MASTER OF SCIENCE IN ENGINEERING

TSM_SecIndOpT

Incident Response (II)

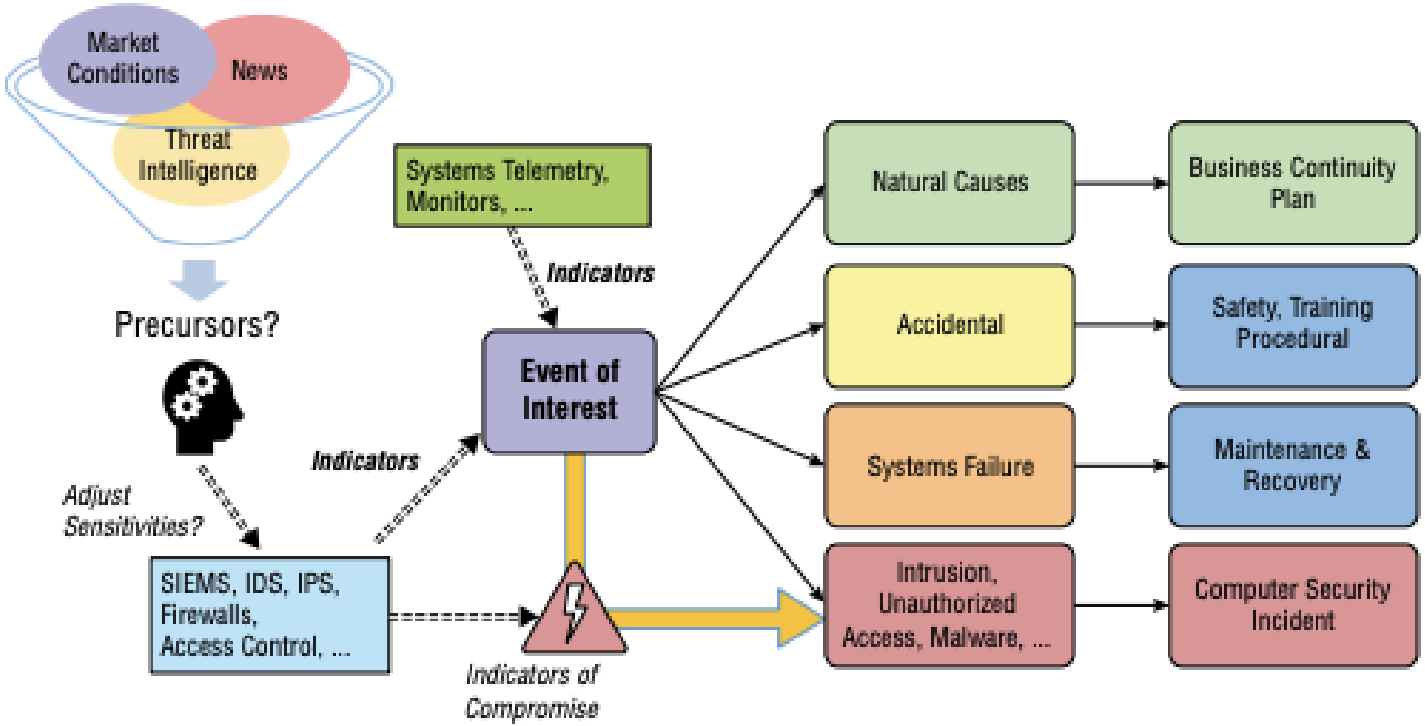
Version: 1.1

Luca Haab | 12.05.2025 | Cours MSE

Business Impact Assessment

Let’s see what your paper reading resulted in…

From events to incident



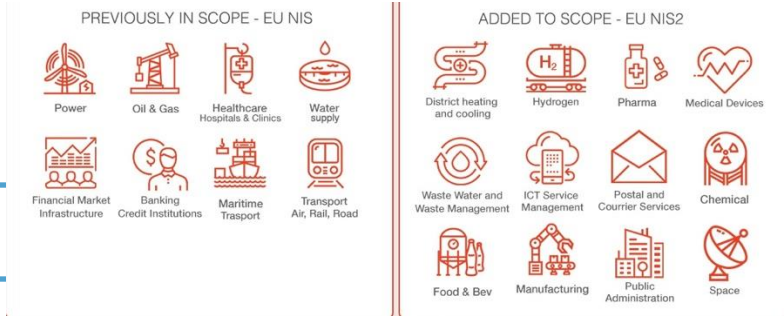
Source: "Triage: from precursors to incident response", The Official (ISC)^2 SSCP CBK Reference, 6th Edition by Mike Wills

Obligation to notify

For Critical Infrastructure

C(H)ritical Infrastructure

- Energy (natural gas supply, oil supply, power supply, district and process heating)
- Finances (financial and insurance services)
- Information & communication (information technologies, media, postal service, telecommunications)
- Public administration (teaching and research, cultural assets, parliament, government, justice, administration)
- Public health (medical care, laboratory services)
- Public safety (armed forces, emergency services, civil defence)
- Transport (air transport, rail transport, road transport, water transport)
- Food and water (food supply, water supply)
- Waste disposal (refuse, sewage)



Source: https://applied-risk.com/resources/valentines-day-industrial-tech-talk-the-eu-nis2-directive-and-cyber-security

