



27th ANNUAL
FIRST BERLIN
CONFERENCE

14 - 19 JUNE 2015

**UNIFIED SECURITY:
IMPROVING THE FUTURE**



Building CERT Team in the Large Energy Company

MIROŚLAW MAJ

Cybersecurity Foundation

ComCERT.PL

Building CERT Team in the Large Energa Company

MIROŚLAW MAJ

Cybersecurity Foundation

ComCERT.PL



Agenda

#Background

#Methodology

#Challenges

#BestPractices



#Background

#Methodology

#Challenges

#BestPractices



Background

- Energy Sector in Poland
- The object is one of the companies
- Initial interest in having IRT
- CERT Energa

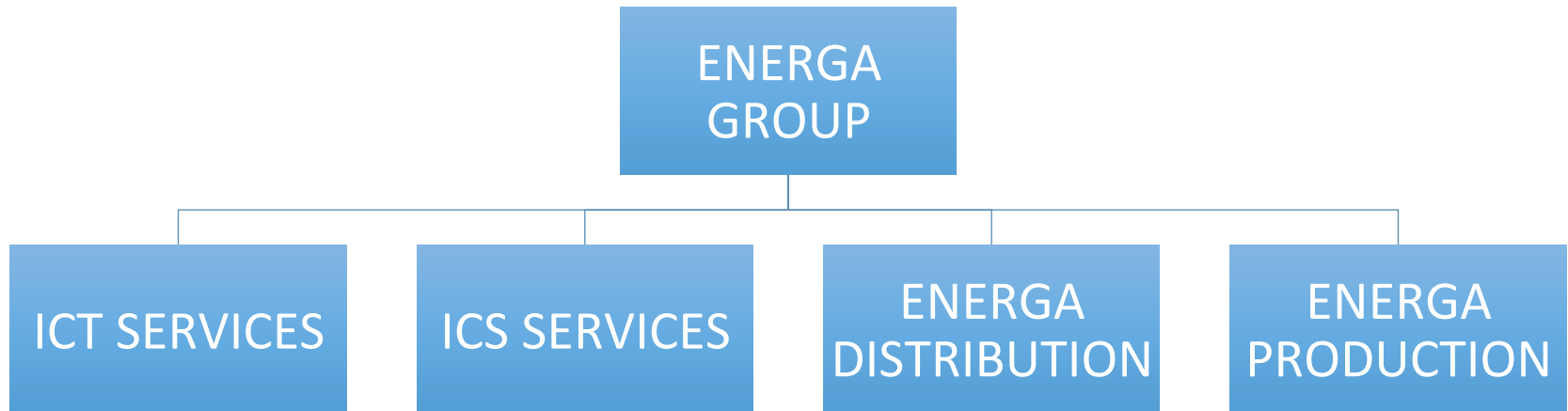


Background

- National Critical Infrastructure Protection Programme
- Recommendation 2.8.2.10
 - To establish CERT



Background



Background

- Incidents
- Only ICT domain
 - Malware
 - Phishing both sides
 - Targeted attacks
 - „Twitter” stock exchange attacks
- Not recognized OT domain

www.energa-operator.pl Infolinia: 801-404-404

Energa

Faktura VAT: 316257034/00001/0162/D/2015
Rozliczenie świadczenia usługi dystrybucji

numer klienta 316257034

D+2 PRIORYTET

Plac IC 50498837 Nr klienta: 316257034
Nadano w UP Brodnica 1, dnia: 13.02.2015

numer klienta F **numer klienta**

SPRZEDAWCA
ENERGA - OPERATOR SA
ul. Marynarki Polskiej 130
80-557 Gdańsk
NIP: 583-000-11-90

NABYWCA
JAN KOWALSKI
ul. Rodzina 57
82-465 MIASTO
NR KLIENKA: 316257034

JAN KOWALSKI
ul. Rodzina 57
82-465 MIASTO

Rozliczenie za okres 04.12.2014 - 04.02.2015	
Zużycie energii elektrycznej:	123 kWh
wartość usługi	51,99 zł
odsetki za nieterminową wpłatę	0,00 zł
nadpłata	0,00 zł

