Cybersichere Energie in herausfordernden Zeiten – Bedrohungen, Risiken und Chancen

Dr. Judith Wunschik
Chief Cybersecurity Officer

Siemens Energy is a

global leader in the energy business

~ 1/6

of global electricity generation is based on our technology.

91,000

employees work as a team to energize society.[1]

We are present in

> 90 countries.

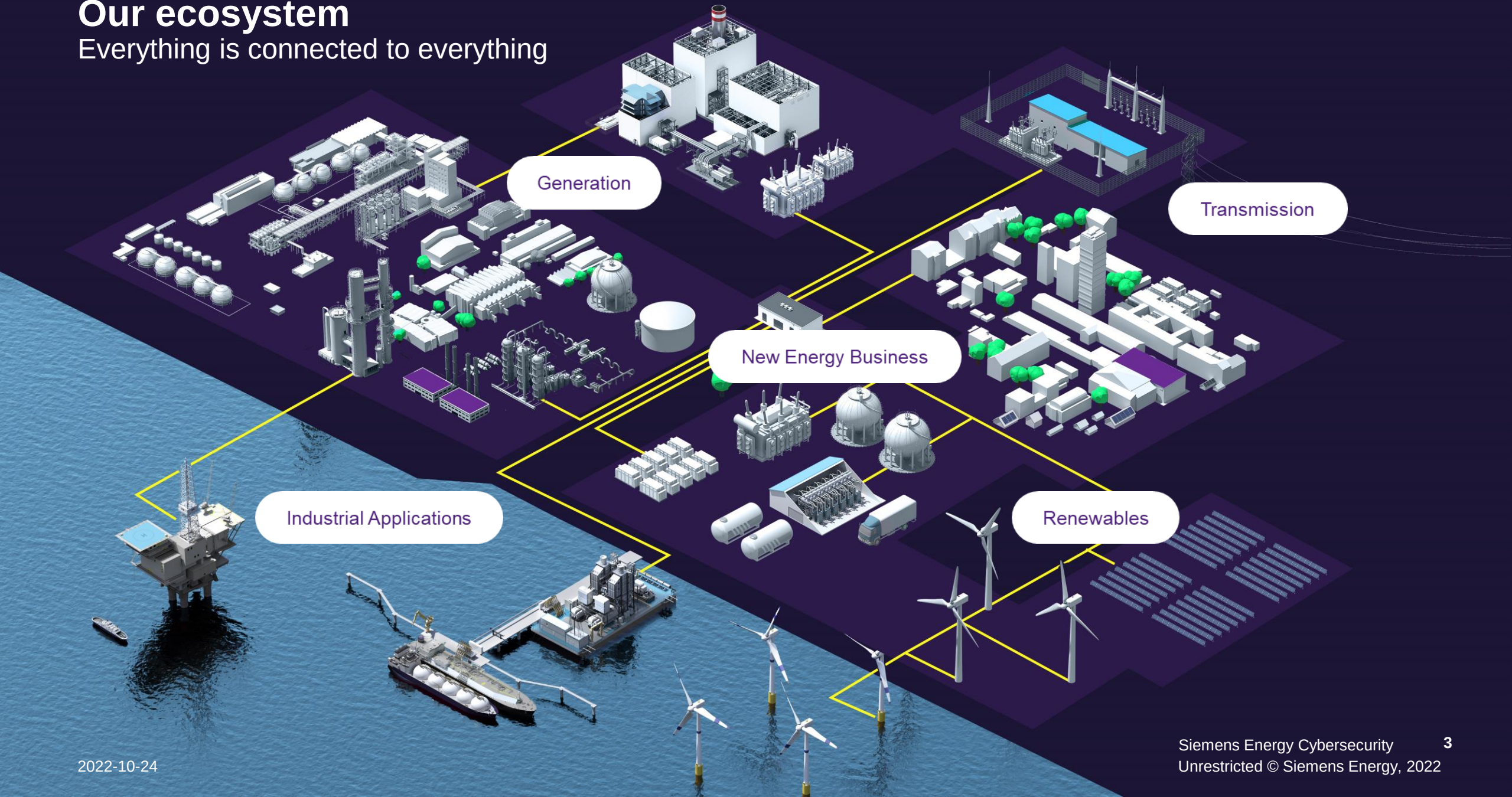
We invest around

€1bn annually in research and development.

