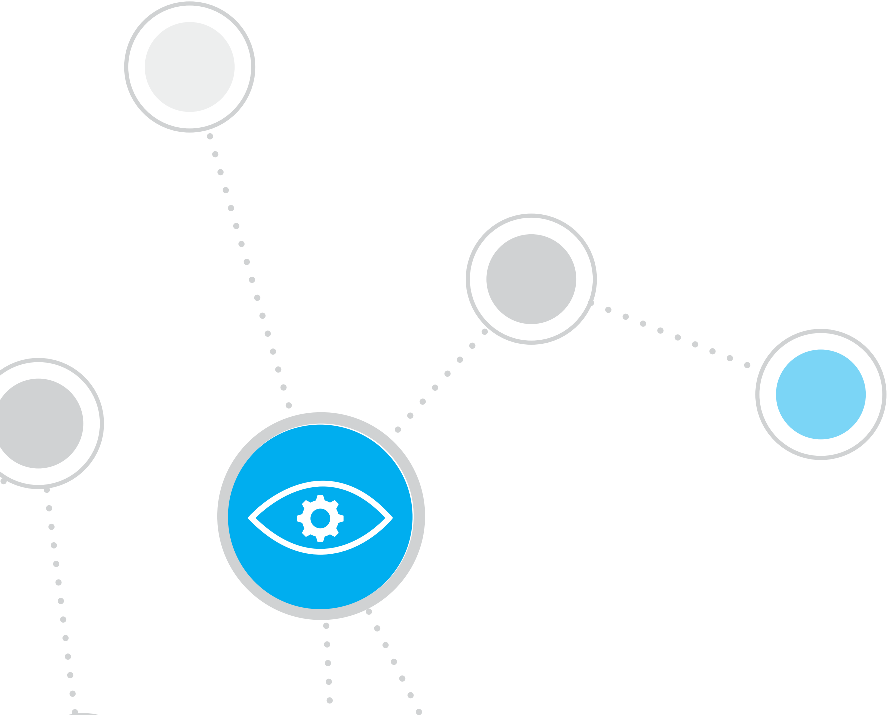
White Paper

Collaboration and Visibility: A Practical Approach to Network and Information Systems (NIS) Directive Compliance



After the implementation of the EU General Data Protection Regulation (GDPR), the EU NIS Directive now takes first place on the priority list for IT security leaders. As the NIS Directive successively becomes law across Europe, aiming to raise the security and resilience levels of critical infrastructure, providers and operators of critical and digital services—including water, electricity, healthcare, transportation and cloud services—need to get their systems and processes in order. For those responsible, this guide is the perfect starting point, offering practical advice from expert practitioners.

As with GDPR, it is up to each organisation to translate the requirements of the legislation to their own environment. This document covers the four key areas of consideration for organisations planning to implement processes and tools to adhere with the NIS Directive.

Collaboration

To successfully achieve NIS Directive compliance, operators and providers need to break down organisational silos in order to encourage the right levels of collaboration, communication and accountability. “Ensure the risk is owned by the right person,” advises Arqiva CISO Denis Onuoha. “Too often, you have an IT director owning the risk for a system [when] it should be owned by the board. They need to own it, understand it and make the right decisions.”

> **Too often, you have an IT director owning the risk for a system [when] it should be owned by the board. They need to own it, understand it and make the right decisions.”**
>
> — Denis Onuoha, CISO, Arqiva

Michael Cock, group IT manager at Sutton and East Surrey (SES) Water, asserts that providers and operators need the “right people in all the right departments” to understand their role in delivering secure processes and knowing what steps to take in the event of an incident.

Collaboration goes even further, however. It means working together with the broader industry, with other parts of critical infrastructure (irrespective of sector) and with competent authorities.

“We’ve done a lot of things externally,” SES Water’s Cock adds, pointing to active collaboration among members of Water UK, his industry’s membership organisation. “We have a Water UK forum that helps us drive toward common standards and shares a lot of information about the technology available. We are not only working with colleagues in our own industry but also across all critical national infrastructure, so the approach is consistent and efficient and makes the UK national infrastructure a hard target.”

Finally, collaboration means working with the supply chain. “We all live in a very complex supply ecosystem, and you can’t pass this off to your supplier,” says Dominic Wood, head of global MFU & HMG security, BT Security.

Arqiva’s Onuoha agrees. “If your supplier screws up, I’m sorry but this sits with you,” he says. “Where possible, you should audit your supply chain because it can quickly turn into a vulnerability for your organisation.”

Visibility

> **Security starts with visibility,"**
>
> — Markus Handte,
> director, systems engineering
> EMEA at ForeScout Technologies

Security starts with visibility," says Markus Handte, director, systems engineering EMEA at ForeScout Technologies. Ensuring internal and external systems are as secure as possible requires a real-time, holistic and continuous approach to data monitoring. With such an approach, operators and providers can view contextual information about people, processes, systems and devices, allowing them to spot unauthorised access and activity.

