Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Managing Insider Threats

Good practices of Dutch organisations

Publication date: March 22, 2024

Authorised distribution:
(Traffic Light Protocol)

This publication bears the label TLP:CLEAR and is distributed by the NCSC. The NCSC uses the Traffic Light Protocol (TLP) to clearly define what may be done with information contained in this report. If information has a TLP designation, you will know with whom the information can be shared. This is described on the NCSC's website (https://www.ncsc.nl/onderwerpen/traffic-light-protocol)

TLP:CLEAR indicates that there are no restrictions on sharing the information more widely.

We welcome your comments or suggestions at info@ncsc.nl.

Contents

Introduction

Insiders can pose a significant risk to your organisation. The impact of an insider threat can be devastating. Unlike external cyber attacks, insiders operate within your organisation.

An insider is an invisible enemy who can misuse authorised access to cause damage. How can you deal with this invisible enemy? We asked this question to the chairpersons and vice-chairpersons of the ISACs in which the NCSC takes part. In this document, we share their insights and good practices.

The issue of insider threats

Malicious insiders can have a significant impact on your organisation's cybersecurity. Research by Ponemon shows that insider-related incidents occur on a regular basis, it takes organisations 77 days on average to contain such incidents, and the associated costs can be very high.[1]

Other consequences of an incident with a malicious insider, such as a breach of trust on the work floor, are hard to express in terms of money but have a serious impact on your organisation, too.

Not all insiders are malicious

This publication focuses specifically on malicious insiders but there are other categories of insider threats such as the unintentional insider, an individual who unwittingly exposes their organisation to a cyber threat through action or inaction without malicious intent.

Another category of insiders consists of individuals who deliberately ignore the rules. They deliberately choose to ignore particular security directives, for instance to work more efficiently. This means they act in a negligent manner but do not immediately have malicious intentions against the organisation that employs them.

We do not discuss these two types of insiders explicitly in this publication but they must be taken into consideration when formulating an insider risk policy.

Multidimensional approach

The issue of insider threats touches upon several professional disciplines, including fraud prevention and organisational psychology. This publication tackles insider threats from the perspective of cybersecurity but we do recommend including these other perspectives on insider threats in your insider risk policy. As such, a good approach to dealing with insider threats is multidisciplinary.

Method and definitions

The definitions in this document on insider threats were produced by the NCSC-UK.[2] They see an insider as 'any individual who has legitimate access to, or has previous knowledge of, the organisation's resources, including people, processes, information, technology and facilities'.

As such, insiders are not just the employees of the organisation but also other employees (temporary or otherwise), such as personnel of partner organisations, service providers or suppliers.

An insider threat is 'an individual who has the intention to harm an organisation'. We therefore discuss insider threats from an intentional perspective.

Implementation of the NIST framework

This document is structured in accordance with the NIST framework.[3] The chapters focus on the functions in the framework, looking at preventive and reactive cybersecurity aspects of managing insider threats.

The issue of insider threats, the associated definitions and the NIST framework constituted the basis for a workshop undertaken by the NCSC with cybersecurity experts in Dutch organisations on 21 November 2023.

That session aimed to identify good practices[4] with regard to insider threats. This document is a result of this session.

Target audience

This document is intended for CIOs, CISOs, security officers and risk managers who want to gain an understanding of insider threats and are involved in setting up an insider risk policy.

Background

This document was created in the course of a workshop with the chairpersons and vice-chairpersons of the ISACs[5] in which the NCSC takes part.

In this workshop, the participants shared good practices on dealing with insider threats. The AIVD (General Intelligence and Security Service) was also a participant in the session and in the dialogue shared insights on managing insider threats. The NCSC enriched the outcomes and incorporated them into this publication.

This is the second publication in a series of documents on good practices for a cybersecurity theme. The NCSC previously published *Omgaan met risico's in de toeleveringsketen'* [Dealing with risks in the supply chain].[6]

Identify & Protect

Which assets might be targeted by insider threats and what is the best way to protect them? This chapter covers these two questions.

Identify

Which assets[7] might be at risk from insider threats?