1 Number of employees as of September 30, 2021

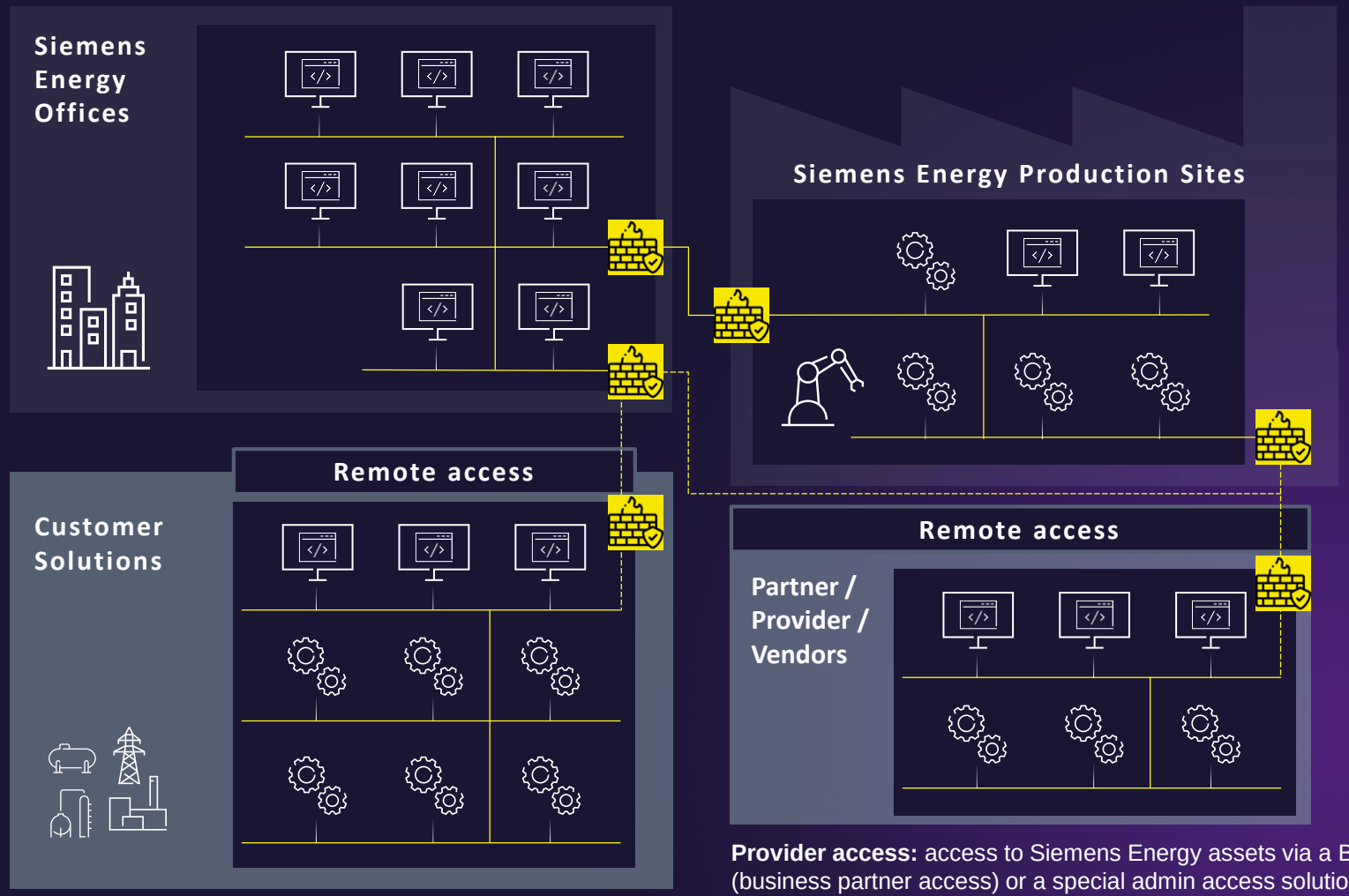
Our ecosystem

Everything is connected to everything



Everything is connected to everything

Growing digitalization and connectivity make cyber resilience imperative



Provider access: access to Siemens Energy assets via a BPA (business partner access) or a special admin access solution