Wartość do zapłaty
51,99 zł
Słownie: pięćdziesiąt jeden złotych 99/100
Termin płatności: 02.03.2015

szeregowe rozliczenie

NR INDYWIDUALNEGO KONTA BANKOWEGO: 52 1240 2092 9909 9116 2570 3417

6 cyfr z nr klienta 316257034

Formy płatności

Zeskanuj kod i zapłać online 	Możesz zapłacić w wybranych sklepach lub na poczcie 	Dane do przelewu Nr faktury VAT: 316257034/00001/0162/D/2015 Termin płatności: 02.03.2015 Kwota płatności: 51,99 zł Słownie: pięćdziesiąt jeden złotych 99/100 Nr rachunku odbiorcy: 52 1240 2092 9909 9116 2570 3417 ENERGA - OPERATOR SA ul. Marynarki Polskiej 130, 80-557 Gdańsk NIP 583-000-11-90 Zobowiązanie:
Płatność przez kod QR Możesz szybko i wygodnie zapłacić fakturę za prąd - przy użyciu smartfona z aparatem fotograficznym oraz specjalną aplikacją. Zaloguj się do swojego banku poprzez aplikację mobilną i zeskanuj QR kod z faktury. Pajawę się gotowy formularz przelewu z uzupełnionymi danymi. Sprawdź dane z fakturą i wykonaj przelew.	Płatność w sklepie lub na poczcie Zabierz ze sobą fakturę i zapłać za prąd na poczcie lub podczas codziennych zakupów - w wybranych sklepach, stacjach benzynowych i punktach usługowych - wszędzie tam, gdzie znajdziesz logo Moje Rachunki.	Wpłata przelewem Wykorzystując dane zamieszczone na fakturze możesz samodzielnie zapłacić przelewem online w swoim banku internetowym. Możesz także zlecić wykonanie przelewu w sposób tradycyjny - na poczcie lub w banku.

0001 0000 50408837 1

1/2



#Background

#Methodology

#Challenges

#BestPractices



#Background

#Methodology

#Challenges

#BestPractices



Methodology

CERT SERVICES

REACTIVE SERVICES

- ALERTS AND WARNINGS
- INCIDENT HANDLING
- VULNERABILITY HANDLING
- ARTIFACT HANDLING

PROACTIVE SERVICES

- ANNOUNCEMENTS
- TECHNOLOGY WATCH
- SECURITY AUDITS OR ASSESSMENTS
- CONFIGURATION AND MAINTENANCE OF SECURITY TOOLS, APPLICATIONS AND INFRASTRUCTURE
- DEVELOPMENT OF SECURITY TOOLS
- INTRUSION DETECTION SERVICES
- SECURITY-RELATED INFORMATION DISSEMINATION

SECURITY QUALITY MANAGEMENT SERVICES

- RISK ANALYSIS
- BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING
- SECURITY CONSULTING
- AWARENESS BUILDING
- EDUCATION TRAINING
- PRODUCT EVALUATION OR CERTIFICATION



