EUROPEAN UNION AGENCY
FOR CYBERSECURITY

BEHAVIOURAL ASPECTS OF COOPERATION BETWEEN CSIRTS AND LE

Handbook, Document for trainers

DECEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

CONTACT

For contacting the authors please use CSIRT-LE-cooperation@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Alexandra Michota (ENISA), Andreas Mitrakas (ENISA), Constantinos Patsakis, Václav Stupka

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN: 978-92-9204-336-0, DOI: 10.2824/822352

TABLE OF CONTENTS

1. INTRODUCTION

1.1 THEMATIC AREA

In 2018, ENISA confirmed that cultural challenges also affect the cooperation between Computer Security Incident Response Teams (CSIRTs) and Law Enforcement (LE) and their interaction with the judiciary. The main difficulty is on the one hand, to allow the judiciary to better understand the technical language used by CSIRTs and on the other hand, support CSIRTs to translate the legal requirements into technical specifications. It seems that the three communities have different approaches to problems and modi operandi and they speak different 'languages': CSIRTs face the issues that arise from a technical viewpoint, while the judiciary need to address them from a legal perspective. LE has to relate with these two different mentalities and languages and 'mediate'.

Figure 1: ENISA training on CSIRT-LE cooperation - Syllabus

ENISA Training on CSIRT – LE Cooperation - Syllabus	
Keywords:	Computer Security Incident Response Teams (CSIRTS), Law Enforcement (LE), Judiciary, Cybercrime, Cooperation, Interaction, Cultural Challenges, Cybersecurity behaviour.
Background:	This module is intended to provide trainees with an understanding of the human aspects that could enhance this cooperation.
Method of teaching and learning:	• Class lectures, interactive learning (class discussions, group work) and practical problems solved in class. • Case studies are assigned to the trainees and are reviewed in class.
Recommended material:	• ENISA reports • ENISA presentations • Trainer's notes based on recommended material and sources

- ### Learning outcomes

As a result of attending this course, the trainee should be able to:

- Analyse the current cybersecurity stance of the organisation, and carrying out an in-depth analysis of the causes of any problem(s)
- Demonstrate knowledge of the ENISA model of analysis and intervention for organisations to systematically plan and implement changes to address human aspects of cybersecurity
- Better understand how to fit security into the business, breaking down silos and leveraging other organisational capabilities; measures to improve security behaviour; using CSIRTs as reference organization model.

- **Target audience**

  The intended target audience are CSIRTs (mainly national and governmental CSIRTs but not limited to them), LE, as well as individuals and organisations with an interest in Cybersecurity.

- **Course Duration**

  4 hours

- **Frequency**

  At least yearly

2. GENERAL DESCRIPTION

2.1 IMPORTANCE OF COOPERATION BETWEEN CSIRTs AND LE

CSIRTs do not have the powers of LE and LE does not have access to information and expertise held by CSIRTs. It is therefore important for these communities to cooperate. However, technical, legal, organisational and cultural challenges can render this cooperation complicated. In addition, those challenges are dealt with differently in each country. A comparison of these different approaches is rather valuable when examining this cooperation. The studies developed by ENISA provide valuable insight into the current state of cooperation and recommendations on how to improve it.

Taking into consideration that cybersecurity incidents do not always correspond to cybercrimes, cooperation between these entities does not take place in all cases.

- Cybercrime: "crimes having a computer as a target and crimes where computer is a tool to commit traditional or new crimes”.
- Cybersecurity incident: “any event having an actual adverse effect on the security of a network and information system”.

Cybercrimes sometimes indeed relate to cybersecurity incidents. Nonetheless, in other cases, cybercrimes that are not related to cybersecurity incidents or that eventually are not reported may occur.

The CSIRT community has materially different duties and objectives than the LE community, depending as well on the type of each CSIRT community (governmental, national, sectoral, etc.) and LE (regional, national, federal, international, etc.). However, when dealing with a potential cybersecurity incident/cybercrime, each community should consider the outreach to other actors that could be involved, keeping in mind the multiple ways of cooperation and the importance of receiving reciprocal feedback on a case. Additional stakeholders may be approached in this cooperation process, such as the judiciary, service operators and service providers, intelligence services, military and international agencies.

Both formal and informal procedures may be followed in this cooperation process with the purpose of achieving each community’s objective of mitigating incidents and prosecuting crimes, depending also on each community’s hierarchical or flat structure, the classification level and the sophistication of the exchanged information. Formal procedures may have the form of an official written request for information regarding a specific case, while informal could have the form of information shared orally during an informal phone call. This cooperation channel may be direct or supported through appointed liaison officers, whose role sometimes has been pointed out as a very important one.

2.1.1 Introduction to behavioural aspects on CSIRT-LE cooperation

The human factor is perceived as a component and at the same time, as “the weakest link” in cybersecurity. (ENISA, 2019) More precisely, humans are often considered to be a top factor contributing to cybersecurity threats. Security policies, mechanisms and sanctions attempt to regulate the human behaviour and cybersecurity experts are constantly looking for ways to mitigate human-induced risks. However, many approaches for mitigating these risks are largely ineffective or even flawed, especially when not taking into consideration the human nature.

In addition, the human factor could also be one of the burdens in the cooperation between communities. For example, if there is lack of trust, training, or knowledge about cooperation opportunities, members of those communities would not be able nor willing to cooperate. Described methods could therefore be used to analyse causes for this lack of cooperation and introduce measures to strengthen it.

Nevertheless, it is not possible to approach human behaviour purely technically. Instead, knowledge of human behavioural science is necessary. “Behavioural science” encompasses a wide range of disciplines (sociology, ethnography, anthropology, human biology, behavioural economics etc.) and takes into account also capabilities, limitations, goals, norms and values of humans when identifying effective tools to manage human factor in cybersecurity.

2.1.2 Evidence reviews

A plethora of academic research has dealt with the role of the human in cybersecurity. ENISA has conducted four **evidence reviews** (ENISA, 2019) of this research focused on:

- Survey studies using social science constructs
- Models of cyber-security attitudes and behaviour
- Qualitative and mixed method studies
- Current practices

Despite the different methods applied and the different approaches followed, all four evidence reviews have drawn the following similar conclusions:

1) Stressing the importance of utilizing measurable metrics in assessing the human factor in cybersecurity and evaluating the efficiency of implemented measures in solving the identified issues.
2) It has been observed that many of the models currently used to study human aspects of cybersecurity are poor to moderate fit to the actual human behaviour. On that note, ENISA identified two behavioural models namely COM-B[1] and B=MAT[2] that are a good fit to deal with behavioural aspects of cybersecurity.
3) Additionally, increasing evidence demonstrates that raising the users’ understanding of the threat posed by cybersecurity breaches, or even raising the fear of the consequences, is not an effective tool for changing behaviour. This relates also to the cooperation aspect between the CSIRT and LE community. For example, CSIRTs are not aware of the fact that their mitigating actions could destroy valuable evidence needed by the LE and they are not expected to collect or protect such evidence. Similarly if LE agencies are not aware of the data and expertise that CSIRTs can provide, they are not expected to seek or request assistance.
4) Finally, it has been noted that there is a moderately reliable link between the people’s ability to cope in face of threats and their cybersecurity behaviour.