Information Technology IT (e.g., PCs, servers, printers, tablets, …)

Network (e.g., switches, routers, firewalls, …)

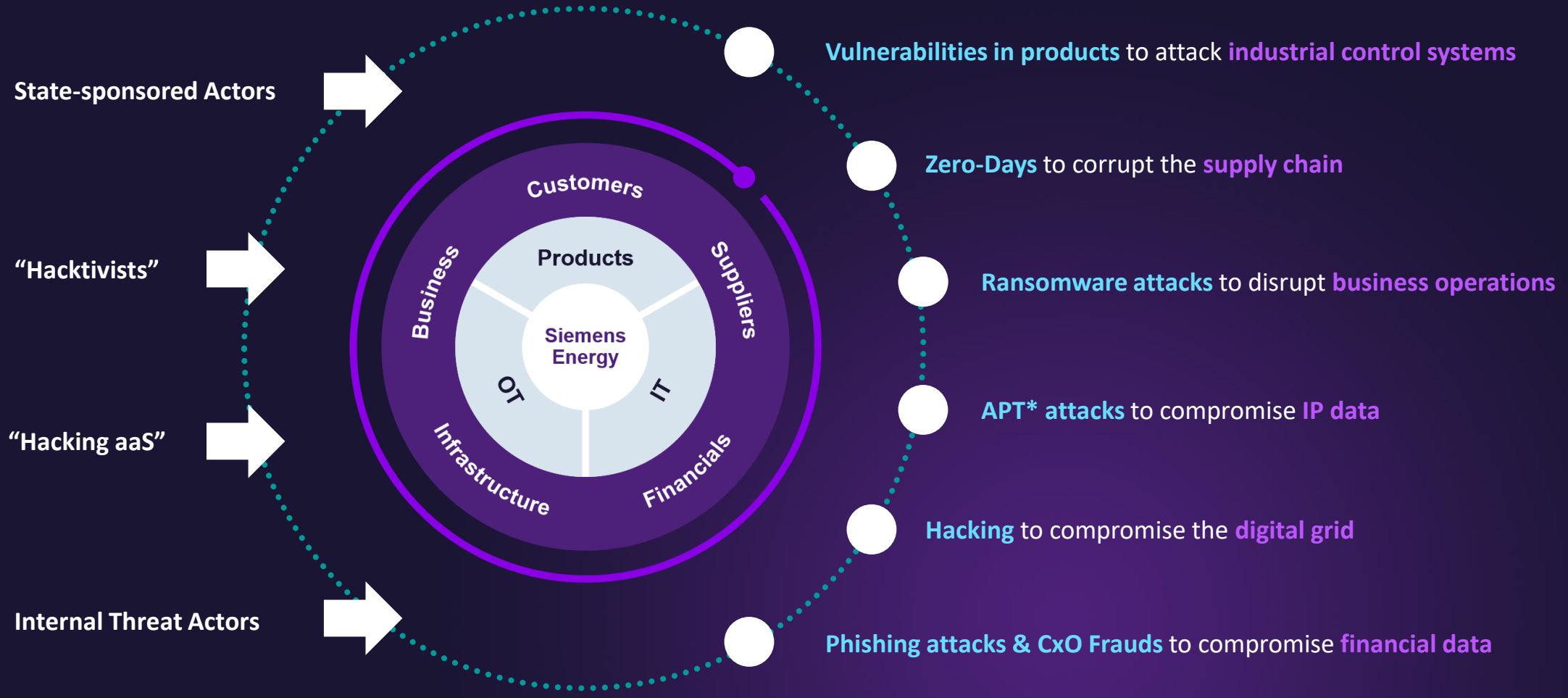
Network Separation/Protection (e.g. DMZ*, firewalls, …)

