enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

BEHAVIOURAL ASPECTS OF COOPERATION BETWEEN CSIRTS AND LE

Toolset, Document for trainees

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: 978-92-9204-340-7, DOI: 10.2824/344314

TABLE OF CONTENTS

1. WHAT YOU WILL LEARN

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'.

- **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.

2. CASE STUDY

2.1 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 1: 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 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 'Segregation of Duties' (SoD) matrix

2.1.1 Objectives

- To learn how to apply the 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.

2.1.2 Scenario

2.1.2.1 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.

2.1.2.2 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.

2.1.2.3 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 his systems show symptoms that, according to the report, indicate an 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.

The 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.

2.1.3 Tasks

2.1.3.1 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 get better understanding of identified issues and drawbacks. You can suggest any suitable measure, like further analysis, survey, group discussions, statistical analysis, etc.

Figure 2: List of suggested measures

Area	Suggested measure

2.1.3.2 Choose appropriate metric

Next step would be to choose a suitable metric to evaluate the severity of the problems identified and measure the effect of measures to resolve these problems. Metric 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.

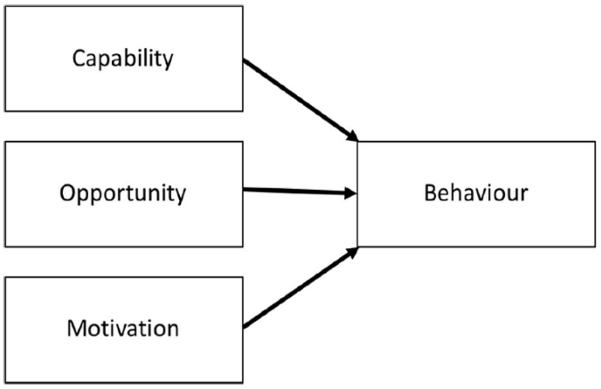
Figure 3: List of suggested metric

Area	Suggested metric

2.1.3.3 Identify causes of unwanted (non)behaviour

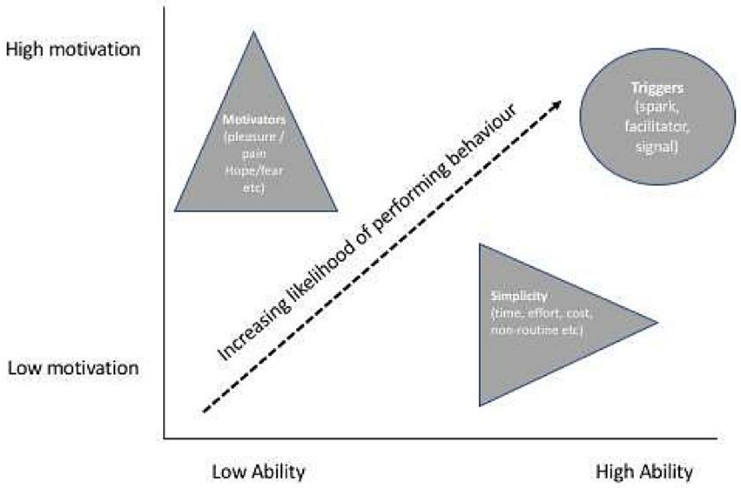
In this step you should use COM-B and/or B=MAT models to identify causes of unwanted (non)behaviour.

Figure 4: 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 5: B=MAT model (adapted from Fogg, 2009)



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 6: List of suggested measures

Area	Suggested measure

2.1.3.4 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 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 that signal that a behaviour is required (like notifications in the information systems, warnings distributed within the organization, etc.)

Figure 7: List of suggested measures

Area	Suggested measure

2.1.3.5 Segregation of Duties

In this step, use the SoD matrix (Figure 8) to identify, what activities can be performed or facilitated by your Law Enforcement Agency (LEA), and what do 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.

2.1.3.6 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 8: ‘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

3. 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

TP-03-20-176-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: 978-92-9204-340-7
DOI: 10.2824/344314