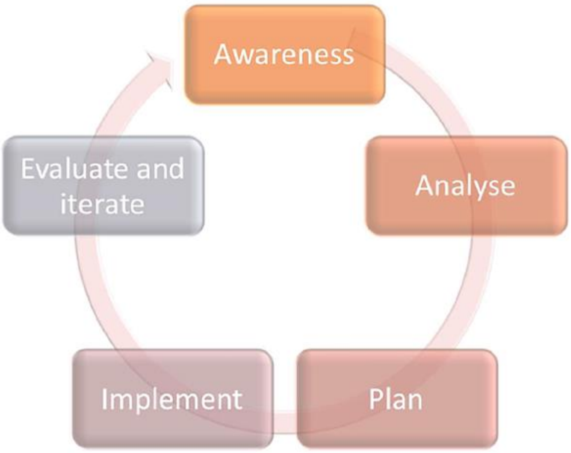
2.2 PRACTICAL GUIDELINES

A practical approach to the behavioural aspects of cybersecurity is hereby presented through a circular, ongoing process that seeks to maintain **awareness** of an organisations’ security stance and the human aspects that contribute to that stance, followed by in-depth **analysis** of why vulnerabilities might exist (and re-visiting previous efforts to address them). This is followed by a strategic **planning** stage where available options are weighed up and interventions are

[1] ENISA report on Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity, p.22
[2] ENISA report on Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity, p.23

designed. Critical at this stage is to identify what the goal of any change is in order to measure the success (or failure) of the interventions that are onwards **implemented**. This leads to a final part of the cycle where the effort achieved is **evaluated** against the original goals **and iterated**, by restarting the awareness process with the experience gained.

Figure 2: Circular approach of the behavioural aspects of cybersecurity



2.2.1 Awareness

At this first stage, the goal is to gain an understanding of an organisation's current cybersecurity status, and the ways in which human factors might support or detract from that defensive stance. The specific methodology that will be adopted by the concerned organisation will in part depend on its maturity in terms of both cyber-security and data collection and analysis.

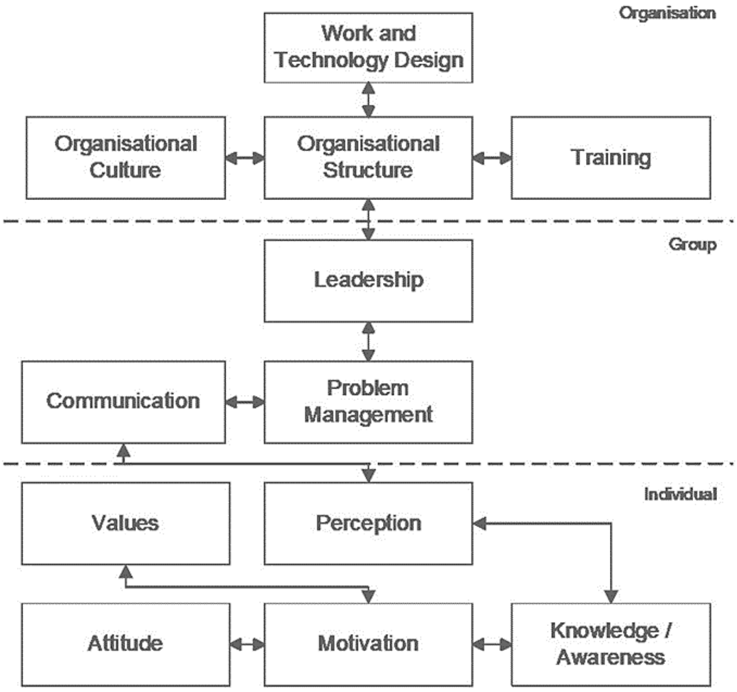
There is a variety of statistical measures an organisation might use to gain awareness, as well as ways in which groups can gain an understanding of security culture through quantitative (e.g. surveys) and qualitative (e.g. interviews) methods. It is preferable to use multiple methods that probe multiple levels in an organization. However the methods chosen could vary between different organisations and communities, for CSIRTs, LE and the judiciary practical exercise, and focus groups could be suggested.

2.2.1.1 Organizational behaviour model

The model of organizational behaviour can be used to guide an open approach to gaining awareness at different levels within an organization. The results of this model indicate concrete starting points for improving and changing the cybersecurity culture.

Main pain points most often focus not on awareness and training, but instead on supporting domains that strongly influence the work environment of the users, like work and technology design, organizational structure, leadership and problem management.

Figure 3: Organisational behaviour model to assess cybersecurity culture (adapted from Schlienger, 2006)



In the case of CSIRT-LE cooperation, we can use a "Segregation of duties" (SoD) matrix for the same purpose as the organisational behaviour model. The SoD matrix might help the three communities to reach a better understanding of each other's duties assigned by the roles each community plays when dealing with cybersecurity incidents/cybercrimes, and then avoid mutual hindering and non-cooperation. A SoD matrix (see Figure 4 — Example of segregation of duties matrix) could be drafted at national level. As shown in the SoD template below, the CSIRTs, LE, judges and prosecutors have to identify the key responsibilities for their communities and then link them with the skills required to fulfil these duties. SoD matrices are usually used to ensure compliance with laws and regulations.

Figure 4: Example of 'Segregation of Duties' matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutor	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training	✓	✓	✓	✓	Problem-solving and critical thinking skills
During the incident/crime					
Evidence collection	✓	✓		✓	Knowledge of what kind of data to collect; organisation skills
Duty to inform other stakeholders/authorities	✓				Obligations and rules for information sharing among communities
Leading the criminal investigation			✓	✓	Knowledge of the incident response plan; leadership skills
Post incident/crime					
Admitting and assessing the evidence			✓	✓	Evidence in a criminal trial
Reviewing the response and update policies and procedures	✓				Knowledge how to draft an incident response and procedures

2.2.2 Analyse

The goal of this stage is to analyse what may be the root causes of weaknesses or problems that may be identified.

This analysis can be divided into two core elements:

1) Analysis of the problem (and root causes), and
2) Choice of appropriate method to study the problem (and to measure success).

Again, a multi-method approach is particularly suitable in this stage. The use of statistical data, surveys and other measurable approaches might not be the best option (surveys are time consuming and measurable data are not useful for the analysis of security culture, etc.). Alternatively, a more suitable method might be to use workgroups or focus groups to identify whether a behaviour is not being conducted due to ability, motivation or another factor before designing any intervention.