Operational Technology OT (e.g., sensors, PLCs**, cameras, embedded systems, robots, 3D printers, …)

*Demilitarized Zone; refers to a computer network with security-controlled access to the servers connected to it. **Programmable Logic Controllers

Threat landscape

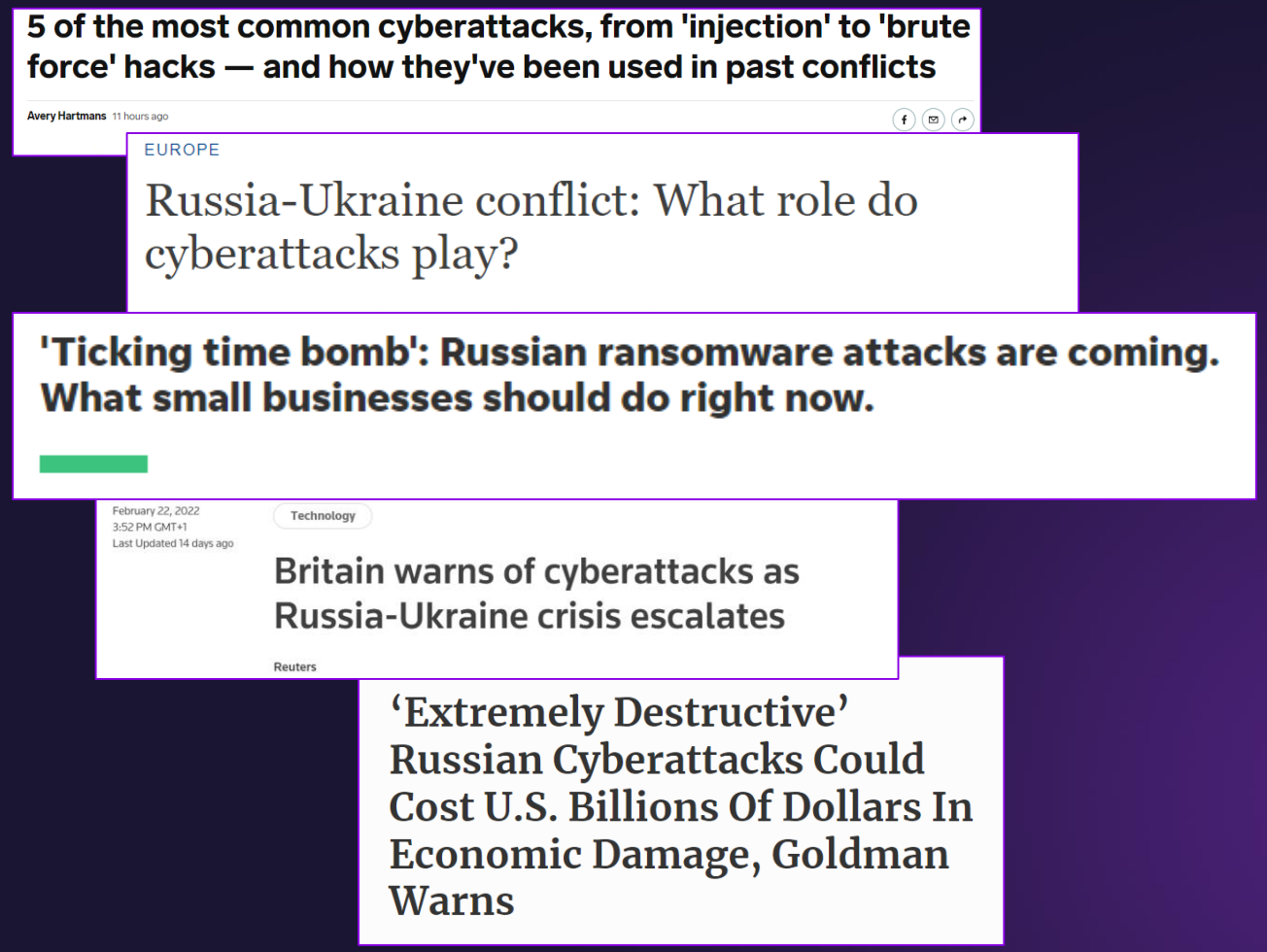
What Siemens Energy is facing



*Advanced Persistent Threat uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences. [Kaspersky 2021]

Cyber warfare linked to Ukraine war

Example for managing a dynamic threat scenario



Threat situation

- War in Ukraine accompanied by cyberattacks on Russian and Ukrainian entities, both by **"Hacktivists"** and **"state-sponsored Actors"**
- Increased threat to countries supporting Ukraine and the critical infrastructure sector
- Increase of negative sentiments for specific brands in hacker communities
- Spread of mis- and disinformation about the conflict and distorted news on social media
- Only few IT security incidents recorded in western countries
- "Hacktivists" joining geopolitical sides, e.g. call for Ukraine IT army, Anonymous threats, Killnet activities

Cyber security at Siemens Energy

Highlights of how we secure and generate value

We provide cyber resilient energy for our society!

We secure our energy assets

Business and risk value-oriented delivery

We create the energy business of tomorrow

Adaptive and customer-centric organization that breaks down the silos

We shape the cyber security ecosystem

People and innovation led growth strategy

Scope

~ 120.000 IT assets

Applications and components.

~ 80 factories

Industrial control systems of SE factories and interfaces to other assets, e.g. IoT or Cloud.

