

Aligning Your Security Program with the NIS Directive (Companion Piece to “Enabling NIS Directive Compliance with Fortinet for Operational Technology”)

Written by **Matt Bromiley**

July 2020

Sponsored by:
Fortinet

Introduction

Network and Information Systems (NIS) provide essential functions to citizens and businesses. They also play an important role in the economic and societal development of any nation. Attacks on these systems can be detrimental to any of these groups and can have long-lasting effects on both direct and third parties affected by the incidents. Consider, for example, recent attacks on healthcare systems during the COVID-19 pandemic that brought hospitals to their knees and limited their ability to provide critical care for their patients.¹

In July 2016, the European Parliament adopted the NIS Directive (referred to as “the Directive” throughout this paper), which addresses the security of network and information systems.² The Directive was adopted to establish legal measures to increase cybersecurity capabilities within the EU across its multiple Member States and various operators. The Directive also set forth best practices to encourage better cyber risk mitigation and incident identification and notification.

In this whitepaper, we explore various measures of the Directive and how to align your organization’s security posture with these measures. The Directive does not offer a comprehensive list of “must-dos,” unlike regulations such as the North American Electric

The NIS Directive does not offer a comprehensive list of “must-dos,” unlike regulations such as PCI DSS or HIPAA. Instead, it clarifies the primary operators at risk and what steps to take to minimize their cyber risk.

¹ “Cyber-Attack Hits US Health Agency Amid Covid-19 Outbreak,”
www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

² “Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016,”
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

Reliability Corporation Critical Infrastructure Protection (NERC CIP) or NIST. Instead, it clarifies the primary organizations at risk—referred to as *operators of essential services (OESes)* and *digital service providers (DSPs)*. The Directive also identifies what steps should be taken by these organizations to minimize their cyberrisk. It also establishes member-specific resources to help promote cyber awareness, security, and incident handling within each Member State.

We have identified the following as core concepts to Directive compliance:

- Risk mitigation among organizations (operators and providers) that provide important economic and societal benefits to the EU
- Incident identification and reporting among operators, providers and Member States
- Establishment and/or improvement of information security capabilities of Member States (and, as a byproduct, the overall EU)
- Collaboration within and among Member States and the EU

Many national and international guidelines provide ideal goals but leave it to the organizations themselves to achieve their goals. Thus, it is prudent to ensure that your organization is aware of its classification and prepared for security requirements. The Directive charges the various Competent Authorities with identifying security requirements. As you read through this whitepaper, we encourage you to consider the following:

- Does the Directive affect my organization?
- If so, are we compliant with its requirements?
- What steps do we need to take to become compliant?
- How does our security posture align with the goals of the Directive?
- Is my organization regulated? If so, by which Competent Authority?

With these thoughts in mind, we also encourage you to consider your current security implementations and how they assist you in solving the aforementioned concerns. As much as this guide is meant to inform you about Directive adherence, it is also intended to give you a reason to evaluate the tools in your environment and their contribution to your overall security posture.

To help you use this guide, we have inserted multiple “NIS Checkpoints.” These checkpoints are an opportunity for you to consider how your current implementations, technology and resources are either assisting or hindering your compliance with the Directive. We will provide guidance where appropriate so you can apply our recommendations to your own organization.

Finding Your Place Within the Directive

Before we examine the core concepts of the Directive, it's crucial to understand the scope of organizations, or operators, to which it applies. Data regulations are often

industry-blind, focusing on the requirements for processing a certain type of data (for example, power utilities in the EU are often subjected to IEC 62443 standards).

Conversely, the Directive begins with geography, in the form of Member States, and then zeroes in on the services provided by organizations within each Member State. Organizations are subsequently classified into operators of essential services and digital service providers. Figure 1 provides a high-level diagram of the types of organizations to which the Directive applies. We will subsequently examine each type in detail.

Understanding how your organization is classified by the Directive will be paramount to considering your security posture and any improvements your organization may need to make.