Selecting the appropriate instrument for any analysis or evaluation process is essential as this could determine the collection of clear and relevant information. When choosing or designing a measurement instrument, it is advised to follow the common "SMART" criteria. SMART stands for Specific, Measurable, Actionable, Relevant and Time-related.

- **Specific →** Does it target a specific area for improvement?
- **Measurable →** Is it quantifiable or does it at least suggest an indicator of progress?
- **Actionable →** Can the results be used to define concrete improvement actions?
- **Relevant →** Is it relevant for your organisation taking your context into consideration and does everybody understands the result?
- **Time Related →** Can it be implemented in the desired time-frame for your organisation?

2.2.2.1 Causes of behaviour

Practitioners should consider conducting a more detailed analysis of the causes or barriers of the desired behaviour. To this end, ENISA has identified two approaches to identifying the causes of (non) behaviour that are particularly suitable for cybersecurity:

- **COM-B behaviour model**
- **B=MAT behaviour model**

ENISA proposes then that the COM-B model is used to identify why a desired behaviour may or may not be carried, and that the B=MAT model is used to guide thinking about possible interventions.

A series of recommendations on the selection of valid, reliable measures that would allow practitioners to track changes in security behaviour or culture, are provided in the technical annex (ENISA, 2019) of the relevant study.

COM-B MODEL:

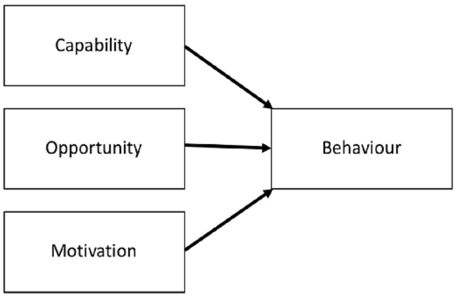
According to this model, behaviour is dependent on 3 interrelated factors:

1. **Capability** → Can the individuals concerned perform an action? Do they know how to?
2. **Opportunity** → Do the individuals have the chance to perform the action? and
3. **Motivation** → Are the individuals motivated to perform the action?

And the **type of intervention** depends upon the cause of the (non) behaviour – for example:

- Lack of capability → skills-building;
- Lack of opportunity → development of tools;
- Lack of motivation → education, awareness, reward/punishment.

Figure 5: COM-B model (adapted from Michie et al., 2011)



B=MAT MODEL:

According to this B=MAT model, the type of persuasion required to bring about a behaviour or generate an action depends on the individual’s motivation and ability to perform the act, with different interventions needed to increase either the motivation or the ability. Based on the B=MAT model, the likelihood of a behaviour occurring is a product of motivation (M), Ability (A), and the appropriate trigger (T).

For instance, if people are motivated to undertake a task (e.g. updating software), then improving their ability (e.g. by reducing the cost or effort) should increase the likelihood of carrying out the behaviour. Similarly, if an action is simple and the person is able to complete it, then addressing motivation (e.g. fear of outcome, hopes, pain) should also increase the likelihood. Once motivation and ability are addressed, according to this model, we should then look to triggers that signal to people that a behaviour is required.

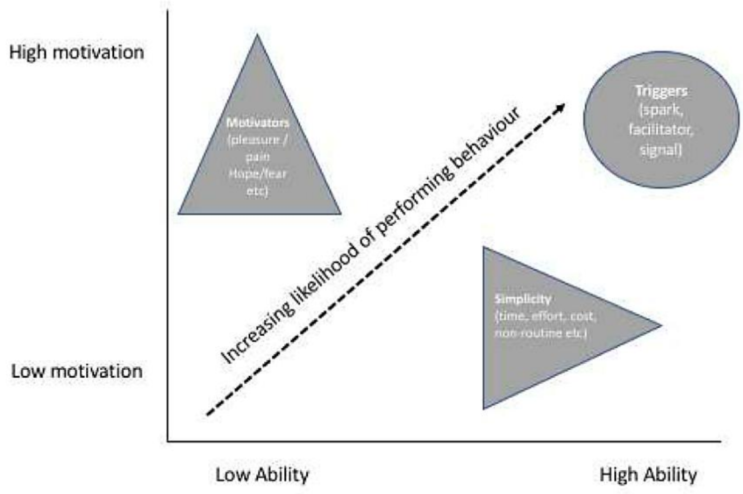
These triggers can take the form of:

1) Signals (e.g. a message saying that updates are ready to be installed), best used when someone has motivation and ability;

2) Sparks that seek to motivate as well as trigger a behaviour (e.g. warning that the computer will be at risk if the update isn't installed); or

3) Facilitators that seek to both trigger a behaviour and make it easier (e.g. "just click here to download and install the update").

Figure 6: B=MAT model (adapted from Fogg, 2009)


High motivation
Low motivation
Motivators (pleasure / pain Hope/fear etc)
Increasing likelihood of performing behaviour
Triggers (spark, facilitator, signal)
Simplicity (time, effort, cost, non-routine etc)
Low Ability
High Ability

2.2.3 Plan

The next stage is to plan activities for the organization based on the outcomes of the previous completed stages of awareness and analysis. The exact nature of that planning will be determined by the diagnosis performed around the problem in the previous two stages. The activities planned should target the problems identified and consider mitigation measures from multiple perspectives. In some cases to mitigate one problem it would be necessary to implement multiple controls (for instance changes in policies and skills building).

The following table explains some responses that might be used to address issues caused by lack of capability, opportunity or motivation and audit.

Figure 7: Example potential responses

Probable cause	Example organisational responses	Common activities
Capability	Redesign policies & tools Education Skill-building Restrict	'Fix security' - review & change policies & tools Build employee security skills ('proper' training) Remove admin rights
Motivation	Awareness campaigns Incentives Organisational response	Security culture programme 'Good security' awards, security performance as Key Performance Indicator Visible organisational reaction to all policy breaches & errors
Opportunity	Engage employees in security review/design Security champions Nudge / prompt	Identify policies & tools that cause friction Identify & support employees who want to build security skills Support transition to secure habits through alerts & reminders
Audit[3]	ISO/IEC 27001 PCI/DSS	Monitoring Identify deficiencies Remediation action plans

2.2.4 Implement

Changing behaviour or even the overall organisational culture is likely to be a long-term project. Some techniques and approaches may yield immediate results. In other cases, it may take considerably longer, not only because habits take time to form, but also because restructuring security policies and practises to align with organisational goals and work tasks is likely to be a considerable undertaking. The implementation stage should also be monitored as a part of the process through interim measurements and analysis, given its ongoing nature.

2.2.5 Evaluate and iterate

The evaluation stage of any intervention can take two main forms:

- **Process evaluation** seeks to identify how the attempted change or intervention ran (Was it implemented correctly? How did the different stakeholders interact? What process elements could be improved?).
- **Outcome evaluation** seeks to identify whether or not the change achieved its stated goals.