Source: https://www.babs.admin.ch/en/critical-infrastructures

Critical Infrastructure Priorities

Sektoren	Teilsektoren (Branchen)
Behörden	Forschung und Lehre
	Kulturgüter
	Parlament, Regierung, Justiz, Verwaltung
Energie	Erdgasversorgung
	Erdölversorgung
	Fern- und Prozesswärme
	Stromversorgung
Entsorgung	Abfälle
	Abwasser
Finanzen	Finanzdienstleistungen
	Versicherungsdienstleistungen
Gesundheit	Medizinische Versorgung
	Labordienstleistungen
	Chemie und Heilmittel
Information und Kommunikation	IT-Dienstleistungen
	Telekommunikation
	Medien
	Postdienste
Nahrung	Lebensmittelversorgung
	Wasserversorgung
Öffentliche Sicherheit	Armee
	Blaulichtorganisationen
	Zivilschutz
Verkehr	Luftverkehr
	Schienenverkehr
	Schiffsverkehr
	Strassenverkehr
	Sehr grosse Kritikalität*
	Grosse Kritikalität*
	Erhebliche Kritikalität*

★► Die Kritikalität steht für die relative Bedeutung des Teilsektors bezüglich möglicher Auswirkungen eines Ausfalls des Teilsektors von wenigen Tagen bis Wochen auf die Bevölkerung und die Wirtschaft.
► Die Gewichtung macht keine Aussagen über die Kritikalität von einzelnen Objekten.
► Die Gewichtung orientiert sich an einer normalen Gefährdungslage. Bei Katastrophen und Notlagen kann sich die Kritikalität der Teilsektoren ändern.

Settori	Sottosettori
Autorità	Ricerca e insegnamento
	Beni culturali
	Parlamento, governo, giustizia, Amministrazione
Energia	Approvvigionamento di gas
	Approvvigionamento di petrolio
	Teleriscaldamento e calore di processo
	Approvvigionamento di elettricità
Smaltimento	Rifiuti
	Acque reflue
Finanze	Servizi finanziari
	Servizi assicurativi
Sanità pubblica	Prestazioni mediche
	Servizi di laboratorio
	Chimica e agenti terapeutici
Informazione e comunicazione	Servizi informatici
	Telecomunicazioni
	Media
	Servizi postali
Alimentazione	Approvvigionamento alimentare
	Approvvigionamento idrico
Sicurezza pubblica	Esercito
	Organizzazioni di pronto intervento
	Protezione civile
Trasporti	Traffico aereo
	Traffico ferroviario
	Traffico navale
	Traffico stradale
	Criticità molto elevata*
	Criticità elevata *
	Criticità marcata*

★► Per criticità s'intende l'importanza relativa del sottosettore in relazione a possibili conseguenze di una sua interruzione di pochi giorni fino a settimane.
► Dalla ponderazione non si possono trarre conclusioni sulla criticità di singoli oggetti.
► La ponderazione si basa su una situazione di minaccia normale. In caso di catastrofi e situazioni d'emergenza, la criticità dei sottosettori può cambiare.

Source: https://www.babs.admin.ch/en/publications-on-critical-infrastructure-protection

swissuniversities

Legal Basis

Information Security Act (ISA)

Already with the publication of the 'The National strategy for the protection of Switzerland against cyber risks (NCS) for 2018 to 2022' there were calls for the feasibility of a reporting obligation to be examined. In 2021, the Federal Council decided to establish the legal basis for introduction of a reporting obligation and to implement this as an amendment to the Information Security Act (ISA).

- On **12 January 2022**, it submitted the proposed draft of the revised ISA for consultation. The results showed general support for a reporting obligation from the private sector, research communities and the cantons.
- On **2 December 2022**, the Federal Council adopted the dispatch on amendment of the ISA to introduce a reporting obligation for cyberattacks on critical infrastructures.
- The amendments to the ISA were then adopted by Parliament on **29 September 2023**.
- On **7 March 2025**, the Federal Council brought the amendments to the ISG into force on **1 April 2025**.

The ISA stipulates that authorities and organisations subject to the reporting obligation, such as energy and drinking water suppliers, transport companies and cantonal and communal administrations, must report cyberattacks to the NCSC within 24 hours of discovery.

Information Security Act (ISA)

Cybersecurity Ordinance (CSO)

With the Cybersecurity Ordinance (CSO), the Federal Council states how it intends to implement the reporting obligation in the future and which organisations will be exempt. The ordinance specifies the exemptions from the reporting obligation for authorities and organisations, indicates which cyberattacks must be reported and clarifies the content to be reported. It also describes the procedures to be followed in relation to the reporting obligation and establishes the deadline and reporting completion requirements.

- On **22 May 2024**, the Federal Council launched the consultation phase for the proposed Cybersecurity Ordinance. The consultation lasted until **13 September 2024**.
- On **7 March 2025** the Federal Council has also adopted the Cybersecurity Ordinance (CSO), which will enter into force on **1 April 2025**. The CSO contains the implementing provisions for the reporting obligation and, in particular, regulates the exceptions.

Cybersecurity Ordinance (CSO)
The document is available in:

German
French

CSO (De): https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/meldepflicht/Cybersicherheitsverordnung.pdf.download.pdf/Cybersicherheitsverordnung.pdf
CSO (Fr): https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/Meldepflcht/Ordonnance_sur_la_cybersecurite.pdf.download.pdf/Ordonnance_sur_la_cybersecurite.pdf

2. Abschnitt: Pflicht zur Meldung von Cyberangriffen

Art. 74a Grundsätze

[1] Behörden und Organisationen nach Artikel 74*b* müssen dafür sorgen, dass dem NCSC Cyberangriffe auf ihre Informatikmittel gemeldet werden.

