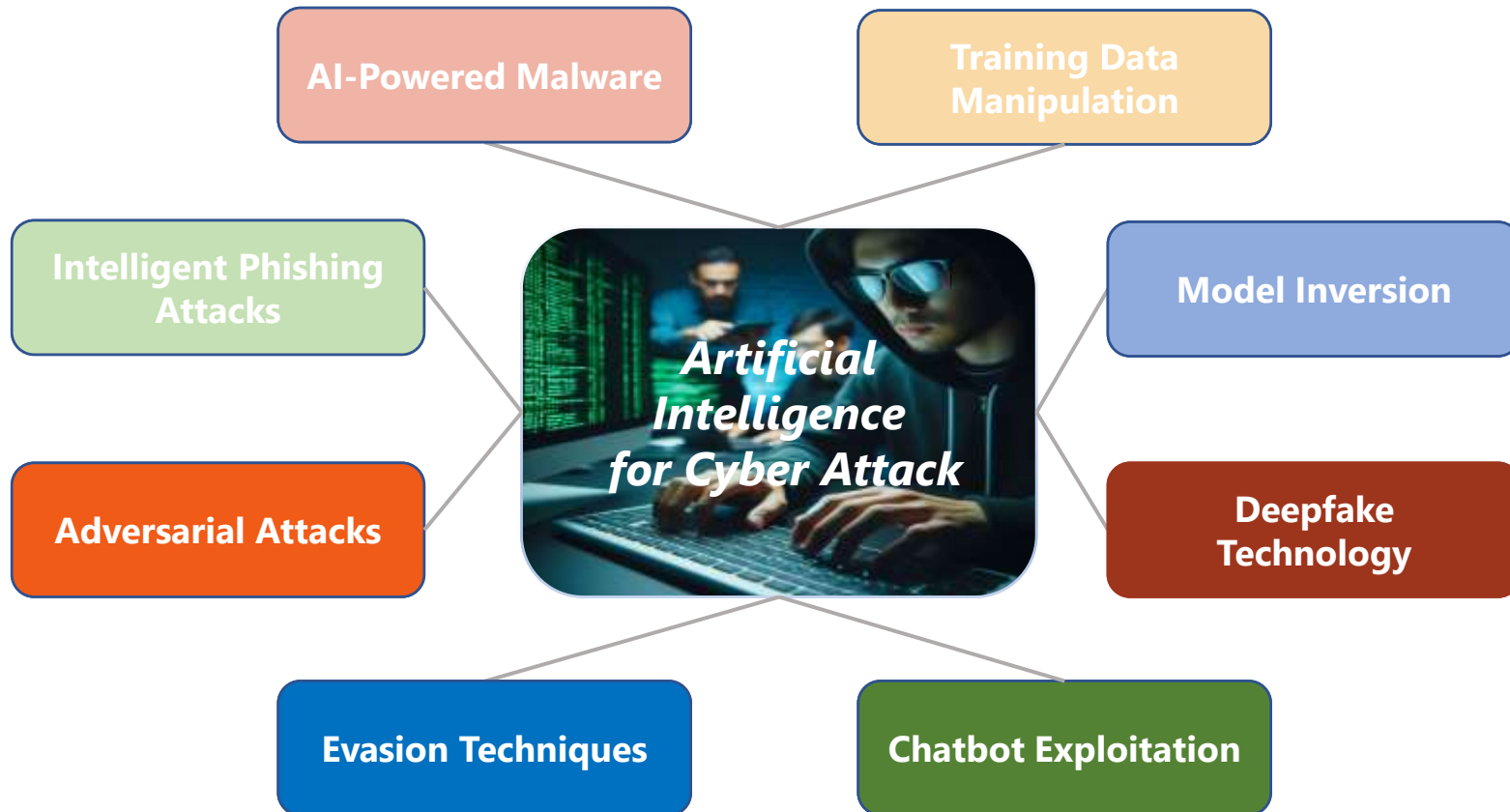
What are you most concerned about in regards to generative AI's impact on cyber?



# Artificial Intelligence for Cyber Defense



# Artificial Intelligence for CyberAttack



*Microsoft Created a Twitter Bot to Learn From Users. It Quickly Became a Racist Jerk.*



WSJ PRO

**Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case**

Scams using artificial intelligence are a new challenge for companies

# Building Cyberresilience

**Assume Breach!**

**Zero Trust  
Philosophy**

**Incident  
Response and  
Recovery Plan**

**Employee  
Awareness and  
Training**

**Continuous  
Monitoring and  
Threat Detection**

**Regularly Update  
and  
Patch Systems**

**Secure Software  
Development**

**Implement a  
Multi-Layered  
Security  
Approach**



*"95% of the attacks could be avoided if simple cyberhygiene is adopted"*

**CyberInt, Romanian Secret Service**

# Q&A

**Yugo Neumorni**, EMBA, CISA  
*President, CIO Council Romania*