This relates closely to the issues around measurement and metrics. It is critical that practitioners know what success looks like and be able to identify what metrics or measures will change in response to any intervention ahead of time.

[3] While audit results are the most complete metrics, today's standards and best practice catalogues do not cover the full spectrum of social and psychological items that influence human behaviour

2.3 RECOMMENDATIONS TO PRACTITIONERS

2.3.1.1 Policy makers

Increasing cybersecurity literacy and skills is an evidenced method to support citizens in protecting their cybersecurity. Further ways in which policy makers can support cybersecurity can be summarized as follows:

- Ensuring responsibilities are assigned based on employees' skills;
- Signposting trustworthy competence;
- Promoting collaboration and trust-building; respect and ban disrespectful language about stakeholders;
- Supporting the development and use of evidence-based metrics and measures to assess cybersecurity skills, knowledge and organisational culture;
- Encouraging and supporting collaboration between technical and social/ behavioural domain experts in tackling cybersecurity behaviours;
- Awareness of threats do not lead to protective action. Citizens (and workers) need to develop skills in order to avoid the threat and gain a better understanding.

2.3.1.2 Management leadership

The organisation's management leadership needs to take an active role to ensure that the security behaviour requested to be demonstrated by the staff is actually feasible in the business context.

- **Take responsibility:** They need to decide which security risks should be managed, and commit the resources required. This includes the cost of buying security equipment and services, but also the total cost of operating those security measures, meaning:
    - the time that staff have to spend on security,
    - the time and effort required to change non-secure behaviours into secure ones,
    - business that may be lost as a result of staff following the policies,
    - building the skills needed by different parts of the organisation.
- **Lead by example:** They also need to follow security policies that are a high-value target. Management leadership should commit a portion of their time to work with security specialists and staff to finding workable solutions in their areas of expertise (e.g. operations, finance, marketing)
- **Manage organisation to help security:** Effective management of security can draw knowledge and tools from safety. Similarly, human resources can assist with the design of incentives and KPIs, and helping to identify staff who are interested in acquiring new skills and take on extra responsibilities. Communications and marketing can help to improve effectiveness of awareness materials. Leveraging your own resources and breaking down silos to solve problems is a management task.

2.3.1.3 CISO and security specialists

Studies with CISOs show a need for a shift in what the job entails, and how to work so as to be effective.

- **Calculate the impact of policies:** Security policies and measures can only be effective if they are adopted and used correctly. To ensure this, CISOs need to know the time and effort required to achieve compliance, before putting a security measure in place.
- **Be visible and approachable:** CISOs should be security leaders, not policemen. To engage staff, they need to be visible and approachable at all times. To build trust, they

need to listen and negotiate, rather than try to 'stamp out' non-compliance and throttle innovation and experimentation.

- **Build soft skills:** CISOs and other security specialists need to acquire the 'soft skills' to do their job effectively.
- **Stop verbally bashing people:** Effective engagement and trust require respect for others. The security profession needs to revise its perspective of non-specialists, and accept they are the only stakeholders in the ecosystem for whom security is the primary role.

2.3.1.4 CSIRTs & SOCs

Incident response teams and security operations centre (SOC) managers are among the most important assets in the fight against cyber threats. Enabling them to perform well is clearly important - and so is having sufficient capacity to fill positions. Organisations need to take steps to manage this precious resource effectively. Therefore managers are suggested to:

- **Look after their staff:** To prevent the work overload of the staff, organisations need to ensure sufficient staffing levels. This can challenging for the CSIRTs staffing where demand is high during incidents, but lower during other times. In addition, more flexible task allocation is advised. For example, having staff work on tool development, skills resources and team building and knowledge-sharing between teams - would be a way forward. Managing incidents that affect safety and cyber physical systems can be stressful and therefore organisations need appropriate support to help staff deal with the aftermath.
- **Invest in training and personal growth:** Having the skills, and ability to grow is a key for effective performance, confidence and job satisfaction of security staff. In a rapidly evolving threat environment, funding for research and specialist skills is essential. Some skill-building can happen through online courses, but hands-on case analysis, master classes and war gaming are more engaging and effective.
- **Support team and multi-team approaches:** Effective cybersecurity defence is a team sport - building trust among analyst teams, between them and the management is essential. This is a new problem for many organisations, so some investment in external expertise (research or consultancy) may be required

2.3.1.5 Software developers

The review of literature on software developers revealed that they - like other staff - are currently caught between producing code and delivering products, and make sure what they deliver is secure. High-impact first steps can be taken to make it easy for developers to produce more secure code by:

- using secure coding practices e.g. Safecode
- ensuring that platforms, tools, APIs they use have secure defaults and settings,

and that code that is frequently copied is vetted and made safe.

Software developers should:

- know that they are not and should not be security experts; however, they need to think about security from the start (security by design) and throughout the whole lifecycle (secure software development lifecycle)
- know that security experts can advise and support them; they need to work with them, and provide them with all the information required
- make sure that security mechanisms used in their code are effective and usable. They should be able to answer the following questions: "How much time will it take?", "Will

they be able to understand the decisions you are asking them to take?". They also need to work with experts in usability matters to help them design and test for usable security.

2.3.1.6 Developers' managers and trainers

Even organisations who claimed to have processes to ensure their software was secure (and usable) often have no criteria or metrics by which staff could determine if it was so. Furthermore, problems arising with security, and usability of security, tend to end up with help desks and staff support, rather than the developers. If they did, they would not only have an incentive to reduce those problems, but learn over time how to avoid them in the first place.

- Similar to other staff, developers need time to keep up-to-date with threats and update their skills.
- Assigning developers to work on help desks and support, they experience first-hand the consequences of failing security.
- It is also needed to include the number of support calls and other costs associated with insecure or unusable code in performance evaluation.

Those who educate developers - computer science and software engineering courses - do currently not teach security-by-design. Some of them offer specialist modules in security, but this is mostly optional. Instead:

- Security courses should be compulsory in academic computer science and engineering courses.
- Programming should be taught as an integral part of computer science studies; security aspects should be included in the syllabus of programming modules.
- Material in all other modules should be reviewed to remove or annotate examples that would lead to insecure code.

2.3.1.7 Awareness raising managers

Our reviews clearly noted that awareness based around threat is not effective. And yet, many awareness campaigns still spend considerable time and energy repeating the scale and vulnerability of cybersecurity threats. Whether we have reached "peak awareness" may be unknown, but the evidence does support that we should be aiming to provide users with the skills in order to cope with threats, and the knowledge that a simple act can be effective protection (e.g. accepting updates immediately). While efforts to further understand the attitudes and beliefs of a population might be worthwhile, they should be linked closely to an analysis that leads to tailored campaigns based on identified issues. The COM-B and Fogg models outlined in the report give a structure to begin strategically tailoring awareness campaigns towards specific causes of a (non) behaviour.