[2] Das NCSC erteilt interessierten Behörden und Organisationen Auskunft darüber, ob sie der Meldepflicht unterstellt sind und erlässt auf Antrag eine entsprechende Verfügung.

[3] Durch die Meldung eines Cyberangriffs haben die meldepflichtigen Behörden und Organisationen Anspruch auf die Unterstützung des NCSC bei der Vorfallbewältigung nach Artikel 74 Absatz 3.

[4] Die Meldepflicht dient ausschliesslich dazu, dass das NCSC Angriffsmuster auf kritische Infrastrukturen frühzeitig erkennen und dadurch mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Art. 74b Meldepflichtige Behörden und Organisationen

[1] Die Meldepflicht gilt für:

a. Hochschulen nach Artikel 2 Absatz 2 des Hochschulförderungs- und -koordinationsgesetzes vom 30. September 2011[10];
b. Bundes-, Kantons- und Gemeindebehörden sowie interkantonale, kantonale und interkommunale Organisationen, mit Ausnahme der Gruppe Verteidigung, wenn die Armee Assistenzdienst nach Artikel 67 oder Aktivdienst nach Artikel 76 des Militärgesetzes vom 3. Februar 1995[11] leistet;
c. Organisationen mit öffentlich-rechtlichen Aufgaben in den Bereichen Sicherheit und Rettung, Trinkwasserversorgung, Abwasseraufbereitung und Abfallentsorgung;
d. Unternehmen, die in den Bereichen Energieversorgung nach Artikel 6 Absatz 1 des Energiegesetzes vom 30. September 2016[12], Energiehandel, Energiemessung oder Energiesteuerung tätig sind, mit Ausnahme der Bewilligungsinhaber gemäss Kernenergiegesetz vom 21. März 2003[13], sofern ein Cyberangriff auf eine Kernanlage erfolgt;
e. Unternehmen, die dem Bankengesetz vom 8. November 1934[14], dem Versicherungsaufsichtsgesetz vom 17. Dezember 2004[15] oder dem Finanzmarktinfrastrukturgesetz vom 19. Juni 2015[16] unterstehen;
f. Gesundheitseinrichtungen, die auf der kantonalen Spitalliste nach Artikel 39 Absatz 1 Buchstabe e des Bundesgesetzes vom 18. März 1994[17] über die Krankenversicherung aufgeführt sind;
g. medizinische Laboratorien mit einer Bewilligung nach Artikel 16 Absatz 1 des Epidemiengesetzes vom 28. September 2012[18];
h. Unternehmen, die für die Herstellung, das Inverkehrbringen und die Einfuhr von Arzneimitteln eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 2000[19] haben;
i. Organisationen, die Leistungen zur Absicherung gegen die Folgen von Krankheit, Unfall, Arbeits- und Erwerbsunfähigkeit, Alter, Invalidität und Hilflosigkeit erbringen;
j. die Schweizerische Radio- und Fernsehgesellschaft;
k. Nachrichtenagenturen von nationaler Bedeutung;
l. Anbieterinnen von Postdiensten, die nach Artikel 4 Absatz 1 des Postgesetzes vom 17. Dezember 2010[20] bei der Postkommission registriert sind;
m. Eisenbahnunternehmen nach Artikel 5 oder 8*c* des Eisenbahngesetzes vom 20. Dezember 1957[21] sowie Seilbahn-, Trolleybus-, Autobus- und Schifffahrtsunternehmen mit einer Konzession nach Artikel 6 des Personenbeförderungsgesetzes vom 20. März 2009[22];
n. Unternehmen der Zivilluftfahrt, die über eine Bewilligung des Bundesamtes für Zivilluftfahrt verfügen, sowie die Landesflughäfen gemäss Sachplan Infrastruktur der Luftfahrt;

Source: https://www.fedlex.admin.ch/eli/oc/2024/257/de#mod_u19

Sezione 2: Obbligo di segnalare ciberattacchi

Art. 74a Principi

[1] Le autorità e le organizzazioni di cui all'articolo 74*b* provvedono affinché i ciberattacchi verso i loro mezzi informatici siano segnalati all'NCSC.

[2] Il NCSC informa le autorità e organizzazioni interessate sul loro eventuale assoggettamento all'obbligo di segnalazione; su richiesta, pronuncia una decisione sull'assoggettamento a tale obbligo.

[3] La segnalazione di un ciberattacco conferisce alle autorità e organizzazioni assoggettate all'obbligo di segnalazione il diritto a ottenere sostegno dall'NCSC nel far fronte all'incidente secondo l'articolo 74 capoverso 3.

[4] L'obbligo di segnalazione è finalizzato soltanto a consentire all'NCSC di individuare tempestivamente il modo operativo utilizzato negli attacchi contro infrastrutture critiche, così da avvisare possibili interessati e raccomandare loro misure di prevenzione e di difesa adeguate.