GP[8] 1.1: Identify critical processes

To determine where insider threats might hit hardest, you need to know what your critical processes are. These are the processes that are vital to your organisation's functioning and are often described as your 'crown jewels'.[9]

- Use CIA classifications in identifying your critical processes, as they tell you the potential impact on the availability, integrity and/or confidentiality of a process and its consequences for your organisation and its stakeholders.
- You can use existing tools, such as a Business Impact Assessment (BIA), to map your critical processes.[10]

GP 1.2: Incidents involving insiders can occur in all organisation layers

Insider threats can manifest in all layers of your organisation. Insiders can be active from the highest decision-making body in your organisation down to the lowest functional level.

GP 1.3: Insider threats can come from suppliers or partner organisations

Insider threats can come from the personnel of your suppliers or organisations you work with.

Supplier or partner organisation employees may have access to your systems or data, for instance when they work within your organisation on a temporary basis.

It is therefore a good practice to map the organisations you do business with and the insider risks associated with them.

- Establish which organisations have access to or an impact on your critical processes. The level of access to or impact on your critical processes is an important starting point in prioritising the organisations, such as suppliers, that require the highest level of attention.

  Map how suppliers and partners manage insider threats and what measures they have put in place to protect your processes and data.
- Be aware that suppliers and partner organisations have their own organisational culture, which in turn has an impact on the risk of insider threats. Make sure you have a feeling for your principal suppliers and partners, and be open to discussing any concerns.
- Suppliers and partner organisations may also be influenced or required by foreign authorities – such as intelligence agencies - to collaborate on information-gathering operations.

  This risk increases if a supplier or partner has ties with countries running a confirmed offensive cyber programme targeting Dutch interests, such as China, Russia, Iran, or North Korea.

If you do business with a foreign organisation, such as a supplier, make sure you are well informed about any insider risks that may result from such collaborations. The Threat Assessment State Actors *(‘Dreigingsbeeld Statelijke Actoren’)* issued by the AIVD, MIVD and NCTV is a good starting point here.[11]

Protect

What preventive measures can be taken to protect assets from insider threats?

GP 1.4: Pre-establish criteria for assessing signals

Prevent prejudice and cognitive bias[12] in the approach to insider threats. Implementing a clear process that devotes attention to reducing bias minimises subjectivity in assessing signs of insider threats.

- You can achieve this by setting up a transparent and widely supported insider risk policy within your organisation.
- By fostering awareness among your employees and within your organisation, blind spots or potential risks can be identified at an early stage. It helps to handle any prejudice and cognitive bias in a deliberate manner.[13]
- Make sure that the procedure for reporting deviant and suspicious behaviour is transparent, as it is the only way to ensure that signals of deviant behaviour reach the right people in your organisation.

GP 1.5: Incorporate soft controls into your insider risk programme

Soft controls are intangible factors that influence behaviour and have an impact on an organisation’s culture and working conditions. Soft controls can also be used in an insider risk policy.

- An open organisational culture in which problems are acknowledged and discussed is an important factor that reduces the risk of insider threats. Insiders are less likely to engage in deviant or incorrect behaviour when working in a safe environment in which people know and are in touch with each other.
- Managers play an important role in this regard. They can open a dialogue about insider threat issues and address deviant behaviour in a timely manner. By doing so in a professional capacity in accordance with objective and transparent guidelines, they contribute to a safe work environment and a healthy organisational culture.
- You should also establish a code of conduct[14]: What do you expect from your employees? How do people interact with one another? Who do you go to if you notice deviant behaviour or worry about a colleague? These are some examples of questions that can be addressed in a code of conduct.

  You should also consider what you expect from employees when they leave your employment. How do you expect them to handle the confidential information to which they had access?

GP 1.6: Work on good network architecture

Good network architecture is important in protecting against multiple threats, including insider threats. While an insider already has access to the network, you can still reduce the impact of insider threats by ensuring that your network architecture is good. You can do this by:

- **Implementing ‘Ethical Walls’.** These are measures that ensure users do not have access to data if it would lead to a conflict of interest.
- **Using data loss protection systems.** This contributes to ensuring that sensitive data cannot easily exit the systems or network.

- **Applying zero trust principles**. This will make your organisation more resilient to attacks from within your organisation.[15]
- **Implementing physical segmentation**. Who will have access to the server room, for instance? And who will monitor this?

GP 1.7: Not everyone should have access to all information

Employees do not necessarily need access to all the information within an organisation. Specify which employees have access to what information. Think in terms of principles such as *need to know*, *need to have*, and *least privilege*.