2.4 SUMMARY

Effective cybersecurity policies need to take into consideration the human factor and implement appropriate technical and organisational measures in order to mitigate human-induced risks. The behavioural aspects have a significant role to play in the way cybercrime response is challenged, even more importantly when the cooperation among different communities is crossing organizational and cultural boundaries, as in the case of cooperation between CSIRTs, LE and the judiciary.

To approach and regulate the behavioural aspects of human intervention in the cybersecurity framework, a socio-technical perspective is required, that examines the actions (and decisions) of policy makers and security professionals; systems designers, developers and requirements engineers; and end users. By utilizing behavioural studies and by assessing the needs and weaknesses within an organisation, improvement can be achieved through the development of a better understanding of the organisational practices, the investment on awareness raising initiatives and on the use of appropriate training and tools.

3. CASE STUDY

3.1 CASE STUDY – CSIRT APPROACH

The objective of this case study is to explain how to analyse and identify root causes for security weaknesses in human behaviour, that occur within an organization, and how to identify and implement effective and proportional measures to address these causes.

This case study should be conducted in groups so that the different results and approaches of each group can be compared. Then, the advantages and disadvantages of the individual solutions should be discussed.

Figure 8: Main objective of the case study

Main Objective	
Targeted Audience	CISOs, security staff, CSIRT members, etc.
Total Duration	30 minutes
Scenario	Trainee is a CISO conducting analysis of behavioural aspects of cybersecurity within the organization. His goal is to address main security weaknesses in staff behaviour.
Task 1	Suggest measures to reach a better understanding of reasons for identified false or improper procedures
Task 2	Choose appropriate method and metric to analyse and study the problem
Task 3	Use COM-B and B=MAT models to identify causes of unwanted (non)behaviour
Task 4	Based on previous analysis identify appropriate measures to resolve the problem
Task 5	Identify expected activities of relevant stakeholders by filling in the SoD matrix

3.1.1 Objectives

- To learn how to apply the ENISA model of analysis and intervention for CSIRTs to systematically plan and implement changes to address human aspects of cybersecurity
- To evaluate your ability to identify suitable metrics for studying and analysis of problems within the CSIRT constituency
- To evaluate your ability to analyse the causes of these problems using COM-B and B=MAT models
- To validate which security measures can be used to address specific security problems and their causes

3.1.2 Scenario

3.1.2.1 Organisational profile

Your organisation is a national CSIRT team responsible for detection and mitigation of cybersecurity incidents/cybercrimes within your constituency which consists of public and private organisations including operators of critical information systems. Your staff is expected to provide support to your constituency and cooperation to other relevant governmental bodies including law enforcement authorities. In your internal policies it is stated that your staff should report any identified crimes to LE and also provide any necessary support and assistance during criminal investigation.

3.1.2.2 Before the breach

Your CSIRT provided to your constituency guidelines on how to identify and report incidents. These guidelines explained how to identify and report phishing attack and that their employees should never provide their credentials via e-mail.

3.1.2.3 Initial response

Breach notification

- Your CSIRT team received multiple reports of a phishing attack within your constituency.
- The attacker implemented spear phishing attack vector targeted at the management of the leading electricity-grid operator. The phishing email contained a link to login website that looked like login website to the company information system.

Response of the CSIRT team

- CSIRT staff collected content data and related meta-data of the attack including email/IP address used to send the phishing mail, email metadata, screenshot and address of the phishing website.
- CSIRT implemented mitigation measures including blacklisting the attacker’s e-mail address, source of the malicious website, updating the spam filter and firewall settings, requesting the change of passwords of all managers within the company, and issuing a warning about the attack and distributing it within the constituency.
- The CSIRT did not file a criminal complaint.

Criminal investigation

- The criminal complaint was filed a week later by one of the targeted managers.
- LE, based on the complaint filed, requested any data related to the incident.
- Some of the data were missing, because the CSIRT team had resolved the incident by implementing the abovementioned measures. The rest of the data (screenshots of the malicious message and source email and IP address) was provided to LE.
- Afterwards, the police requested additional information about the possible source of attack – primarily information about possible sources of employee data, and list of users with access to company’s mailboxes.
- The provision of this information was refused for personal data protection reasons, and the police referred to the company's management.
- The police were not able to identify the attacker due to lack of evidence and closed the case.
- About a year later, somebody launched a similar attack against a different company in the constituency and successfully gained access to valuable trade secrets and critical infrastructure management systems.

Investigation analysis

- The police stated that the second attack was probably launched by the same attacker as in the previous case, and therefore could be prevented.

- Analysis of this incident suggested, that better cooperation with the police would make it more likely, that the attacker would be caught and prosecuted.
- The CSIRT therefore decided to analyse causes of insufficient cooperation and identify measures that would allow and motivate the staff to improve it.

3.1.3 Tasks

Your task is to analyse how to motivate CSIRT staff to apply improved practices in these areas and identify measures to do so using ENISA model.

3.1.3.1 Identify expected behaviour of CSIRT members

Describe the correct procedure that should be followed by the CSIRT in order to ensure effective cooperation with LE and identify areas highlighting the main drawbacks of the procedure applied in the described scenario. As a guidance, you can use the segregation of duties matrix.

For each of identified areas identify the best measures that can be implemented to reach a better understanding of identified issues and drawbacks. You can suggest any suitable measure, like further analysis, survey, group discussions, statistical analysis, etc.

Figure 9: List of suggested measures

Area	Suggested measure
Identification and reporting of crimes	Analysis of internal guidelines, survey among CSIRT operators, group discussion with LE, training scenario with LE
Collection and sharing evidence	Availability of suitable tools, analysis of internal guidelines, analysis of applicable law, survey among CSIRT operators.
Active support to LE	Discussion with LE, identification of suitable methods of cooperation, analysis of relevant law.

3.1.3.2 Choose appropriate metric

Next step would be to choose a suitable metric to evaluate the severity of the problems identified and measure the effectiveness of measures to resolve these problems. Metrics should be chosen while following common SMART criteria. SMART stands for Specific (Does it target a specific area for improvement?), Measurable (Is it quantifiable or does it at least suggest an indicator of progress?), Actionable (Can the results be used to define concrete improvement actions?), Relevant (Is it relevant for your organisation taking your context into consideration and does everybody understands the result?) and Time-related.

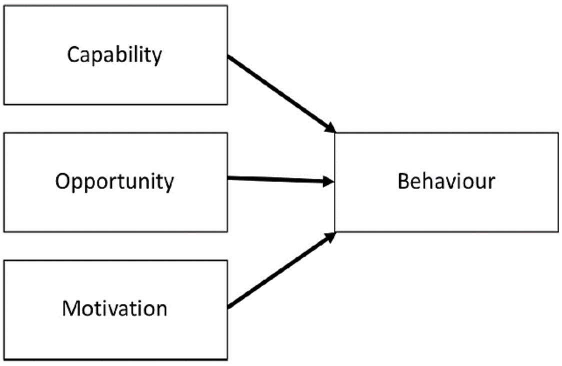
Figure 10: List of suggested metrics

Area	Suggested metric
Identification and reporting of crimes	Number of filed criminal complaints, number of identified crimes, the ratio between the number of incidents and the identified offenses, existence of taxonomy, etc.
Collection and sharing of evidence	Amount of shared evidence, number of available tools for evidence gathering, existence of guidelines, etc.
Active support to LE	Existence of guidelines, number of cases of active support, etc.