Art. 74b Autorità e organizzazioni assoggettate all'obbligo di segnalazione

[1] L'obbligo di segnalazione si applica:

a. alle scuole universitarie secondo l'articolo 2 capoverso 2 della legge federale del 30 settembre 2011[10] sulla promozione e sul coordinamento del settore universitario svizzero;
b. alle autorità federali, cantonali e comunali nonché alle organizzazioni intercantonali, cantonali e intercomunali; è eccettuato l'Aggruppamento Difesa, laddove l'esercito presti servizio d'appoggio secondo articolo 67 o servizio attivo secondo l'articolo 76 della legge militare del 3 febbraio 1995[11];
c. alle organizzazioni cui sono affidati compiti di diritto pubblico nei settori della sicurezza e del salvataggio, dell'approvvigionamento di acqua potabile, del trattamento delle acque di scarico e dello smaltimento dei rifiuti;
d. alle imprese attive nel settore dell'approvvigionamento energetico secondo l'articolo 6 capoverso 1 della legge federale del 30 settembre 2016[12] sull'energia, nonché nel commercio, nella misurazione e nella gestione dell'energia; sono esentati i titolari di licenze conformemente alla legge federale del 21 marzo 2003[13] sull'energia nucleare, per quanto riguarda i ciberattacchi effettuati contro un impianto nucleare;
e. alle imprese che sottostanno alla legge dell'8 novembre 1934[14] sulle banche, alla legge del 17 dicembre 2004[15] sulla sorveglianza degli assicuratori o alla legge del 19 giugno 2015[16] sull'infrastruttura finanziaria;
f. agli stabilimenti che figurano nell'elenco cantonale di cui all'articolo 39 capoverso 1 lettera e della legge federale del 18 marzo 1994[17] sull'assicurazione malattie;
g. ai laboratori medici che dispongono di un'autorizzazione secondo l'articolo 16 capoverso 1 della legge del 28 settembre 2012[18] sulle epidemie;
h. alle imprese che dispongono di un'omologazione secondo la legge del 15 dicembre 2000[19] sugli agenti terapeutici per la fabbricazione, l'immissione in commercio e l'importazione di medicamenti;
i. alle organizzazioni che forniscono prestazioni volte a coprire le conseguenze di malattie, infortuni, incapacità al lavoro e al guadagno, vecchiaia, invalidità e grande invalidità;
j. alla Società svizzera di radiotelevisione;
k. alle agenzie di stampa d'importanza nazionale;
l. ai fornitori di servizi postali registrati presso la Commissione delle poste secondo l'articolo 4 capoverso 1 della legge del 17 dicembre 2010[20] sulle poste;
m. alle imprese ferroviarie secondo gli articoli 5 o 8*c* della legge federale del 20 dicembre 1957[21] sulle ferrovie e alle imprese che gestiscono impianti di trasporto a fune, linee filoviarie, autobus e battelli e sono titolari di una concessione secondo l'articolo 6 della legge del 20 marzo 2009[22] sul trasporto di viaggiatori;

Source: https://www.fedlex.admin.ch/eli/oc/2024/257/it#mod_u19

How should it be reported?

Reporting form on the CSH

To make the reporting process as simple as possible, the reporting form will be available on the NCSC's Cyber Security Hub, which it already uses to exchange information with critical infrastructure operators.

The NCSC reporting form allows for the quick collection of the necessary information and, if requested, forwarding to other authorities to which a reporting obligation also exists, for example to the Swiss Financial Market Supervisory Authority (FINMA) or the Federal Data Protection and Information Commissioner (FDPIC).

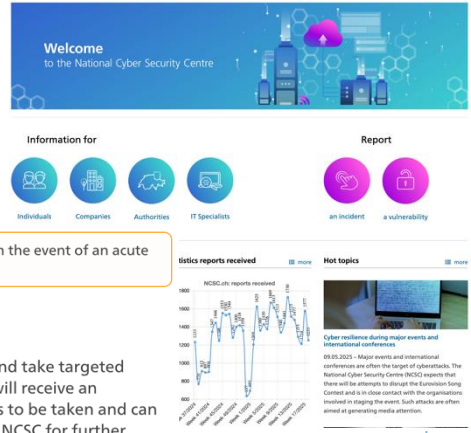
After submitting the initial report within 24 hours of discovering the incident, they have 14 days to complete their report.

Registering on the CSH

The NCSC recommends that organisations that do not yet have a login for the CSH register:

Information about the CSH

If organisations do not wish to register with the Cyber Security Hub, clicking on the 'Report' button on the NCSC home page will provide information on an alternative reporting option and an email template with questions.



Please note that reports are not processed around the clock. In the event of an acute emergency, call the police emergency number 112 or 117.

Voluntary notification

We can identify possible trends in dangers on the internet and take targeted action against them. After answering a few questions, you will receive an automated initial assessment of your case with the measures to be taken and can then forward the case to the National Cyber Security Center NCSC for further processing. Report the incident here

Mandatory notification

From 1 April 2025, critical infrastructures must report critical cyber incidents to the NCSC. You can find the criteria whether your authority or organisation is required to report on the federal law publication platform (in german, french and italian only). In a step-by-step guide, you can find out whether your incident has to be reported and how to report it correctly.

Online criminal complaint

Online complaints can only be filed for the offences listed below. For all other criminal offences, you must contact a police station . The NCSC does not accept criminal complaints.