All customer-facing products and solutions

Products, solutions and services for the entire energy value chain, incl. remote access and monitoring.

~ 43.000 Siemens Energy suppliers

IT, software, components and services provided by external suppliers and business partners of Siemens Energy.

Cyber defense capabilities

- ✓ Identify and manage your **third parties** and **supply chain**
- ✓ Test your **products and processes** via black box and white box testing
- ✓ Have an up and running **Security Operations Center (SOC)** to manage your attack surface mitigation
- ✓ Generate **blueprints** for environments which already cover a secure operation
- ✓ Implement and monitor **rules, regulations** and **compliance** to legislations
- ✓ Create a foundational **cyber security awareness culture**
- ✓ **Know you scope** … or: **Know your unknown knows!**

Deep Dive: Third-Party Risk Management (TPRM)

Identifying and managing cyber risks in the supply chain

Why?

Critical Infrastructure

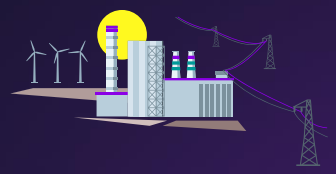
Companies operating in critical infrastructure are at a higher risk of being targeted by hackers. These attacks are often executed by exploiting weaknesses in third-party products and solutions.

Laws and Regulations

Laws and regulations in various jurisdictions worldwide mandate cybersecurity in the supply chain.

Customer Expectations

Customers and external auditors expect Siemens Energy to demonstrate existence of a comprehensive risk program.



TPRM

How?

ISO 27001 Standard

Consistent approach using the ISO 27001 standard to assess third parties' cyber security posture.

Contract Clauses

Third parties must agree to cyber security contract clauses when engaging with Siemens Energy.