3.1.3.3 Identify causes of unwanted (non)behaviour

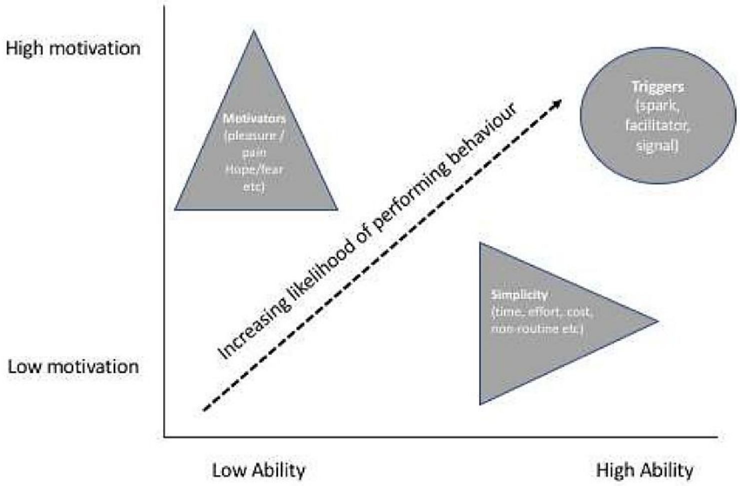
In this step you should use COM-B and/or B=MAT models to identify causes of unwanted (non) behaviour.

Figure 11: COM-B model (adapted from Michie et al., 2011)



The ‘COM-B’ model argues that whether or not a behaviour is enacted is dependent upon three interrelated factors: 1) capability (Can they do it? Do they know how to?); 2) opportunity (Do they have the chance to do the action?); and 3) motivation (Are they motivated to lock the screen?).

Figure 12: B=MAT model (adapted from Fogg, 2009)


High motivation
Low motivation
Low Ability
High Ability
Motivators (pleasure / pain Hope/fear etc)
Increasing likelihood of performing behaviour
Triggers (spark, facilitator, signal)
Simplicity (time, effort, cost, non-routine etc)

According to the B=MAT model, the type of persuasion required to bring about a behaviour depends on where it lies in the motivation/ability dimensions, with different interventions needed to increase either motivation or ability. Once motivation and ability are addressed, we should then look to triggers that signal to people that a behaviour is required.

Both models can be used to find the cause or causes for (non) behaviour. For instance, if employees are required to use electronic signatures for communication but they are not using them, the cause could be in the realm of capability (they are unable to use electronic signature, because it is technically too complicated), opportunity (they can use it, but they do not have proper tools to do so), motivation (they know they should use it, but there is no reward if they do so or punishment if they do not), or triggers (they are not requested by the information system to attach the signature).

Figure 13: List of suggested measures

Area	Suggested measures
Identification and reporting of crimes	Motivation – operators do not see any benefits of cooperation; Simplicity – operators do not know how to identify or report crimes; Triggers – the incident handling system does not suggest reporting offenses.
Collection and sharing of evidence	Motivation – operators do not need specific kinds of evidence to mitigate the incident; Simplicity – they do not have tools to collect, store or safely share the evidence; Triggers – there is no trigger in internal guidelines.
Active support to LE	Motivation – It takes too much time to help LE; Simplicity – they do not know what LE needs and their procedures; Triggers – LE does not request support.

3.1.3.4 Identify appropriate measures to resolve problems

In this step, you should identify measures/interventions that can partially or completely resolve identified problems. For this purpose, you can use identified causes as a guidance of what kinds of measures should be used.

For instance, if people are motivated to undertake a task, then addressing their ability should increase the likelihood of carrying out the behaviour. Similarly, if an action is simple and the person is able to complete it, then addressing motivation should also increase the likelihood. The problem could be also resolved adding triggers, which signal that a behaviour is required (like notifications in the information systems, warnings distributed within the organization, etc.)

Figure 14: List of suggested measures

Area	Suggested measure
Identification and reporting of crimes	Implementation of taxonomy and internal guidelines, training on how LE can help CSIRTs, templates of criminal complaint, etc.
Collection and sharing of evidence	Tools for collection, storage and sharing of evidence, internal guidelines on what to collect and how to collect it, training with LE on evidence collection and sharing, etc.
Active support to LE	Training with LE, common guidelines on cooperation, etc.

3.1.3.5 Segregation of Duties

In this step, use the SoD matrix (Figure 15) to identify, what type of activities can be performed or facilitated by your CSIRT, and what you expect from LE and the judiciary. The SoD matrix should help you to reach a better understanding of each other's duties based on the roles each community has throughout the cybercrime investigation lifecycle.

3.1.3.6 Outcomes

After following all steps, each group should be able to identify the causes of unwanted (non) behaviour, to implement effective and proportional measures to address these causes and to measure the effectiveness of the solutions selected.

We would suggest this case study to be conducted in groups so that the different results and approaches of each group can be compared. Then, the advantages and disadvantages of the individual solutions should be presented and discussed.

Figure 15: ‘Segregation of Duties’ matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training	✓	✓	✓	✓	Problem-solving and critical thinking skills
Collecting cyber threat intelligence	✓	✓		✓	Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats	✓	✓		✓	Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats	✓				Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime	✓	✓			Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cybersecurity incident/crime	✓	✓			Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cybersecurity incident/crime	✓	✓		✓	Incident and crime classification and identification
Identify the type and severity of the compromise	✓	✓		✓	Knowledge of cyber threats and incident response procedures
Evidence collection	✓	✓		✓	Knowledge of what kind of data to collect; organisation skills
Providing technical expertise	✓				Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial	✓	✓		✓	Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)	✓			✓	Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime	✓	✓		✓	Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)	✓				Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling	✓				Communication skills; communication channels
Mitigation of an incident	✓				Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation		✓		✓	Knowledge of the legal framework; decision-making skills
Leading the criminal investigation			✓	✓	Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation			✓	✓	Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE		✓	✓	✓	Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution	✓	✓	✓	✓	Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery	✓				Technical skills
Protecting the constituency	✓				Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view	✓				Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence		✓	✓	✓	Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE			✓	✓	Testimonies in a criminal trial
Admitting and assessing the evidence			✓	✓	Evidence in a criminal trial
Judging who committed a crime			✓		Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost	✓	✓	✓	✓	Evaluation skills
Reviewing the response and update policies and procedures	✓				Knowledge how to draft an incident response and procedures

**Differences may be highlighted in this matrix depending on the legal framework of each Member State.*

This is just an indicative example.