- It is also well worth making clear what kind of behaviour you expect from different user types. Deviant behaviour can then be detected by monitoring user logs.
- It is important to be transparent about monitoring towards employees and keep them informed.

GP 1.8: Develop a screening policy and be transparent about it

You can gain insight with regard to any insider risks by means of personnel screening. On the other hand, screening employees (including new employees) is a serious measure. Consider whether screening is a proportionate measure to deal with insider threats and whether it is necessary for all or just specific positions.

- Specific employee characteristics may contribute to raising insider risk. Risk factors include employees being in debt or saying negative things about your organisation.
- Make sure your screening policy has a sound legal basis, particularly if you ask an external organisation to do a screening.
- Be transparent about your screening policy for specific positions. Be aware that a screening may represent an unintended obstacle for people to apply for specific positions.
- Establish an expectation of privacy and discuss it with employees. This may specify what information an employer can see and what is expected from employees. You can also include your screening policy for specific positions.
- Sometimes it is not enough to do a preliminary screening alone. You can keep an eye on employees in confidential positions by doing a periodical screening.
- You do not have to do the screening in-house; there are organisations that specialise in defining and implementing screening policies for confidential positions.

Detect

How do you detect insider threats in a timely manner? This chapter discusses detection measures that you can implement to recognise malicious insiders.

A challenging issue

Recognising insider threats is quite a challenge. Insider threats share common ground with cyber or ICT-related and fraud incidents. Insider threats may also occur throughout the organisation and, if not adequately addressed, lead to an organisation-wide crisis situation.

The conversations with the chairpersons and vice-chairpersons of the ISACs show that in many cases, different departments are responsible for dealing with these types of incidents.

- In some cases, the risk and/or compliance department bears responsibility; integrity or fraud coordinators take the lead in others.
- In addition, reports, alerts and incidents often do not end up in the same centralised place, making it is hard to ensure an organisation-wide overview and detect connections.
- This underlines the need for a multidisciplinary approach in your insider risk policy, also for the detection of malicious insiders.

Detect

How can you detect insider threats within your organisation in a timely manner?

GP 2.1: Create a shared standard

If you want to be able to determine what behaviour deviates from the norm, you must have a definition of normal behaviour. You can then use this standard to check for deviant behaviour.

- What normal behaviour constitutes in your organisation, depends on your organisational culture, its key values and maturity, and the degree to which the organisation is already required to comply with rules, legislation and frameworks (of standards).
- You must also determine the aspects of behaviour on which you want your standard to be based. Make sure that your standards do not unintentionally obstruct your employees' individual freedom.

  Example: If an employee suddenly copies huge amounts of data to a flash drive in the middle of the night, this is an indication of deviant behaviour that may be related to an insider threat.

GP 2.2: Lower the threshold for reporting suspicious situations

Make sure that employees can report suspicious situations easily and conveniently. The threshold to report and discuss a suspicious situation may be high.

- Ensure that managers know how to handle a report and address it in a confidential manner.
- Make sure that there is a single point of contact where employees can submit their report, even if it is not their manager. It can also be a general desk for an 'incident report'.
- Offer your personnel feedback on what was done with reports. You do not have to talk about the details but it is important to show that you follow up on reports in a serious and confidential manner.

GP 2.3: Train your personnel

Make sure that your employees are aware of your integrity policy, the code of conduct, who their confidential advisor is, that a whistle-blowing scheme is in place and where to find it. This can be part of an onboarding programme for new workers.

GP 2.3.1: Specific employee training

- Let employees experience what risks exist on the work floor regarding insiders. And how they can contribute, in their position, to the detection of malicious insiders.
- Explain which key positions are extra vulnerable to insider threats, for instance positions with more (administrative) authorisations or a higher mandate.
- Teach employees the best response to a suspicious situation and how to report such situations.

GP 2.3.2: Specific managerial training

- Allow managers/supervisors to attend a training to talk to people on the work floor about deviant behaviour.

  A good relationship with their team means that managers/supervisors have an important part to play in preventing and detecting insider threats in a timely manner. Clearly explain what you expect from managers/supervisors in this respect.
- Be aware of how the organisation handles reports, investigations, and the consequences for individuals subject to investigation. Practice this together on a regular basis, both at the process level and in terms of the skills needed to deal with a report.