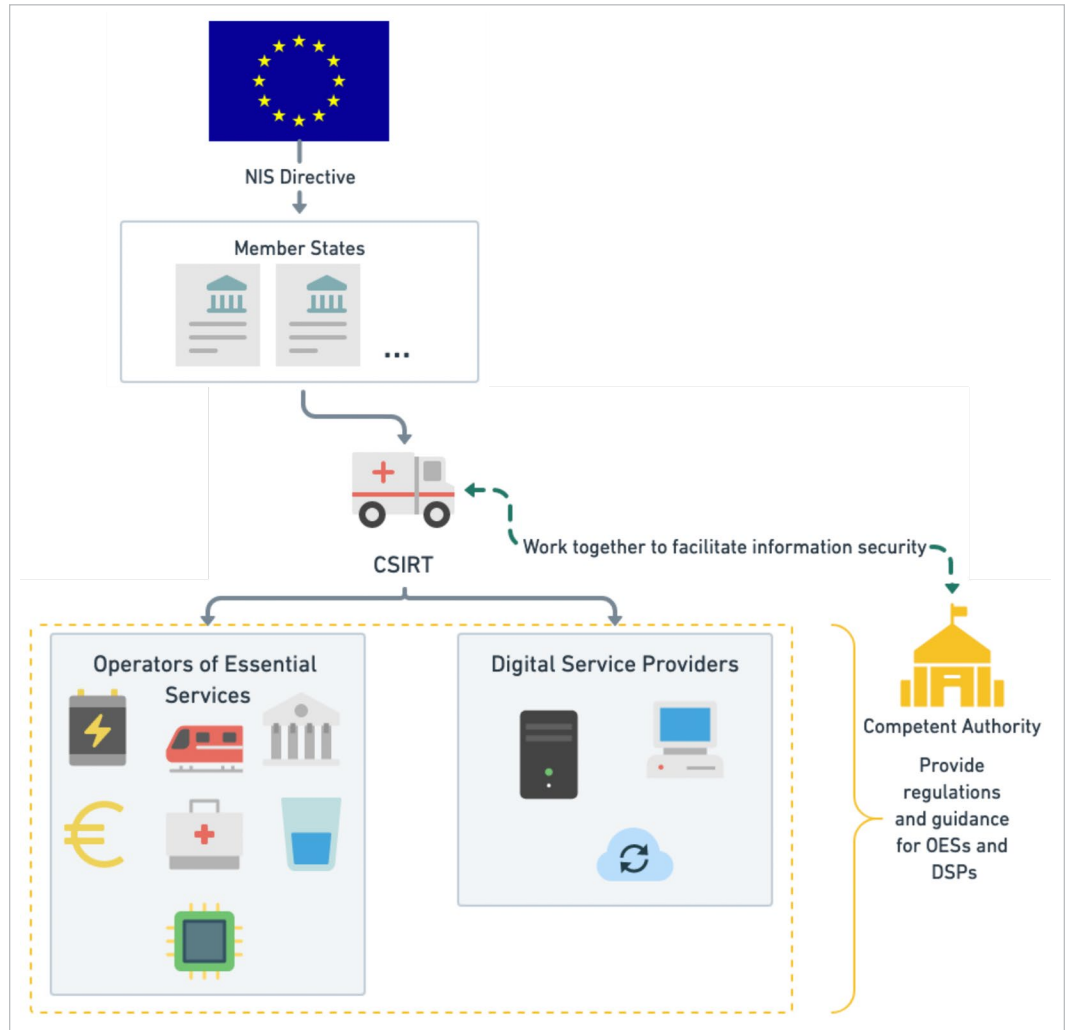


Figure 1. NIS Directive Flow of Responsibility

Member States

The Directive first recognizes that cybersecurity awareness and protection begin with each Member State of the EU, highlighted in Figure 2. Note that the UK will keep the Directive in place after Brexit, and as such they are subjected to the concepts we identify in this whitepaper. The Directive tasks Member States with multiple high-level requirements:

- Define a national strategy on network and information systems security, including policy and regulatory measures to maintain a high level of cybersecurity preparation and protection.

- Establish computer security incident response teams (CSIRTs) to help facilitate cyber protections throughout the Member State and among the EU countries.
- Utilize CSIRTs to facilitate cooperation between operators in each Member State, as well as among different Member States.
- Ensure that incidents are scoped and reported correctly, including their impacts on the Member State(s) and EU, if applicable. The Member State is also tasked with determining the significance of cyber incidents and measuring their effect on parties involved.

Overall, the Directive declares that protection of network and information systems is of both EU and national interest, and charges each Member State with addressing those concerns. It recognizes that most NIS are privately operated and encourages cooperation between private and public sectors.

