Monthly Review

Cybersecurity news from around the world

ARTICLE

Building resilience: Sweden's new cyber-security law

Read article →

SECTRA

Newsletter introduction

As autumn settles over northern Europe, the digital landscape keeps shifting, bringing both innovation and new risks.

Sweden is preparing for the future with its 2026 cybersecurity law, while FOI's Ragnarök exercises help critical sectors practice realistic cyber scenarios. Across Europe, discussions on digital sovereignty are shaping strategies to reduce reliance on foreign tech giants.

Operational Technology Security Operations Centers (OT-SOC) are emerging as a key tool to protect essential infrastructure—ensuring societies stay resilient and ready for the unexpected.

Stay resilient. Stay secure.

General cybersecurity news

1 Don't put all your cyber-eggs in one digital basket

"In the worst case, it can also be that someone decides to 'unplug the cord' and turn off our access. What do we do then?" says Johan Linåker, senior researcher at the Research Institutes of Sweden (RISE).

The discussion regarding digital sovereignty in Europe has been going on for months, as the U.S. CLOUD Act conflicts with European data protection laws such as GDPR. Europe—and many other parts of the world—has relied on American tech giants for much of its digital infrastructure. From electronic health record systems to municipal e-services, daily operations depend on them. As Johan asks, what would happen if someone simply pulled the plug?

While there is no need to panic, awareness is growing. Countries like France, the Netherlands, Germany, and Italy are collaborating to develop solutions for public services, aiming to strengthen Europe's digital sovereignty. Beyond international collaboration, RISE points out measures such as open-source solutions, which allow an "exit strategy" to move digital operations if needed, and spreading critical services across multiple platforms to avoid putting all eggs in one basket.

These steps may not make Europe fully self-sufficient, but they help build resilience and reduce risk—ensuring that digital infrastructure can withstand unexpected disruptions.

2 Ragnarök — Preparing society for cyber storms

With cyber threats on the rise, Sweden's civil society faces growing risks. To strengthen resilience, researchers at the Swedish Defense Research Agency (FOI) have developed the "Ragnarök" exercise concept for critical sectors, including energy, transport, telecom, finance, and healthcare. Unlike traditional drills that focus solely on technical systems, Ragnarök centers on participants' needs—helping organizations practice incident response, build trust across sectors, and learn from realistic scenarios, such as simulated overload or ransomware attacks.

Flexible and scalable, the exercises can be adapted to different organizations and include clear ways to measure outcomes. "The goal is to equip the civilian part of society as part of total defense," says Malin Granath, researcher at FOI. With threats evolving and cyberattacks already affecting municipalities, Ragnarök offers a proactive path to preparedness. How ready is your organization if the unexpected strikes?

3 Italy steps onto the cyber frontline

Italy is taking a decisive step to close its long-standing gap in cyber defense. Defense Minister Guido Crosetto has announced the creation of a national cyber army—a force of 1,200 to 1,500 specialists integrating military, intelligence, and private-sector expertise. The initiative marks a strategic shift toward building an autonomous structure with both defensive and offensive capabilities.

The move comes amid a surge in cyberattacks from pro-Russian groups targeting European infrastructure since the start of the war in Ukraine. Crosetto stressed that Europe still lacks the capacity to effectively counter such operations.

Beyond defense, Italy's new cyber force signals the country's ambition to become a stronger European security actor. As cyber joins land, sea, air, and space as a key operational domain, Italy positions itself among nations advancing military modernization and digital sovereignty.

ARTICLE

The what, why and how — Of an OT SOC

Imagine a sudden silence in a water treatment plant, or a conveyor belt that stops mid-production. Often, it's just a glitch—but what if it isn't? As industrial systems become more connected, the line between IT and OT grows thinner, and with it, the risk of disruption increases.

To manage these types of risks, many organizations are turning to something long established in IT but still relatively small in the operational world: the Operational Technology Security Operations Center, or OT-SOC.

Its purpose is simple yet vital: to detect, understand, and respond to anomalies before they turn into incidents. By monitoring the networks that control physical processes like pumps, turbines, and sensors, an OT-SOC provides continuous awareness of what is happening inside an environment where downtime is rarely an option.