GP 2.4: Map vulnerable moments

Certain events may have an impact on the manifestation of an insider threat.

- **Turbulent periods:** A malicious insider may choose to exploit a turbulent period in an organisation, assuming that monitoring may have lapsed, for instance. Such situations may include holidays, bank holidays or periods of transition and personnel changes.
- **Triggering events:** Events may also cause an insider to engage in malicious actions, such as a reorganisation that is announced, the upcoming end of an (employment) contract or a termination procedure.

GP 2.5: Enable detection

Deviant behaviour can also be detected by means of technical measures.[16] This includes the detection of deviant behaviour on systems, unexplained data streams, or deviant employee authorisations.

- Good logging and adequate retention periods are necessary to realise this. Such logs can be used to detect deviations in behaviour and, in the event of an incident, to trace the incident back to its cause.
- Logging may be subject to maximum retention periods, please keep this in mind.
- Detection can be implemented at different points in a network. By mapping potential attack paths of a malicious insider, an organisation can identify different points in a network for detection. Determine the detection indicators for each point.

GP 2.6: Share your experiences and insights with partner organisations

It is valuable to learn about insider threats and how to handle them from other organisations. Because this is a sensitive topic, a lot of information is kept behind closed doors – not least due to a fear of reputational damage and loss of face. Sharing experiences can help you deal with insider threats more effectively, however.

- Trust is the basic requirement for sharing knowledge and experiences. Make sure that people know each other and know how to find each other. An ISAC is an example of a place where people meet and build trust so they can share knowledge and experiences in a confidential environment.[17]

- Adhere to a fixed structure when exchanging experiences. Discuss modus operandi, for instance: What did the insider do? How was the incident detected? And how did people respond to the incident? This information can help others deal with insider threats.

GP 2.7: Collaborate and make expectations explicit

You are not alone in your task of having to detect insider threats.[18] Several departments and/or organisations in your organisation can contribute to detecting malicious insiders.

- An accountant or IT auditor investigation may also lead to detection of deviant behaviour in an employee.
- Supervisory bodies, knowledge authorities and investigation agencies can also share knowledge and expertise on insider threats. In this way, trends observed in an industry may lead to concrete detection measures in an organisation.

Respond & Recover

' The question is not if but when you will be facing an insider threat.' [19]

This chapter focuses on how you can respond to an incident with an insider threat and how you can recover from the consequences.

Respond

How can you respond to an incident with a malicious insider?

'It is about people. The insider is the criminal but they are also the colleague' [20]

GP 3.1: Dealing with insider threats is people's work

An incident with an insider threat has an impact on the work floor. In addition to sharing similarities with general aspects of cybersecurity incidents, social elements play a part in insider threat incidents. After all, you or your colleagues have to deal with a breach of trust: A colleague or acquaintance turns out to be a malicious insider. This has an impact on trust and job satisfaction on the work floor.

- Be aware that these social aspects are important in your response to the incident. Depending on the motivation and type of incident, emotions like sadness, anger or pity may easily come to the fore. Handle this in a suitable way.
- At the same time, you must respond to a malicious insider quickly and effectively. The longer it takes to respond, the more extensive the damage.[21]
- You should be aware that both aspects may have an impact on your decision-making. Allow these emotions to be and keep in mind that perceived urgency and time pressure may also affect your decision-making process. You can do this by relying on plans and protocols that were established beforehand.

GP 3.2: Let an external partner provide support in your response

There are organisations specialising in insider threat issues and forensic investigation of what may be a crime.

They can provide advice and support in responding to an insider. Calling on an external partner can be warranted, particularly if your organisation does not have the expertise to respond adequately to an insider.

This external partner may have access to confidential information, so make sure to have a thorough legal foundation before involving an external partner in the event of an incident. Get timely legal advice and incorporate such legal considerations into your insider risk policy beforehand.

GP 3.3: Take expeditious action in consultation with stakeholders

Responding to insider incidents is a complex and challenging issue. A range of stakeholders must be involved to ensure an adequate reaction, such as HR, your legal department, and the board. Alignment and good collaboration between these stakeholders is required if you are to act in a balanced and effective manner.

- Prepare an incident procedure beforehand so you have something to rely on in the event of an incident. The procedure should include escalation options. You must also discuss the possibility of creating an incident response team.