- False flat advertisement / false real estate advertisement
- Online purchase but did not receive goods
- My data has been misused for orders

Report

https://www.report.ncsc.admin.ch/en/

https://www.ncsc.admin.ch/ncsc/en/home.html

Cyber Security Hub (CSH)

Information about the CSH

The Cyber Security Hub (CSH) is an important information system of the National Cyber Security Centre (NCSC). It is used to share and manage information on cyber threats, cyber incidents and cybersecurity practices.

The CSH is specifically designed to support authorities and critical infrastructure in Switzerland in preventing, detecting and responding to cyber threats. The CSH is regulated in Art. 74 para. 2 and Art. 74f of the Information Security Act (ISA).

Key features of the CSH:

- **Sharing information:** The CSH enables its users to share up-to-date information on cyber threats, security warnings and best practices in a secure and controlled environment.
- **User-centred design:** the platform is designed to be user-friendly, with easy navigation to help users quickly find and share relevant information.
- **Collaboration and networking:** the CSH promotes collaboration between various stakeholders in the field of cybersecurity, including authorities, private organizations and experts.
- **Regular updates and improvements:** The CSH is continuously developed to meet the changing requirements in the field of cybersecurity and to provide users with up-to-date and effective tools.

The CSH plays a central role in the national strategy for strengthening cyber resilience and is an essential element for a comprehensive and coordinated response to cyber threats in Switzerland.

Who is the Cyber Security Hub (CSH) targeted at?

Operators of critical infrastructure

The Federal Office for Civil Protection (FOCP) defines which organizations are considered critical infrastructure:

- FOCP website Critical infrastructure
- National strategy for the protection of critical infrastructure: BBl 2023 1659

Service providers of the operators of critical infrastructure

Service providers of the operators of critical infrastructure that are relevant for cyber security can also be included after consultation with NCSC.

Which specialists within the organizations should have access to the Cyber Security Hub?

The information published on the CSH is targeted at employees of registered organizations in the following roles:

- **IT security specialists, cyber security specialists, etc.**
- **Chief Information Security Officer (CISO), Chief Security Officer (CSO), etc.**
- **Employees of the organisations' Security Operations Centre (SOC) (or similar units)**

The information published on the CSH regarding current cyber threats, security warnings, vulnerabilities and best practices is mostly in English. In-depth IT knowledge is also a key requirement for understanding and appreciating such information.

swissuniversities

Source: https://www.ncsc.admin.ch/ncsc/en/home/meldepflicht/informationen-csh.html

Content and timeline of report

The report shall be handed in

- Within 24 hours from the moment of detection
- If all the necessary information is not available within 24 hours, the OFCS will give the authority or organisation concerned 14 days to complete the report.

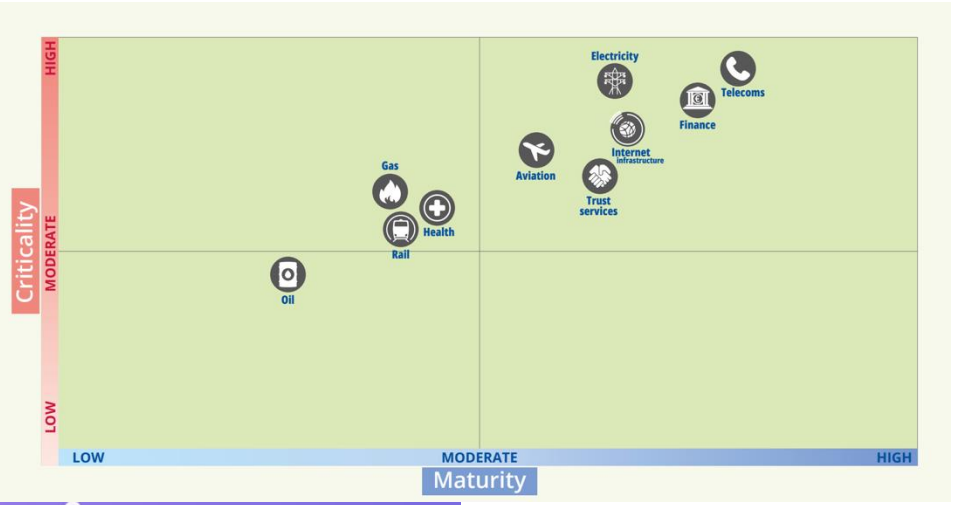
- If the necessary information has not been provided in full within the time limit, the National Cyber Security Centre (NCSC) shall request the authority or organisation concerned to supplement it immediately or to confirm that the information is not available.

What happens if I do not report within 24 hours?