Modern operational systems are built for efficiency, but efficiency often comes at the cost of exposure. Connectivity enables remote maintenance, cloud analytics, and faster decision-making, all of which are invaluable—but each new connection is also a potential entry point. This is where an OT-SOC becomes essential. By constantly observing patterns and behaviors, it helps distinguish between normal fluctuations and genuine irregularities, whether caused by malfunction, misconfiguration, or malicious intent. →

Unlike traditional IT systems, which can be patched, rebooted, or replaced, OT systems often run continuously and control real-world processes.

When something fails, the impact can be immediate: water supply stops, energy distribution falters, production lines halt. The consequences are tangible—not just data loss, but societal disruption. The value of an OT-SOC, therefore, lies not only in protection but in maintaining trust. It safeguards the systems we rely on every day, ensuring that essential services remain stable, even under pressure.

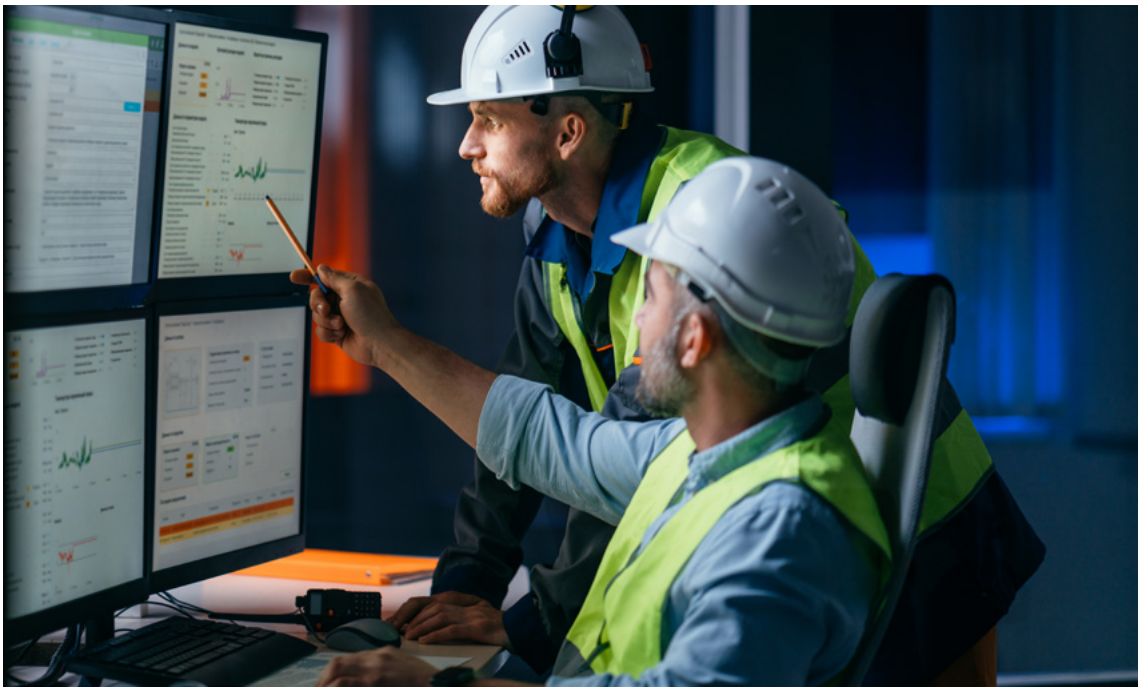
"The consequences are tangible—not just data loss, but societal disruption."

So how does it actually work?

In practice, an OT-SOC gathers signals from sensors, control systems, and industrial devices and correlates them with known threat patterns or deviations from expected behaviors. When something looks unusual, analysts review the data, separate false alarms from real risks, and guide operational teams on how to respond.

The process builds a growing understanding of how systems behave, a knowledge base that strengthens both security and efficiency over time.For many organizations, the idea of setting up such a function can sound complex, but it doesn't have to be. Some choose to build it internally, integrating monitoring into existing control rooms.

Others rely on specialized partners or companies that provide monitoring as a service. The key is to start with visibility: mapping what systems exist, how they connect, and what would happen if one stopped working. →



Monitoring can begin small, focusing on a few critical assets, and expand as insight grows. What matters most is awareness. Knowing what "normal" looks like is the first step toward recognizing when something isn't.