- A hasty response to an insider threat without informing direct stakeholders comes with risks. If possible, you should involve the principal stakeholders in your response.

  You can save time by taking temporary measures that are less invasive but do mitigate the risks, for instance temporarily freezing and isolating a user account.

- An insider incident may have different causes. An angry employee who teams up with a criminal actor requires a different response than a supplier who gives another party access to your systems due to blackmail. This influences the way in which you should respond.

- You can use the OODA-loop in your response, which stands for observe, orient, decide and act. This prevents hasty decision-making and refines your insight into what parties must be involved to come to a well-considered response.

GP 3.4: Align your actions with the available information

'Having well-organised processes helps you respond to a malicious insider. This ensures that you are not led by emotions that would hinder a suitable response.'[20]

When action is required in the face of an insider threat, you usually do not have a full assessment of the scope and circumstances of the incident. Emotions and the wish to eliminate the threat as quickly as possible may get the better of you in a response.

- Make a clear distinction between facts and assumptions in your analysis. Take action based on the available facts and exercise restraint in acting on the basis of assumptions.

- Playbooks and response plans can help you decide on a suitable response to an insider threat. They help you focus on implementing the process instead of acting on the basis of emotions.

GP 3.5: Decide on a suitable response to an insider threat

GP 3.5.1: The response within your organisation

A good response within your organisation to a malicious insider generally requires a multidisciplinary approach, which also takes account of legal, technical or policy-related aspects that may play a part in an insider incident. Consider the following measures in your response:

- **Isolate the insider**. You can do this by freezing or blocking the insider's user accounts to prevent them from accessing your systems and data.

- **Investigate the insider.** Sometimes, you need to gather more information about the circumstances, motivation and scope of a possible incident with the insider. This may include collecting evidence by means of monitoring and logging.

- **Confront the insider**. This requires experienced and well-trained employees who can ensure that the confrontation proceeds in a responsible manner. Always ensure a fair hearing, and consider subsidiarity and proportionality in your response throughout the process.

- **Inform your organisation of the incident.**[22] By the time that a response to the insider threat is required, stories about the insider are usually already circulating in your organisation. Informing your own employees may be necessary with an eye to the circumstances and available information. Keep in mind that there is no such thing as internal communication in isolation. Internal usually also means external communication. In this phase, you must already consider whether you need to inform customers, suppliers/vendors and other stakeholders.

GP 3.5.2: Report the incident

- **Report the incident.** You can report an incident to the competent authorities. Critical suppliers and providers of critical services are required to report grave digital security incidents to the NCSC.[23]

  Report the incident to the police if a crime is suspected.[24] Report the incident to the Dutch Data Protection Authority in case of a data leak involving sensitive data.[25] If you suspect that state-sponsored actors may be involved, contact the AIVD.[26]

  Your report may prevent further damage arising from an incident. In doing so you are contributing to (digital) security in the Netherlands.

- **Consider taking legal action**. You may have to resort to legal action. Reporting a crime may lead to a criminal investigation, but steps under civil, administrative or disciplinary law may also be an option. In some cases, an integrity commission may be useful. Here, too, the cause and gravity of an insider threat determine the level of action.

Recover

How can your organisation recover and learn from an incident with a malicious insider?

GP 3.6: Recover from the vulnerability

Recovering the compromised systems and data is the first priority after shutting down the insider threat. You must also determine the causes that led to the insider threat.

- Investigate how the incident was able to occur. Were there any measures that proved ineffective? Or did you overlook important information that kept you from detecting the insider threat in time? Undertaking a thorough review and assessment will allow you to recover and learn from an incident.
- Be aware that overreacting to an incident may be part of your response. An insider incident can have a serious impact on your emotions, but some risks are not easily eliminated or, in the case of extremely far-reaching measures, the remedy may be worse than the disease.

GP 3.7: Communicate about an incident

An insider incident may damage your organisation’s reputation. Open communication about an incident and your response will make sure you retain the trust of your customers, suppliers and other stakeholders.

- An important precondition for open communication is to think well in advance about the target groups you need to approach, always focusing on legal requirements, information needs, interests, and reputation-related risks. You can structure this in a crisis communication plan.