3.2 CASE STUDY – LE APPROACH

The objective of this case study is to explain how to analyse and identify root causes for weaknesses in human behaviour, that occur within an organization, and how to identify and implement effective and proportional measures to address these causes.

This case study should be conducted in groups so that the different results and approaches of each group can be compared. Then, the advantages and disadvantages of the individual solutions should be discussed.

Figure 16: Main objective of the case study

Main Objective	
Targeted Audience	LE, investigators, public prosecutors, etc.
Total Duration	30 minutes
Scenario	Trainee is an officer leading a cybercrime investigation unit, whose responsibility and goal is to implement measures to motivate his staff to better cooperate with CSIRTs.
Task 1	Suggest measures to reach a better understanding of reasons for identified false or improper procedures
Task 2	Choose appropriate methods and metrics to analyse and study the problem
Task 3	Use COM-B and B=MAT models to identify causes of unwanted (non)behaviour
Task 4	Based on previous analysis, identify appropriate measures to resolve the problem
Task 5	Identify expected activities of relevant stakeholders by filling in the SoD matrix

3.2.1 Objectives

- To learn how to apply ENISA model of analysis and intervention for LE to systematically plan and implement changes to address human aspects of cybersecurity cooperation
- To evaluate your ability to identify suitable metrics for studying and analysis of problems within the LE unit
- To evaluate your ability to analyse the causes of these problems using COM-B and B=MAT models
- To validate which security measures can be used to address specific security problems and their causes.

3.2.2 Scenario

3.2.2.1 Organisational profile

Your unit is specialised in investigating and prosecuting cybercrimes. You often encounter situations where cooperation with CSIRT teams is necessary, either because the investigated crime threatens infrastructures or information systems within your constituency, or because you need to use the specific knowledge or equipment that CSIRT teams have. There are however no specific guidelines or laws, that would allow or require closer cooperation with the CSIRTs.

3.2.2.2 Before the breach

As a precautionary activity, you have informed in the last six months the media about new types of attacks directed against critical infrastructures. These were attacks that occurred mainly abroad and consisted of exploiting the vulnerability of SCADA systems used to control industrial plants.

3.2.2.3 Initial response

Breach notification

- In response to a report published in the news, a local power plant control system operator contacted you to inform you that their systems bear signs of a potential attack on SCADA systems.

Criminal investigation

- In cooperation with the staff of the power plant the investigator managed to secure an infected SCADA router, which allowed communication between SCADA infrastructure and information systems of the power plant
- By using the national ICT experts list, you have requested an expert examination to identify the sources of infection. Since the expert did not have the appropriate equipment to analyse the router, he concluded that the device had to be infected by an employee who had physical access to it.
- The following investigations were aimed at identifying employees with access, interrogating them and analysing camera and access records.
- However, this did not lead to the identification of the offender and the investigation was thus closed.
- The investigator informed the company management about the findings of the investigation. In response, the management requested the CSIRT to perform security audits on all SCADA systems and, where appropriate, to replace or update them.

Response of the CSIRT team

- The CSIRT immediately contacted the investigator and he explained that some SCADA systems, including the infected router, are controlled remotely and therefore connected to the internet via an information system. This is the reason why the attack could not be conducted by an employee but instead, by an external source.
- The CSIRT also informed him that if they were aware of the ongoing investigation, they could provide not only their analytical tools and more data on the attack, but they could also trace the attacker using detection tools installed in their network.
- Later during the security audit, the CSIRT concluded, that since the incident was not directly addressed by the CSIRT team, the infection spread to critical systems during the installation of updates, and this could threaten the plant operation and lead to severe damage.
- Based on these facts, the company decided to file a complaint for incorrect police investigations.

Investigation analysis

- When handling the complaint, it was found that the investigator did not expect the CSIRT to be in charge of the security of industrial systems.
- In addition, despite the fact that the expert opinion contained information that the router in question has an interface for communication in the computer network, he did not try to contact the network infrastructure administrator.
- Finally, it was found that the expert who examined the router, did not have the necessary equipment, and that it would be much more effective, if the police had asked directly the administrators of the system or CSIRT to conduct the analysis.

3.2.3 Tasks

3.2.3.1 Identify expected behaviour of CSIRT members

Describe the correct procedure that should be followed by the CSIRT in order to ensure effective cooperation with LE and identify areas highlighting the main drawbacks of the procedure applied in the described scenario. As a guidance, you can use the segregation of duties matrix.

For each of identified areas identify the best measures that can be implemented to get better understanding of identified issues and drawbacks. You can suggest any suitable measure, like further analysis, survey, group discussions, statistical analysis, etc.

Figure 17: List of suggested measures

Area	Suggested measure
Awareness of functions of the CSIRT	Survey among investigators, cooperative training with CSIRTS.
Lack of cooperation with CSIRTs	Analysis of relevant guidelines and laws, survey among investigators, comparative analysis comparing procedures of other of foreign units etc.
Sharing of the information about the investigation	Analysis of relevant law, analysis of applicable guidelines, discussion groups with CSIRTs.

3.2.3.2 Choose appropriate metric

Next step would be to choose a suitable metric to evaluate the severity of the problems identified and measure the effect of measures to resolve these problems. Metrics should be chosen while following common SMART criteria. SMART stands for Specific (Does it target a specific area for improvement?), Measurable (Is it quantifiable or does it at least suggest an indicator of progress?), Actionable (Can the results be used to define concrete improvement actions?), Relevant (Is it relevant for your organisation taking your context into consideration and does everybody understands the result?) and Time-related.

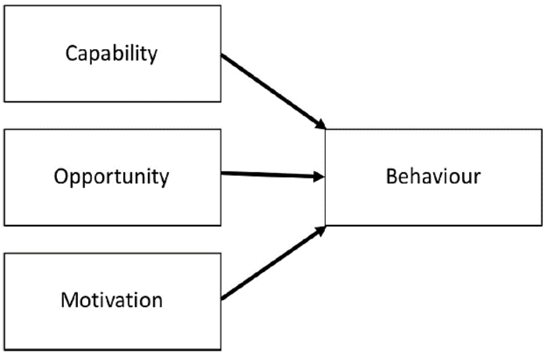
Figure 18: List of suggested metric

Area	Suggested metric
Awareness of functions of the CSIRT	Number of investigation where CSIRTs are involved, existing guidelines, awareness of functions and duties of CSIRTS, etc.
Lack of cooperation with CSIRTs	Existence of relevant guidelines, existence of list of contacts to relevant CSIRTS, number of cases where support from CSIRTs is requested, etc.
Sharing of the information about the investigation	Number of cases where information is shared or requested, existence of relevant guidelines and legal regulation, etc.