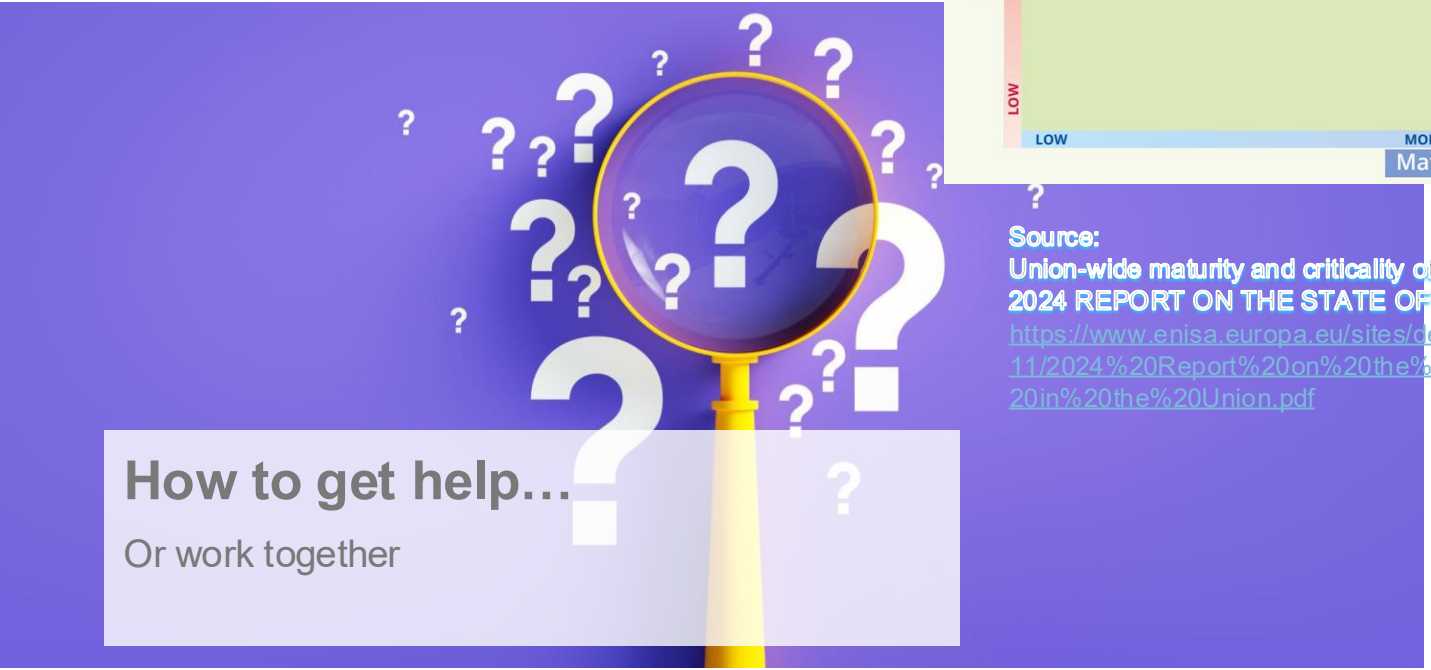
The NCSC can only inform a company subject to the reporting obligation of this obligation if it becomes aware of a reportable cyber incident itself. If there is no response within the deadline after the submission of the report, the NCSC will issue a decision with a threat of a penalty. If the report is still not submitted, the NCSC can report the incident to the competent prosecution authorities.

- The report of a cyberattack must specify:
  - the information on the authority or organisation subject to the reporting obligation, on the planned measures and on the reasons for the report.
  - the date and time when the attack was detected
  - the date and time of the attack
  - information about the attacker
- It must also indicate whether the attack is linked to an act of blackmail, threat or coercion and whether it has been reported to the police
- It must also provide on the consequences of the cyber attack. Namely:
  - the severity of the damage to the availability, integrity and confidentiality of information, and
  - the effects on the functioning of the authority or organisation.
- If the report is not submitted via the CSH communication system, it shall contain the information about the entity subject to the reporting obligation:
  - the company name, name or designation and address, and
  - the contact details of the person submitting the report.

Source: Cybersecurity Ordinance (CSO)



Source:
Union-wide maturity and criticality of 10 (sub-sectors),
2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION,
https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf



How to get help…

Or work together

Companies may (partially) lack

- Resources
- Knowledge
- Continous availability of experts
- …

- Cybersecurity Emergency Response Team (CERT)
- Cybersecurity Incident Response Team (CSIRT)
- Security Operations Center (SOC)
- …

Security Operation Center

- A Security Operations Center (SOC) is the focal point for security operations and cyber network defense for an organization. A SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization.[1]
- SOC activities[2]
  - Asset inventory
  - Routine maintenance and preparation
  - Incident response planning
  - Regular testing
  - Continuous, around-the-clock security monitoring and Log management
  - Threat intelligence (and detection)
  - Incident response
  - Recovery and remediation
  - Post-mortem and refinement
  - Compliance management
  - …

Example	In house		Outsourced	
	Pros	Cons	Pros	Cons
Threat Intel (TI)	Better business context. Can look for intel relating to specific, relevant threats.	Resource intensive. Cost.	Typically, an abundance of TI that is shared across many organisations, a wide net.	Potentially very generic. Lacking business context.
Digital Forensics and Incident (DFIR)	Better business context and expedited access to devices.	Not always required.	Can be called upon when required.	Potentially lacking business context. Delayed incident response.

https://www.ncsc.gov.uk/collection/building-a-security-operations-centre/operating-model/designing-an-operating-model

[1]: NIST SP 800-53, Rev. 5 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[2]: https://www.ibm.com/think/topics/security-operations-center

SOC: (A more) Formal definition

Service Area	SOC	CSIRT	PSIRT	ISAC
Information Security Event Management				
Monitoring and Detection	MUST	-	-	-
Event Analysis	MUST	-	-	-
Information Security Incident Management				
Information Security Incident Report Acceptance	-	MUST	-	-
Information Security Incident Analysis	-	MUST	-	-
Artifact and Forensic Evidence Analysis	-	-	-	-
Mitigation and Recovery	-	MUST	-	-
Information Security Incident Coordination	-	MUST	-	-
Crisis Management Support	-	-	-	-
Vulnerability Management				
Vulnerability Discovery/Research	-	-	-	-
Vulnerability Report Intake	-	-	MUST	-
Vulnerability Analysis	-	-	MUST	-
Vulnerability Coordination	-	-	MUST	-
Vulnerability Disclosure	-	-	MUST	-
Vulnerability Response	-	-	MUST	-
Situational Awareness				
Data Acquisition	-	-	-	MUST
Analysis and Synthesis	-	-	-	MUST
Communication	-	-	-	MUST
Knowledge Transfer				
Awareness Building	-	-	-	-
Training and Education	-	-	-	-
Exercises	-	-	-	-
Technical and Policy Advisory	-	-	-	-