GP 3.8: Keep an eye on grief

‘As a crisis team, you are often two steps ahead in the grieving process. You may already see the insider as the villain whilst your employees are still in denial. Ensure a good debriefing and offer space and aftercare.’[20]

In addition to technical and financial damage, incident can have a big impact on employees.[27] Insider incidents add another dimension since some of them may know the culprit. It may be someone they worked with, trusted, and perhaps even shared stories and information from their personal lives.

- This is why there must be space for a grieving process. It is good to be aware of this, especially since members of the crisis or response team may already be in a different stage of grief than other employees.[28]

GP 3.9: Review and learn

An important component in recovering from insider incidents is to improve resilience. After all, incidents are the moment at which the effectiveness of your preparations is tested in actual practice. Which procedures worked and what requires further improvement?

- In this context, it is important to document all steps taken in the course of the incident carefully and thoroughly. In hindsight, you should identify the lessons learned in relation to the entire chain of protection, detection, response and recovery.
- You can use this input to improve your response and recovery plans. Moreover, such insights can help you improve your process for identifying and detecting malicious insiders in the future.
- Consider doing a hot debrief with your crisis team immediately after the incident is under control. You can record the first lessons learned from your crisis team and allow them to vent any emotions and frustrations if necessary.

GP 3.9.1: Use crisis exercises and simulations

You can also evaluate and learn after going through a tabletop exercise. Working through a scenario with a malicious insider incident allows you to determine whether your organisation is able to deal with this type of incidents.

- A tabletop exercise allows you to walk through procedures and crisis plans without undue pressure. It also enables you to discuss responsibilities and expectations between departments and employees.
- This should include discussing your communication plan in the event of a malicious insider incident. Talk about the type of message you want to communicate in the event of such incidents and which channels you plan to use.

Govern

How do you ensure that your insider risk policy is in line with your organisational objectives and decision-making process? This chapter discusses administrative aspects that you need to incorporate into your insider risk policy.

Govern

How do you ensure that your insider risk policy is in line with your organisational objectives and decision-making process?[29]

GP 4.1: Get legal advice

An approach relating to insider threats may come with legal implications. Before implementing any measures, check that they comply with the applicable regulations and legislation.

Elaborating a screening policy as described in section GP 1.8 may give rise to legal questions and considerations, for instance. Get clarity on the legal feasibility of any measures before you implement them.

GP 4.2: Organise monitoring of your insider risk policy

An insider risk policy may have consequences for the privacy of your employees. As such, it is important that your insider risk policy is subject to independent monitoring.

It is important for employees to know that their confidential information is handled with care and you do not collect any other data than is strictly necessary.

An independent commission with representatives from different stakeholder groups in your organisation should monitor the implementation of your insider risk policy and check that it is in line with your ethical framework.

Further reading

The Fraud Triangle

When handling insider threats, you can also learn from adjacent disciplines, such as accountancy and fraud prevention. One of the concepts they use is the fraud triangle, which features three factors that are required to engage in fraud.

Frauderisicobeheersing: Aanbevelingen voor bestuurders en toezichthouders [Fraud Risk Management: Recommendations for executive and supervisory boards], Koninklijke NBA, 2022

NCSC-UK: Reducing data exfiltration by malicious insiders

The NCSC-UK also devotes a lot of attention to dealing with insider threats. You can find advice and recommendations to mitigate the risk of data exfiltration by insiders on their website.

Reducing data exfiltration by malicious insiders, NCSC-UK, 30 June 2022

The MICE model

MICE is an acronym for the indicators *Money*, *Ideology*, *Coercion* and *Ego*. The MICE model can help organisations think about measures and ways to detect and prevent insider threats in a timely manner.

Charney, David L., and John A. Irvin. ‘The Psychology of Envy’. *Intelligencer: Journal of US Intelligence Studies* 22 (2016): pp 71-77.

NPSA: Reducing Insider Risk

The British *National Protective Security Authority* has published a toolbox on how to manage insider risks. In addition to recommendations on how to handle insider threats, the toolbox also offers insights on how to communicate about insider threats and provide training within an organisation.

Reducing Insider Risks, National Protective Security Authority, 2023

CISA: Insider Threat Mitigation

The CISA also published a comprehensive manual on insider threat management. The manual contains several supplementary handouts with recommendations and advice on this theme.

