

Countdown to compliance: Is your organization ready for NIS 2 and the future of cybersecurity?

The NIS 2 Directive is reshaping the cybersecurity landscape across the European Union, with a focus on protecting critical infrastructure and ensuring business resilience.

As digital threats continue to grow, particularly in sectors reliant on both IT (Information Technology) and Operational Technology (OT), organizations must prioritize compliance to safeguard their operations. **With a looming deadline of October 17, 2024, and penalties of up to €10 million for non-compliance, the stakes are high.** NIS 2's regulatory requirements drive organizations to strengthen risk management, corporate accountability, and business continuity to protect both their systems and the communities they serve.

CYBER RESILIENCE IS A REGULATORY REQUIREMENT

Cybersecurity is not just about compliance, it's about compliance—it's about ensuring your organization can withstand and recover from cyberattacks. Is your cybersecurity strategy resilient enough to protect critical infrastructure?



67%

OF ORGANIZATIONS ARE BEHIND ON OT CYBERSECURITY

A shocking 67% of organizations haven't fully implemented NIS 2's minimum requirements for their OT environments. With only 33% implemented on average, the majority are leaving themselves with gaps in their protection. Where do you stand?



60%

HAVE EXPERIENCED AN OT CYBERSECURITY INCIDENT

Over 60% of organizations have experienced OT-focused cyber incidents, highlighting the need for robust incident response to analyze incidents and ensure continuity. Is your organization equipped to defend both IT and OT systems?



BUSINESS CONTINUITY AT RISK: LESS THAN 25% PREPARED

Fewer than a quarter of organizations have an business continuity plan in place for cyber incidents. Can your business survive an incident and prevent shutdown, or will you be unprepared?

48%

ARE TURNING TO MANAGED SERVICES FOR HELP

Nearly half of organizations are using managed security services to meet NIS 2 compliance. If in-house expertise is a challenge, are you ready to follow suit and bolster your cybersecurity resilience?

To learn more... [click here](#) →

<https://www.honeywell.com/us/en/company/ot-cybersecurity>