Rather than implementing disparate solutions for asset discovery and audit, a single tool is better able to review every part of the process and reduce reliance on manual intervention.

Real-time visibility of a whole estate is not easy, concedes Gordon Morrison, director of EMEA government affairs at Splunk, but it is essential to fulfill compliance needs. "Utilise the value of all the data you have in your organisation, visualise it and link it to all the open source information you can," he advises.

People, Skills and Automation

The NIS Directive requires upper-level security professionals and executives to meet the demands of the regulation.

"Particularly for smaller teams," says SES Water's Cock, "one of the hardest things is working out how we can man the tools. We're very good at going out finding the right solutions—using tools like ForeScout—but you've got to have the right skills to use those as effectively as possible."

When people with the right skills are not present in-house or cannot be recruited easily, a way of integrating existing solutions should be considered. "There are technologies on the horizon such as machine learning and automation," notes Splunk's Gordon Morrison. "These do have the potential to reduce dwell time and help to get to [the intelligence] in real-time."

Security 101

While the NIS Directive makes fresh demands on organisations, those that already have a pragmatic, risk-based approach to security will succeed. Those that don't should adopt one fast.

"You have to start with what's in scope," advises BT Security's Wood. "This is a regulation, so you're going to be challenged to prove you've got an assurance regime around the assets that fall in scope."

Next, apply sensible and tested security techniques and solutions, including security information and event management (SIEM), limiting access to data and systems, patching and – says ForeScout's Markus Handte – a network segmentation approach. "Find a way to segment critical systems and data from other systems," he says.

Network Segmentation

Network segmentation will allow you to contain any attacks and prevent threats from spreading.

Stuart Peters, head of EU Cyber Security Regulatory Policy at the UK's Department for Digital, Culture, Media & Sport (DCMS), urges organisations to speak to their competent authority and to review national authority guidance – the National Cyber Security Centre's NIS security guidance and cyber-assessment framework in the case of the UK. "It provides a very good understanding of where you should be looking," Peters says.

NIS Resources available:

NIS Guidance:
https://www.ncsc.gov.uk/guidance/nis-guidance-collection

Cyber Assessment Framework:
https://www.ncsc.gov.uk/guidance/nis-directive-cyber-assessment-framework.

Overview of Competent Authorities by industry:
https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-uk

The next step is to identify which systems are central to the critical services provided. This means looking beyond industrial control systems. Why? Because the NIS Directive is based on the provision of your service, and, if billing software, for example, is a potential point of failure, it's as important to secure this service as it is to secure operational technology. "You need to look at the entire system and have a good understanding of where a failing in one could impact the service you are providing."

A final word of advice? "Don't panic," says Peters from DCMS. "The main thing is to have a plan, demonstrate how you reach compliance, demonstrate how you are going to get to where you want to be. Remember our ultimate aim is to deliver more secure critical services. Authorities are not there to punish operators."

The NIS Directive gives your security leaders an opportunity to establish an ongoing process of improving your security posture, staying up to date and driving more secure services for your customers—all of which will help your CISO justify investment and resource allocation.

You don't have to do this alone: work with industry colleagues, experts and vendors to implement the NIS Directive consistently and efficiently. You can get in touch with ForeScout to discuss how you can optimise your processes and put measures in place to meet NIS requirements:

Phone: +44 20 38 654 437

Email: uk@forescout.com

Get started with this NIS Checklist:

1. **Take a holistic approach to compliance.** Ensure you have a complete view of systems and processes. Use relevant data and solutions to shine a light on your entire infrastructure.
2. **Identify potential skills gaps.** Fill those gaps where you can. Explore machine learning and automation alternatives as appropriate.
3. **Break down organisational silos.** Ensure that the right people in the right departments know what's expected and that they are on board. Don't just leave the responsibility with the IT Director or CISO.
4. **Break down industry silos.** Join forces with sector competitors and share best practices.
5. **Engage with competent authorities.** Understand what they expect from you. They are there to assist.
6. **Audit your supply chain.** Third-party suppliers are a potential point of weakness. Identify issues upfront, and address them.
7. **Educate the board.** It's where the buck stops and where NIS knowledge is likely to be most limited. Ensure understanding, responsibility and buy-in.
8. **Test your procedures.** It's no use filing contingency plans away to collect dust. Make sure they work in practice.
9. **Embrace the business opportunity.** Don't treat the NIS Directive simply as a compliance exercise. Use it to increase customer engagement and improve operating efficiency.
10. **Don't panic.** This is not a game of "gotcha." The NIS Directive is designed, first and foremost, to keep critical infrastructure secure.

Learn more at
www.ForeScout.com

About ForeScout

ForeScout Technologies, Inc. is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of March 31, 2018, more than 2,800 customers in over 80 countries improve their network security and compliance posture with ForeScout solutions.

*As of March 31, 2018

ForeScout®

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Fax +1-408-371-2284