Insider Threat Mitigation, CISA, 2023

‘The Critical Pathway to Insider Risk Model’

This article by Mark Lenzenweger and Eric Shaw discusses the CPIR model, which focuses on behavioural factors that help gain insight into insider risks in a timely manner. It primarily discusses the behavioural dimension in insider issues.

Lenzenweger, M. F., & Shaw, E. D. ‘The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions‘, *Counter-Insider Threat Research and Practice*, 2022

Integrity in Practice

In this document, the Dutch Whistleblowing Authority (Huis voor Klokkenluiders) discusses how organisations can proceed with an internal investigation of suspected wrongdoing

Integriteit in de praktijk [Integrity in Practice], Huis voor Klokkenluiders, 1 April 2020

References

[1] https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/

[2] https://www.ncsc.gov.uk/guidance/reducing-data-exfiltration-by-malicious-insiders

[3] https://www.nist.gov/cyberframework

[4] Good practices in this document are operating methods, habits and practices that have been shown in actual practice to be effective in tackling an issue.

[5] ISAC is the acronym for Information Sharing and Analysis Centre, a consultation body focusing on cybersecurity in which organisations from a single industry exchange sensitive and confidential information about incidents, threats, vulnerabilities and mitigation measures.

[6] *Dealing with risks in the supply chain; Good practices in Dutch organisations*, NCSC, 15 August 2023

[7] In terms of cybersecurity, assets are information or digital systems that are of value to an organisation, such as intellectual property, a customer database, personnel information, etc.

[8] In this document, we have marked the good practices identified by participants with 'GP'.

[9]Crown jewels are the information and information systems that are absolutely vital to an organisation. Not being able to access this information will have dramatic consequences for the organisation. This is also true if the information is no longer correct or is unwittingly divulged to others.

[10] https://csrc.nist.gov/pubs/ir/8286/d/final

[11] https://www.rijksoverheid.nl/documenten/rapporten/2022/11/28/tk-bijlage-dreigingsbeeld-statelijke-actoren-2

[12] Cognitive bias refers to thinking errors that result from the way in which people process and interpret information. Such thinking errors can be based on a variety of causes.

For more information about cognitive bias, please refer to:

Psychology of intelligence analysis, Richards J. Heuer, Jr., 1999

[13] *Strategies for Addressing Bias in Insider Threat Programs*, Intelligence and National Security Committee, 2022

[14] The national government has a code of conduct, for example. It features paragraphs on dealing with confidential information and preventing data leaks.

https://www.rijksoverheid.nl/documenten/richtlijnen/2017/12/01/gedragscode-integriteit-rijk-gir

[15] *Bereid u voor op zero trust* [Prepare for zero trust], NCSC, 18 August 2021

[16] https://insights.sei.cmu.edu/documents/1260/2016_005_001_454627.pdf

[17] *Samenwerking in een ISAC* [Collaborating in an ISAC], NCSC, visited on 23 June 2023

[18] https://www.pwc.nl/nl/spotlight/assets/documents/pwc-spotlight-uitgave-2021-4.pdf

[19] For an overview of large-scale insider threat incidents, please refer to this blog: https://www.mandiant.com/resources/blog/insider-threat-impact-studies

[20] Statement from a session participant.

[21] Ponemon. *The Cost of Insider Risks Global Report 2023.* https://www.dtexsystems.com/resource-ponemon-insider-risks-global-report/

[22] Please refer to our publication on crisis management and crisis communication for digital incidents: https://www.ncsc.nl/documenten/publicaties/2022/maart/4/aandachtspunten-crisismanagement-en-crisiscommunicatie

[23] https://www.ncsc.nl/contact/wbni-melding-doen

[24] https://www.politie.nl/aangifte-of-melding-doen/

[25] https://www.autoriteitpersoonsgegevens.nl/datalek-melden

[26] https://www.aivd.nl/contact

[27] See *The Human Consequences of Ransomware Attacks* (isaca.org)

[28] Kübler-Ross, E., & Kessler, D. (2009). 'The Five Stages of Grief'. In Library of Congress Catalog in Publication Data (Ed.), *On grief and grieving* (pp. 7-30)

[29] The NCSC added this chapter at a later stage based on the results from earlier chapters and feedback received from several participants.

Published by
National Cyber Security Centre (NCSC-NL)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

maart 2024