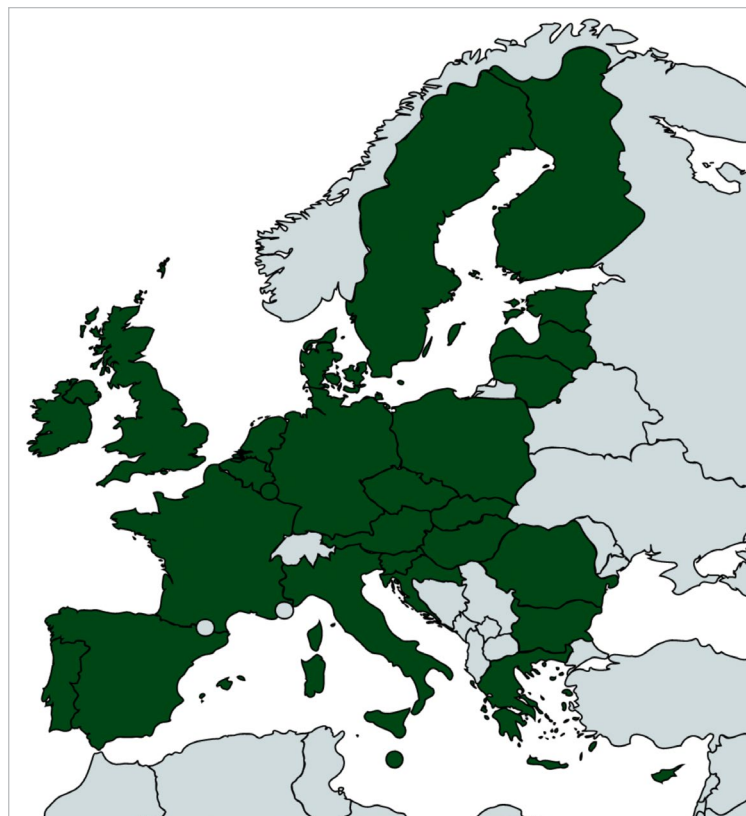


Figure 2. EU Member States as of June 2020

NIS Checkpoint No. 1

The NIS Directive highlights the requirement for cooperation among multiple groups:

- CSIRTs of the EU Member States, actively supported by the European Union Agency for Cybersecurity (ENISA)
- Organizations and Member States, mainly to be facilitated by their Member-respective CSIRTs. In the event of an incident, you should expect cooperation from the national group(s) tasked with implementing Directive standards.

Compliance Check: As an organization with business in a Member State or as a Member State CSIRT, you will be expected to cooperate and provide incident details to the appropriate authorities. For national CSIRTs, ENISA will be a valuable resource for collaboration and incident coordination. For OESes and DSPs, the national CSIRT is a valuable resource, helping to establish best practices and guidelines for protection of network and information systems.

Implementation Recommendation: Has your organization identified and formed relationships with the appropriate national or international teams? They can help identify Member State-specific requirements and/or best practices.

Note: We will discuss incident identification requirements in a subsequent section.

Helping Hands: The NIS Directive requires each Member State to establish its own CSIRT. These CSIRTs are meant not only to help establish standards for the Member State but also act as important sources of intelligence, communication and cooperation for the organizations within each nation.

Organizations

The Directive also defines the organizations or entities that do business in each Member State. These various organizations, deemed as either “operators” or “providers,” are classified by the types of services provided to their customers and/or to the economies of the Member State(s). In our opinion, this classification presents several benefits to organizations doing business in the EU:

- It is highly likely that an organization doing business in the EU provides multiple essential and/or digital services, which allows the respective organization to be subject to multiple security controls *per* service, in turn offering a more holistic defense.
- It is also highly likely that an organization operates in more than one Member State. The Directive states that the organization must choose a primary locale of operation.
- The Directive identifies sectors that are *critical* to the economic and/or societal needs of a Member State. In the event of an incident on a network and information system, the affected operator or provider can utilize the resources of the national CSIRT(s) and other organizations.
- Sector-based classification also implies that the Directive represents protections that should be implemented for both IT and OT environments—not one or the other.

Food for Thought:
In organizations where regulations and/or protections are assessed on types of data, not services, security controls typically apply *only* to the subject data type. By assessing based on the services they provide, the NIS Directive forces more holistic protections for operators and providers.

Operators of Essential Services

The first subset of public and/or private organizations is *operators of essential services* (OESes). The Directive identifies seven key sectors and subsectors, where appropriate. Figure 3 outlines these sectors.



Figure 3. Diagram of Essential Sectors, as Defined by the NIS Directive

As mentioned earlier, it is possible that OESes find themselves providing multiple services, operating in multiple sectors, and/or providing services to multiple Member States, leading to increased cooperation among the OESes and the respective CSIRTs.

