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

COPYRIGHT NOTICE

ISBN: 978-92-9204-337-7, DOI: 10.2824/73305

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 carry 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 STUDIES

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

2.1.1 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.

2.1.2 Scenario

2.1.2.1 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.

2.1.2.2 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.

2.1.2.3 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 metadata on 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 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..

The 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.

2.1.3 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.

2.1.3.1 Identify expected behaviour of CSIRT members

Describe the correct procedure of the CSIRT to ensure effective cooperation with LE and identify areas where you see the main drawbacks of the procedure applied in the described scenario. As a guideline, you can use the segregation of duties matrix provided below in 2.1.3.2.

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 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.

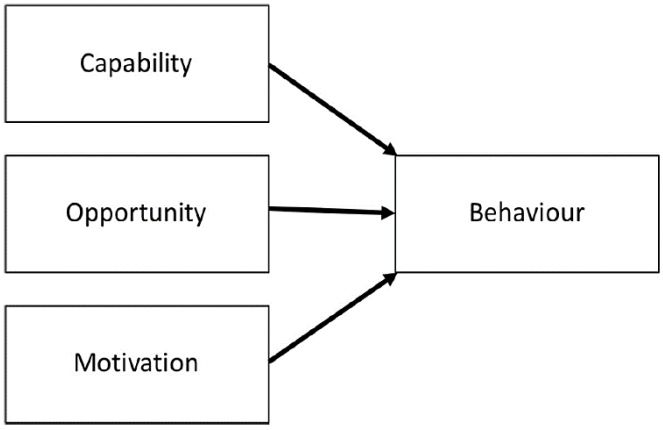
Figure 3: List of suggested metrics

Area	Suggested metric

2.1.3.3 Identify causes of unwanted (non)behaviour

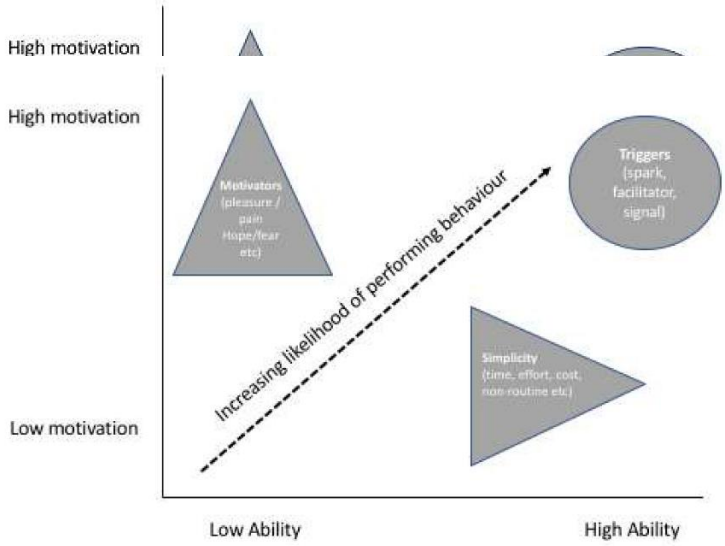
In this step you should use COM-B and/or B=MAT models to identify causes of unwanted (non) behaviour.

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 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 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 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 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, please use the SoD matrix (Figure 8) to identify, what activities can be performed or facilitated by your CSIRT, and what do 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.

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

TP-03-20-174-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: 978-92-9204-337-7
DOI: 10.2824/73305