3.2.3.3 Identify causes of unwanted (non)behaviour

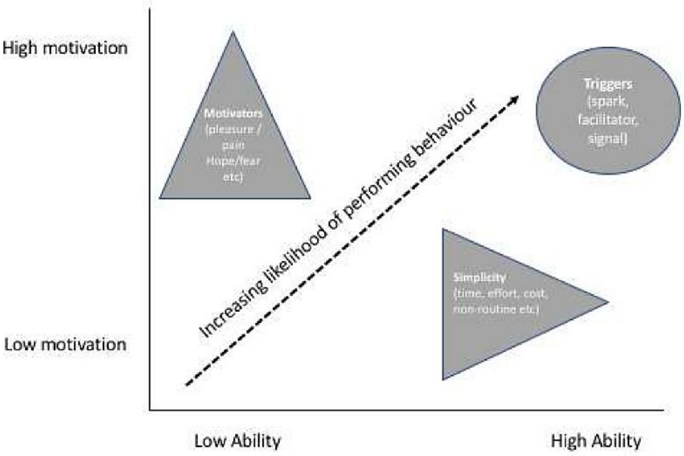
In this step you should use COM-B and/or B=MAT models to identify causes of unwanted (non) behaviour.

Figure 19: COM-B model (adapted from Michie et al., 2011)



The ‘COM-B’ model argues that whether or not a behaviour is enacted is dependent upon three interrelated factors: 1) capability (Can they do it? Do they know how to?); 2) opportunity (Do they have the chance to do the action?); and 3) motivation (Are they motivated to lock the screen?).

Figure 20: B=MAT model (adapted from Fogg, 2009)


High motivation
Low motivation
Motivators (pleasure / pain Hope/fear etc)
Triggers (spark, facilitator, signal)
Increasing likelihood of performing behaviour
Simplicity (time, effort, cost, non-routine etc)
Low Ability
High Ability

According to the B=MAT model, the type of persuasion required to bring about a behaviour depends on where it lies in the motivation/ability dimensions, with different interventions needed to increase either motivation or ability. Once motivation and ability are addressed, we should then look to triggers that signal to people that a behaviour is required.

Both models can be used to find the cause or causes for (non) behaviour. For instance, if employees are required to use electronic signatures for communication but they are not using them, the cause could be in the realm of capability (they are unable to use electronic signature, because it is technically too complicated), opportunity (they can use it, but do not have proper tools to do so), motivation (they know they should use it, but there is no reward if they do so or punishment if they do not), or triggers (they are not requested by the information system to attach the signature).

Figure 21: List of suggested measures

Area	Suggested measure
Awareness of functions of the CSIRT	Motivation – investigators do not see any benefits of cooperation; Simplicity – operators do not know how the CSIRT can help, or what their functions are; Triggers – there are no available contact to CSIRTs.
Lack of cooperation with CSIRTs	Motivation – investigators do not see any benefits of cooperation; Simplicity – there are no guidelines on how to cooperate with CSIRTS; Triggers – there is no trigger in internal guidelines.
Sharing of the information about the investigation	Motivation – Investigators do not know how useful the information might be to CSIRTs; Simplicity – there is no legal regulation that would allow them to share information from live case; Triggers – there are no requests from CSIRTs.

3.2.3.4 Identify appropriate measures to resolve problems

In this step you should identify measures/interventions that can partially or completely resolve identified problems. For this purpose, you can use identified causes as a guidance what kind of measures should be used.

For instance, if people are motivated to undertake a task, then addressing their ability should increase the likelihood of carrying out the behaviour. Similarly, if an action is simple and the person is able to complete it, then addressing motivation should also increase the likelihood. The problem could be also resolved adding triggers, which signal that a behaviour is required (like notifications in the information systems, warnings distributed within the organization, etc.)

Figure 22: List of suggested measures

Area	Suggested measure
Awareness of functions of the CSIRT	Training on responsibilities and functions of CSIRTs, etc.
Lack of cooperation with CSIRTs	Internal guidelines, list of contacts to CSIRTs, cooperative training of CSIRTs and LE, etc.
Sharing of the information about the investigation	Training with LE, common guidelines on information sharing, implementation of secure communication channels, new laws that would allow sharing, etc.

3.2.3.5 Segregation of Duties

In this step, use the SoD matrix (Figure 23) to identify, what activities can be performed or facilitated by your Law Enforcement Agency (LEA), and what you expect from the CSIRT and the judiciary. The SoD matrix should help you to reach a better understanding of each other's duties based on the roles each community has throughout the cybercrime investigation lifecycle.

3.2.3.6 Outcomes

After following all steps, each group should be able to identify the causes of unwanted (non) behaviour, to implement effective and proportional measures to address these causes and to measure the effectiveness of the solutions selected.

We would suggest this case study to be conducted in groups so that the different results and approaches of each group can be compared. Then, the advantages and disadvantages of the individual solutions should be presented and discussed.

Figure 23: 'Segregation of Duties' matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training	✓	✓	✓	✓	Problem-solving and critical thinking skills
Collecting cyber threat intelligence	✓	✓		✓	Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats	✓	✓		✓	Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats	✓				Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime	✓	✓			Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cybersecurity incident/crime	✓	✓			Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cybersecurity incident/crime	✓	✓		✓	Incident and crime classification and identification
Identify the type and severity of the compromise	✓	✓		✓	Knowledge of cyber threats and incident response procedures
Evidence collection	✓	✓		✓	Knowledge of what kind of data to collect; organisation skills
Providing technical expertise	✓				Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial	✓	✓		✓	Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)	✓			✓	Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime	✓	✓		✓	Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)	✓				Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling	✓				Communication skills; communication channels
Mitigation of an incident	✓				Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation		✓		✓	Knowledge of the legal framework; decision-making skills
Leading the criminal investigation			✓	✓	Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation			✓	✓	Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE		✓	✓	✓	Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution	✓	✓	✓	✓	Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery	✓				Technical skills
Protecting the constituency	✓				Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view	✓				Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence		✓	✓	✓	Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE			✓	✓	Testimonies in a criminal trial
Admitting and assessing the evidence			✓	✓	Evidence in a criminal trial
Judging who committed a crime			✓		Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost	✓	✓	✓	✓	Evaluation skills
Reviewing the response and update policies and procedures	✓				Knowledge how to draft an incident response and procedures

**Differences may be highlighted in this matrix depending on the legal framework of each Member State.*

This is just an indicative example.

4. REFERENCES

ENISA. (2018). *Review of Behavioural Sciences Research in the Field of Cybersecurity*. Retrieved from https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/

A ANNEX: ABBREVIATIONS

Abbreviation	Description
CSIRT	Computer Security Incident Response Team
IOC	Indicators Of Compromise
IP	Internet Protocol
LE	Law Enforcement
LEA	Law Enforcement Agency
SOC	Security Operation Centre
SoD	Segregation (or separation) of Duties

TP-03-20-173-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-336-0
DOI: 10.2824/822352