If your organization falls outside of the sectors defined above, the Directive also allows for voluntary incident disclosure from non-OESes without being subject to OES requirements.

Digital Service Providers

The second grouping recognizes organizations that provide digital services, and are aptly referred to as *digital service providers (DSPs)*. This designation includes organizations that are:

- Online marketplaces
- Online search engines and/or
- Cloud computing services

The Directive also states that digital services are vital to economic and societal stability in Member States and that they should fall under NIS protections. There is a stipulation, however, that DSPs should have representatives in Member States in which they do business, as well as a head office in a “primary” Member State.

NIS Checkpoint No. 2

The NIS Directive first sets requirements for each Member State, primarily dictating the creation of CSIRTs and establishing policies and best practices. It further breaks businesses and organizations into either OESes or DSPs, depending on the types of service(s) they provide. Thus, if you operate within the EU, it is paramount to identify which Competent Authority is in charge of the NIS Directive application. Once identified, you must adhere to cybersecurity standards put forth by said Competent Authority.

Compliance Check: Utilize the information provided above to identify key sectors as defined by the Directive. Does your organization align with any of these? Are you unsure about a particular service?

Implementation Recommendation: If you are already aware that your business is classified by a certain sector, there is likely Member State-specific guidance available for that particular sector. Note that there should also be a national CSIRT you can contact for support—one of their mandates is to facilitate nationwide cooperation and collaboration.

What Does This Mean for My Organization?

The Directive defines the competent authorities and sectors of industry and business that are critical for economic and societal stability. Identifying where your organization aligns within the various sectors defined by the Directive will help identify the support available to your team(s), the policies and requirements that you may be subject to, and the best practices as defined by the Member States. For example, a Member State CSIRT will be relying on ENISA and helping to facilitate internal national coordination. An OES or DSP, on the other hand, will be relying on the respective Competent Authorities within the States where it operates.

After confirmation that your organization is or is not a national CSIRT, OES or DSP, the next step in your assessment should be focused on ensuring adherence with the standards.

Key Components of NIS Directive Compliance

As mentioned earlier, understanding how your organization is classified by the Directive is only half the battle. After this is done, the next step is to identify the Member-specific requirements, as established by the appropriate authorities. The Directive also allows for Member State CSIRTs to establish best practices and encourage private organizations to adhere to those standards. We've compiled the following list of best practices and standards that, in our experience, can help lead to a robust security architecture:

- ISO 27001, 27019, 27032
- IEC 62443
- IEC 62351
- IEEE 1402-2000
- NIST SP 800-82
- NISTIR 7628
- NERC CIP

Always double-check with the Competent Authorities on their recommendations. It is beyond the scope of this whitepaper to cover Directive requirements for each and every Member State. Based on our experience with NIS security and incident handling, however, there are key components to any robust security posture that can help achieve the incident handling and risk mitigation concerns addressed by the Directive.

Identifying Critical Assets and Networks

Good security posture and risk mitigation begins with visibility into the environment. After all, you cannot protect what you cannot see. Additionally, as your organization profiles which Directive-defined sectors apply to your organization, visibility into the environment will help you correctly assess operations and report to the Member State CSIRTs appropriately. As we will explore in subsequent key Directive components, correctly detecting and scoping incidents are *absolutely essential* for incident handling and reporting, per the Directive. However, visibility into environments is often easier said than done.

The first step an organization should take toward achieving compliance is addressing any visibility gaps in monitoring, detection and response capabilities. The current security posture of many organizations around the globe is unfortunately a mishmash of technologies acquired over the years, often with little comparison of visibility. This kind of setup simply won't work because failure to detect and/or correctly report an incident under the Directive can lead to penalties and fines as imposed by the Member States.

Another consideration for this space is a platform-based, or holistic, security solution. Having multiple tools that intertwine "out of the box" to provide both network and endpoint visibility will be significantly more efficient as a drop-in solution as opposed to implementing multiple vendors that may or may not work together.

Correctly detecting and scoping incidents are absolutely essential for incident handling and reporting per the NIS Directive.

The time is right to evaluate your current security posture and determine whether you have appropriate visibility into the environment. It’s also time to push your security controls beyond simple visibility. Correctly assessing threats to the environment relies on correlation between the various elements of your enterprise, data enrichment with threat intelligence and effective incident response capabilities, which we’ll examine next.

NIS Checkpoint No. 3

Having visibility into your organization’s entire environment is crucial to effective security and protection of network and information systems. Security solutions that offer partial insight into your environment do not align with the needs of the Directive.