There is no single formula for an OT-SOC, but the goal is universal: to create a capability that not only detects threats but builds resilience. In an era when industrial systems are more connected than ever, it's not about eliminating risk entirely. It's about seeing it, understanding it, and managing it before it manages you.

Because in the end, it's not just about keeping machines running. It's about ensuring that when someone, somewhere, metaphorically "pulls the plug," the lights don't go out. ■

ARTICLE

Building resilience: Sweden's new cybersecurity law

416 pages — the proposition for Sweden's new cybersecurity law is here. Published by the Swedish government in mid-October, it outlines how the country will strengthen digital protection and oversight.

Sweden is set to implement a new cybersecurity law on January 15, 2026, aimed at achieving a high level of cybersecurity across society. The law, Prop. 2025/26:28, is part of Sweden's efforts to implement the EU's NIS 2 Directive, adopted in 2022, which sets common standards for protecting network and information systems across Europe. In short, it's about making sure that both public authorities and private operators in key sectors can withstand cyber threats and continue delivering critical services even when disruptions occur.

The purpose behind the law is clear: to safeguard digital infrastructure, protect users, and maintain trust in essential services. From government agencies and municipalities to cloud providers and online platforms, a wide range of operators will now have specific responsibilities for cybersecurity. →

The law outlines obligations for risk management, reporting, and oversight—ensuring that Sweden's digital backbone is resilient and well-prepared for modern cyber risks.

At its core, the law revolves around three main areas: security measures, incident reporting, and supervision & enforcement.

First, operators must implement robust and proportionate security measures. This isn't just about firewalls or antivirus software—it's a full-spectrum approach covering risk assessments, incident handling, continuity planning, supply chain security, secure system development, cyber hygiene, cryptography, access control, and secure communications. Even staff training and education are emphasized so that the people running systems understand the threats and know how to respond.

"Its three pillars—comprehensive security measures, fast incident reporting, and strong supervisory powers—work together to reduce risk and increase resilience"

Second, the law strengthens incident reporting and information duties. Operators are required to report significant incidents to the designated authority—sometimes within as little as 24 hours. Significant incidents are those that could seriously disrupt services, cause economic damage, or harm individuals. Operators must provide status updates, a final report, and, if needed, alert their users about threats or ongoing incidents. This creates transparency and allows both authorities and users to take timely protective actions.

Third, the law establishes clear supervisory powers and enforcement mechanisms. A designated authority will monitor compliance, conduct security audits, and perform risk scans. →

If operators fail to meet their obligations, the authority can issue injunctions, impose fines, or even ban individuals from holding management positions. Sanctions are scaled depending on the severity of the breach and the type of operator, ranging from fixed fines to percentages of global revenue for major companies. These tools ensure that cybersecurity rules are taken seriously and that noncompliance carries real consequences.

The law also includes provisions for exemptions, mainly for sensitive security or law enforcement activities, and integrates with existing regulations on electronic communication and domain administration. Public authorities, private operators of essential services, and providers of trusted digital services all fall under its scope—meaning no one can overlook the importance of securing the digital ecosystem.

In summary, Sweden's new cybersecurity law aims to fortify network and information systems, establish clear obligations for operators, and create effective oversight and enforcement. Its three pillars—comprehensive security measures, fast incident reporting, and strong supervisory powers—work together to reduce risk and increase resilience. While it won't make Sweden invulnerable to cyberattacks, it ensures that the country is better prepared to prevent, respond to, and recover from incidents. ■

Key takeaways

1. Europe is strengthening digital sovereignty with open-source solutions and multi-platform strategies.

2. FOI's Ragnarök exercises boost trust, resilience, and preparedness across critical sectors.

3. Italy is launching a 1,200–1,500-strong cyber army to enhance European cyber defense.

4. An OT-SOC monitor industrial systems, detect anomalies, and safeguard essential services.

5. Sweden's 2026 cybersecurity law enforces security measures, incident reporting, and oversight.

www.communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden, and operates through offices in Sweden, the Netherlands and Finland.

Linkedin

SECTRA