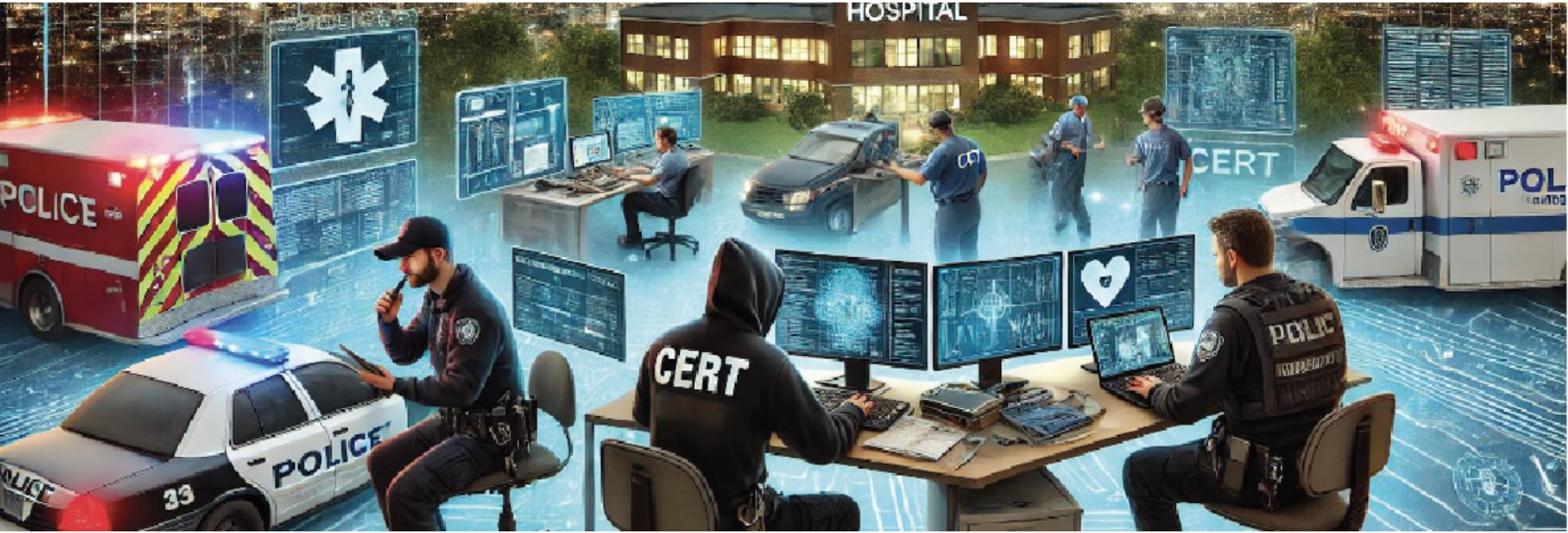
Source: https://www.first.org/standards/frameworks/csirts/team-type_1-1

ISAC: Information Sharing and Analysis Center
PSIRT: Product Security Incident Response Team
CSIRT: Cybersecurity Incident Response Teams

FIRST: Forum for Incident Response and Security Teams

swissuniversities


Imagine a situation

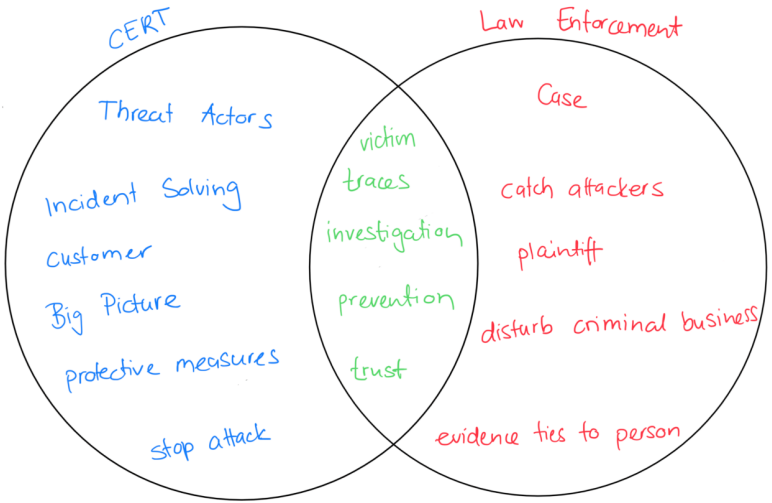


Cyberattack on a hospital - a fictive case

Cyberattack on a hospital - a fictive case

Different perspectives

- CSIRT wants to assess traces the attackers have left behind, take protective measures, stop the attack and return to normal operation with as little damage as possible
- Police is responsible for public safety, law and order. In this case, they want to investigate the perpetrators and needs usable evidence