Compliance Check: Examine your current security posture. Do you have visibility gaps in any areas of the environment? Is there a quick fix or do you currently have solutions in place that do not afford holistic visibility?

Implementation Recommendation: Piecemeal or solution-by-solution security implementations may be providing redundant visibility in some areas and gaps in others. Consider looking at a platform-based or holistic security solution that offers unified awareness of and visibility into the environment. Remember that visibility comes in the traditional forms of network *and* endpoint—don’t ignore either element.

Incident Handling and Reporting

The Directive spends a good amount of text discussing incident handling and reporting requirements for Member States, OESes and DSPs. One of the primary goals of the Directive is to facilitate a means by which organizations can detect and report on incidents in an effort to increase incident awareness and promote public safety. This goal also goes hand-in-hand with the environmentwide visibility previously mentioned.

In addition to incident reporting requirements, the Directive provides guidelines for relevant parties to determine the significance of incidents. These qualifiers are to be used by OESes and DSPs to help facilitate quick and rapid reporting, without undue delay, to the relevant CSIRT(s) for further handling. Incident notifications should also include any possibility of cross-border impact, such as an organization that operates in multiple Member States.

Figure 4 provides a quick comparison of the factors contributing to the significance of an event, to be used by OESes and DSPs for reporting.

You’ll notice in Figure 4 that incident scope, duration and impact are critical for both OES and DSP incident declaration. This goes hand-in-hand with our assessment that

OESes	DSPs
<ul style="list-style-type: none">■ Number of users affected by essential service disruption■ Duration of the incident■ Geographical spread in area affected by the incident	<ul style="list-style-type: none">■ Number of users relying on the affected service■ Duration of the incident■ Geographical spread in the area affected by the incident■ Extent of the service disruption■ Extent of the impact on economic and societal activities

Figure 4. Key Factors in Determining Incident Significance for OESes and DSPs

environmental visibility is crucial to Directive compliance—your security teams must be able to accurately and swiftly detect incidents in essential networks and scope them. Simply detecting incidents is not enough for the Directive, however. Organizations must also be able to respond to incidents swiftly and effectively, confirming the need for a holistic security program. Incidents can take multiple forms and have multiple sources and entry vectors. Thus, an advanced and holistic security platform must be augmented with data enrichment and include internal and external threat intelligence capabilities.

NIS Checkpoint No. 4

Visibility goes hand-in-hand with swift incident detection and scoping.

Compliance Check: Following up on Checkpoint No. 3, if you do not have visibility gaps in your organization, the next step is to assess the capabilities of your current security implementations. Do they offer incident handling and response capabilities? Can you detect and neutralize an incident seamlessly or is there a gap in response capabilities?

Implementation Recommendation: If you need to work on increasing visibility, be sure to choose security controls that can offer advanced response capabilities. If your environment has visibility, perform thorough tests to confirm that your current controls provide incident response capabilities. Ensure also that they provide data to simulate accurate incident reporting capabilities to the respective CSIRT(s).

Speaking of threat intelligence, another Directive task required of the respective Member State CSIRTs is to help facilitate the collection and transmission of threat intelligence within the State and between States. For OESes and DSPs, this provides an excellent resource for relevant, actionable threat intelligence from trusted sources. These sources should be utilized and integrated into your security setups, in addition to any third-party intelligence sources that may also be procured.

NIS Checkpoint No. 5

Threat intelligence, both internal and external, is critical to detecting advanced threats in your organization. The Directive stipulates that the Member State CSIRTs are responsible for facilitating information sharing both internally and externally and may rely on the resources of the EU to help provide actionable intelligence to OESes and DSPs.

Compliance Check: Does your current security implementation both capture and utilize threat intelligence? Knowledge of ongoing active threats and actors, as well as previous incidents, is paramount to advancing your security capabilities.

Implementation Recommendation: Considering a platform or an add-on that allows for the integration of threat intelligence from one or multiple sources? As mentioned earlier, EU CSIRTs are sources that can be used for threat intelligence and incident awareness. You can also rely on third-party sources that provide real-time intelligence about the threats they observe.

NIS Risk Mitigation

Another key concept from the Directive, one that is perhaps most prevalent throughout the entire document as it was published, is the mitigation of risk by Member States, OESes and DSPs. This mitigation is, of course, often easier said than done. In our opinion, the Directive is asking for the various parties to consider ways to minimize successful intrusions into their networks. Stringent incident reporting requirements are useful, but they are even better if rarely necessary.