Continuous Monitoring

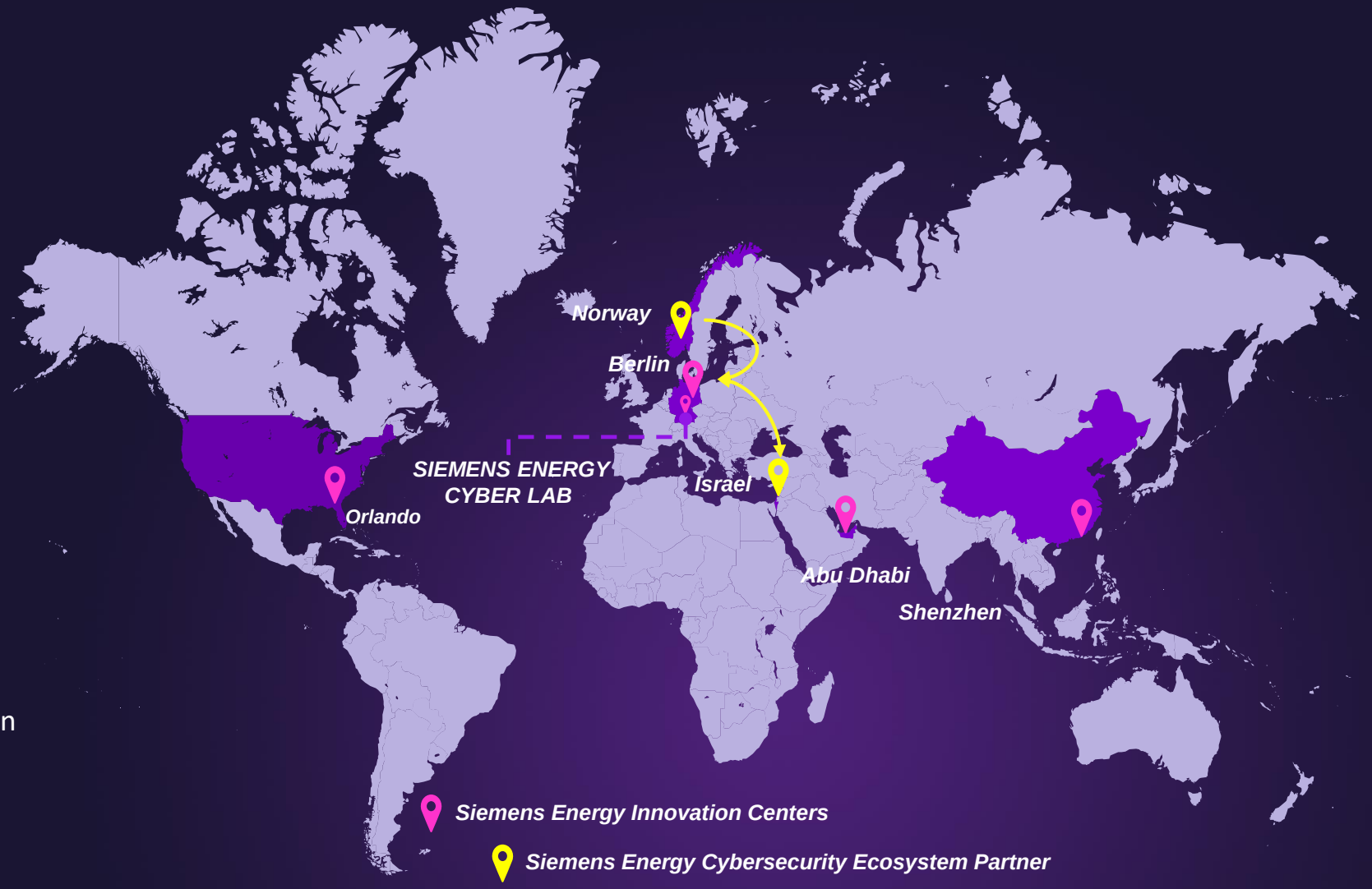
Third Parties are monitored for compliance with Siemens Energy cyber security requirements.

Third Parties are monitored for security incidents and their disaster recovery capabilities. Investigations are triggered in case Siemens Energy is affected.

Deep Dive: Value creation by managing trends & innovations

Foster strong collaboration and innovation power

- ✓ External partner collaboration
- ✓ Trend management
- ✓ Startup scouting
- ✓ Innovation funding
- ✓ Cyber innovation development
- ✓ Innovation network orchestration










We energize society



Vielen Dank.