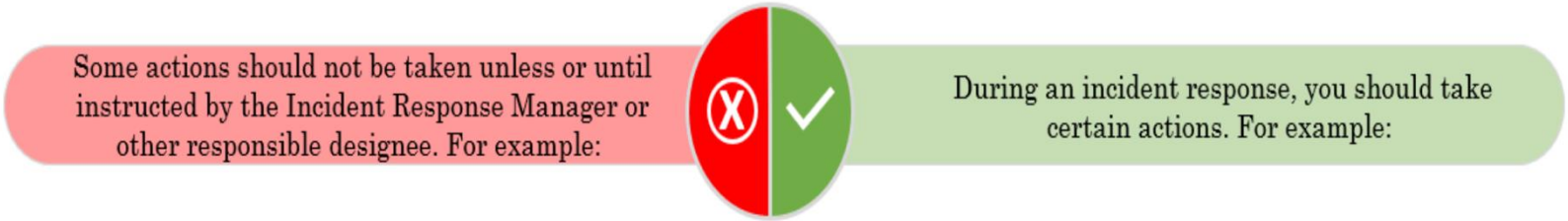


Source: https://www.switch.ch/en/insights/cyberattack-hospital-between-it-security-and-law-enforcement

Cyberattack on a hospital - a fictive case

real

Figure 3. Example Do's and Don'ts During Initial Response



Source: https://healthsectorcouncil.org/wp-content/uploads/2024/11/MEDICAL-PRODUCT-MANUFACTURING-CYBER-INCIDENT-RESPONSE-PLAYBOOK-2.pdf

swissuniversities

A concrete case

Incident Response

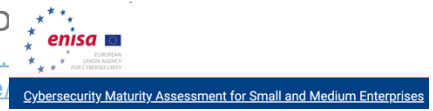
Company	Groupe E SA		
CFC Case	[redacted]		
Detection Date	[redacted]	**CSIR engaged**	[redacted]
Time Estimation	10 Hours	**Time consumed**	10 Hours
Context	Groupe E SA had discovered that one of their user's email accounts had been compromised when that user had been found to have sent mass mails to multiple parties with a phishing link.		
Impacted Asset(s)	[redacted]		
Scope	Entra ID Investigation		

A little help from my friends…

Friends in

- Peers/Maturity
  - EU CSIRT (https://tools.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map)

  - There are available tools for assessing the maturity of a co (https://tools.enisa.europa. =/topics/incident-response/ maturity/csirt-survey)



  - And more (like Building a SOC https://www.ncsc.gov.uk/collection/building-a-security-operations-centre/operating-model/designing-an-operating-model)

- Tools
  - Potentially, your beloved tool already offers support for OT specificities

Application	Protocol	VLAN	Client	Server	Actual Thpt	Total Bytes	Info
IEC60870	TCP	21	:2404	:44404	0 bps	100.48 KB	<- S, RX 21582
IEC60870	TCP	21	:2404	:59749	0 bps	53.31 KB	-> I, RX 65, TX 28985
IEC60870	TCP	21	:58463	:2404	0 bps	8.44 KB	<- S, RX 14
IEC60870	TCP	21	:54827	:2404	0 bps	12.1 KB	-> U (TESTFR con)

Source: https://www.ntop.org/guides/ntopng/scada/IEC60870-5-104.html

swissuniversities [1]: based on https://www.enisa.europa.eu/sites/default/files/publications/Study_on_CSIRT_Maturity_29042019.pdf

10 tips for a successful IR

1. An army marches on its stomach
2. Y'all got any more of that whiteboard
3. Brace yourself – the phone will ring
4. Stress, stress everywhere
5. Nobody cares – get the help you need
6. Minimum Champion!
7. Ight Imma Head Out – Exercise!
8. No regrets – creativity
9. Run a marathon they said, It'll be fun they said
10. Are you sure about that?

Source: https://www.switch.ch/en/insights/10-tips-successful-incident-response

Going beyond

NIST Special Publication 800-34 Rev. 1

Contingency Planning Guide for Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

NIST National Institute of Standards and Technology • U.S. Department of Commerce

NIST Special Publication 800
NIST SP 800-61r3

Incident Response Recommendations and Considerations for Cybersecurity Risk Management

A CSF 2.0 Community Profile

Alex Nelson
Sanjay Rekhi
Murugiah Souppaya*
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity

**Former NIST employee; all work for this publication was done while at NIST.*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-61r3

April 2025

U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST Special Publication
NIST SP 800-82r3

Guide to Operational Technology (OT) Security

Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman
Victoria Pillitteri
Suzanne Lightman
Adam Hahn
Stephanie Saravia
Aslam Sherule
Michael Thompson

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r3

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

References

- Contingency Planning Guide for Federal Information Systems, NIST Special Publication 800-34 Rev. 1
- Computer Security Incident Handling Guide, Special Publication 800-61 Rev. 3
- Computer Security Incident Handling Guide, Special Publication 800-61 Rev. 2 (withdrawn)
- Guide to Operational Technology (OT) Security
- IoT Device Cybersecurity Guidance for the Federal Government, Special Publication 800-213A
- Technical Resilience Navigator, Site Planning, U.S. Department of Energy
- Security and resilience — Business continuity management systems — Guidelines for business impact analysis, ISO/TS 22317:2021
- The Official $(ISC)^2$ SSCP CBK Reference, 6th Edition by Mike Wills