To accomplish that, the Directive places policy establishment, training requirements and formation of best practices in the hands of each Member State, its respective CSIRT and other NIS governing parties. The Directive also realizes that many organizations may already be following best practices and standards (identified previously in this paper), which can easily be adopted by the respective states.

We feel this responsibility presents a twofold challenge to OESes and DSPs in multiple Member States. An organization may provide different types of services, some that fall under different scrutiny or direction from the Competent Authorities than others. In our opinion, this presents an opportunity for the OES or DSP to choose the “highest” requirement, thereby going above and beyond the minimum requirements. The Directive states minimums but fully accepts that many organizations may wish to do more than that.

Aside from the requirements put forth by Competent Authorities, it’s prudent to prepare your organization for incidents of all sizes and severities as one normally would without the Directive. This preparation includes these typical best practices:

- Having an incident response plan in place
- Performing periodic internal and external assessments of your network(s)
- Tracking internal security metrics to provide insight into security operations

NIS Checkpoint No. 6

Risk mitigation from the NIS Directive perspective focuses on preparation in minimizing risk and attack surfaces and possibilities. In the event that an NIS incident occurs, the Directive expects organizations to report details and provide relevant information so that the respective CSIRT(s) can assess the significance of an event and evaluate its impact on the EU. Typical security posture best practices include having an incident response plan in place, collecting security metrics and performing periodic assessments.

Compliance Check: Does your organization have the above in place? Can you locate them? Are the teams empowered to act upon them? How would your team respond to an incident today, given the requirements of the Directive?

Implementation Recommendation: Evaluate the current state of risk mitigation with regard to your security team. Aside from technology, what measures are in place to ensure your team(s) can detect, respond to and report security incidents effectively?

Take Action Now

In this whitepaper, we examined various aspects of the EU's Directive and explored the core concepts put forward in 2016 by the EU. It's clear that the goal of the Directive is to enhance the defense of cybersystems and advanced cybersecurity in the EU, a benefit realized by all Member States. The Directive focused on the following five core competencies:

1. Creating an overall increased level of cybersecurity in the EU by establishing and enforcing best practices
2. Establishing national cyber policies and CSIRT(s) for each Member State
3. Increased cooperation between Member States and entities within each state
4. Guidelines for incident handling and reporting to facilitate the swift disclosure of incidents affecting services essential to economic and/or societal success
5. Guidance on risk mitigation so as to minimize the number of incidents by achieving a high state of security posturing

If your organization has operations in one or more of the EU Member States, it is vital that you assess your place within the various sectors as defined by the Directive. It's equally important to ensure that your organization understands the requirements it may be subject to, with respect to best practices, incident handling and expected levels of communication.

It is clear that the Directive was designed with the concept of "All for One and One for All" in mind. If all Member States of the EU, and all organizations that do business within the EU, adopt and adhere to advanced cyberrisk mitigation and defense mechanisms, the entire EU will benefit. Furthermore, the Directive called out the issue of information sharing among Member States, which serves to advance cybersecurity awareness and defense.

The Directive provides an example of an ideal state of security but one that is easily attainable with the right guidance and investment.

NIS Checkpoints

Throughout this whitepaper, we inserted multiple NIS checkpoints, which were designed to encourage our readers to consider their own security postures compared to the guidelines set forth by the Directive. These checkpoints have been condensed into the following checklist, to be used by your organization as guidance for its next steps.

#	Category	Implemented?	Next Steps
1	Identify key Members of national CSIRT(s) and begin to build relationships with them.		
2	Identify where your organization aligns with the sectors and/or business types defined by the Directive.		
3	Examine your current security technologies to confirm visibility of the entire enterprise.		
4	Do your security controls provide incident detection, as well as response and remediation capabilities?		
5	Does your organization utilize threat intelligence? Evaluate where it is sourced and what value is derived from the intelligence provided.		
6	<p>The Directive's risk mitigation focuses on preparation. Ensure that your organization has the following in place, and that they are updated:</p> <ul style="list-style-type: none"> • Incident response plan • Tracking and reporting of security and risk metrics • Periodic internal and external risk and security assessments of the enterprise 		

About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor, teaching [FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics](#) and [FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response](#).

He is also an IR consultant at a global incident response and forensic analysis company, combining his experience in digital forensics, log analytics, and incident response and management. His skills include disk, database, memory, and network forensics, incident management, threat intelligence, and network security monitoring. Matt has worked with organizations of all shapes and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