Methodology

8 steps by CERT/CC

STEP 1

**Obtain Management
Support and Buy-In**

STEP 2

STEP 3

STEP 4

STEP 5

STEP 6

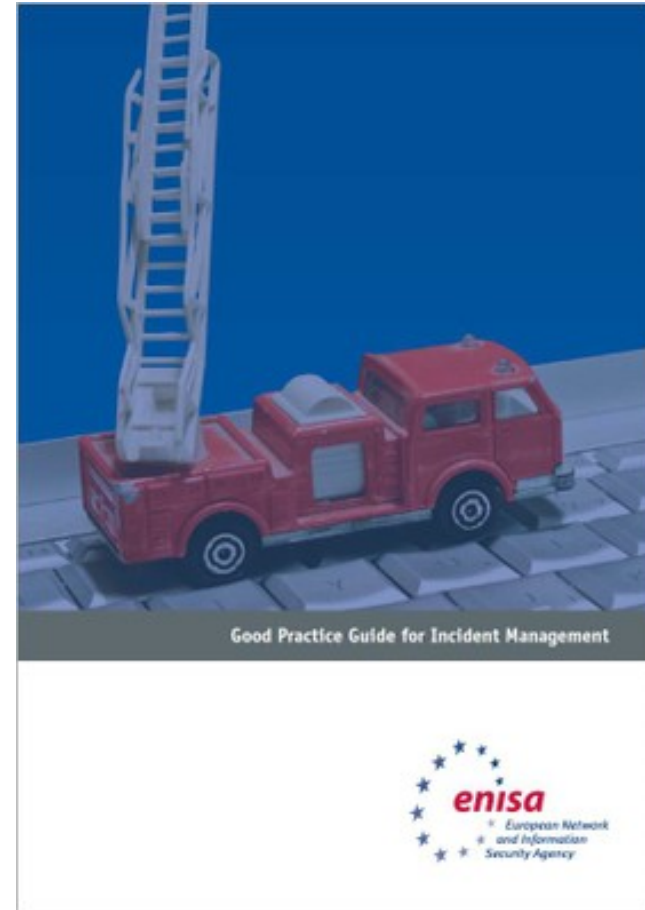
STEP 7

STEP 8



Methodology

- ENISA Good Practice Guide for Incident Management

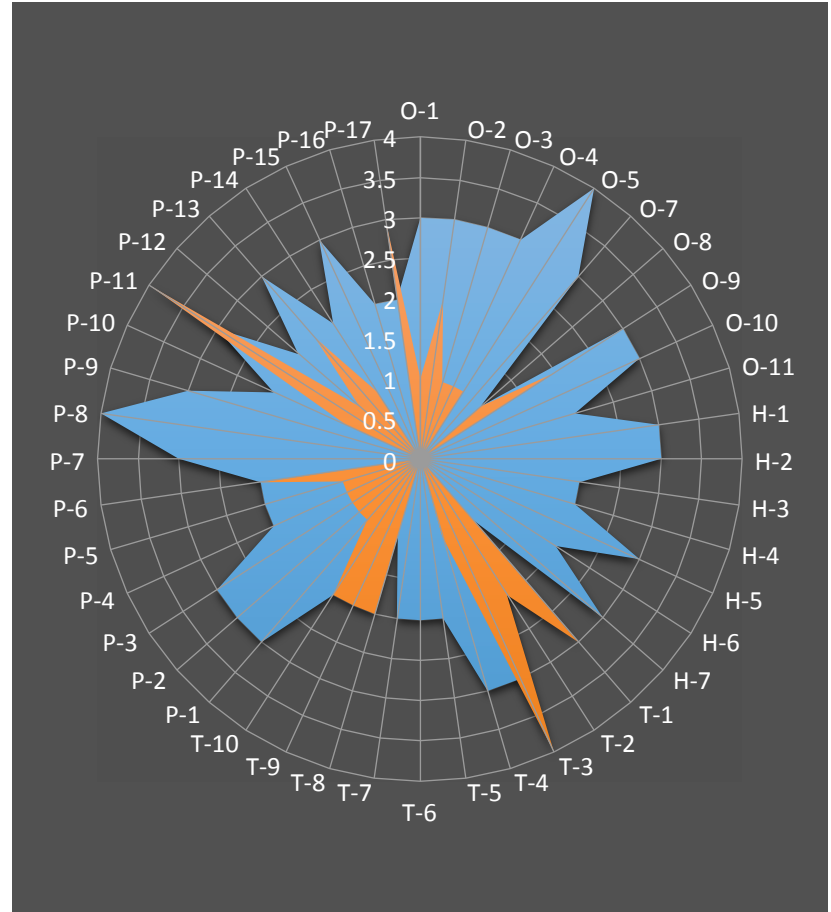


Methodology



Methodology

- **SIM3 - Security Incident Management Maturity Model**



#Background

#Methodology

#Challenges

#BestPractices



#Background

#Methodology

#Challenges

#BestPractices



Challenge #1

Formal regulatory mess

- Personal data protection
- Classified information
 - State level
 - Company level
- National Cybersecurity Policy
- National Strategic Plan For Protecting Critical Infrastructure



Challenge #2

Documentation

- Different documentation in all companies
- A lot of documents
- Inconsistency
- No clear rules about incident reporting schema
- In fact – many changes needed



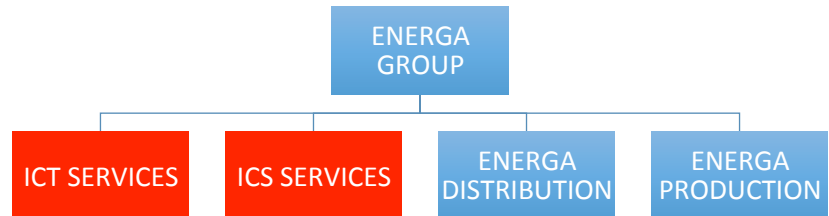
Picture: <http://rcmguy.com/>



Challenge #3

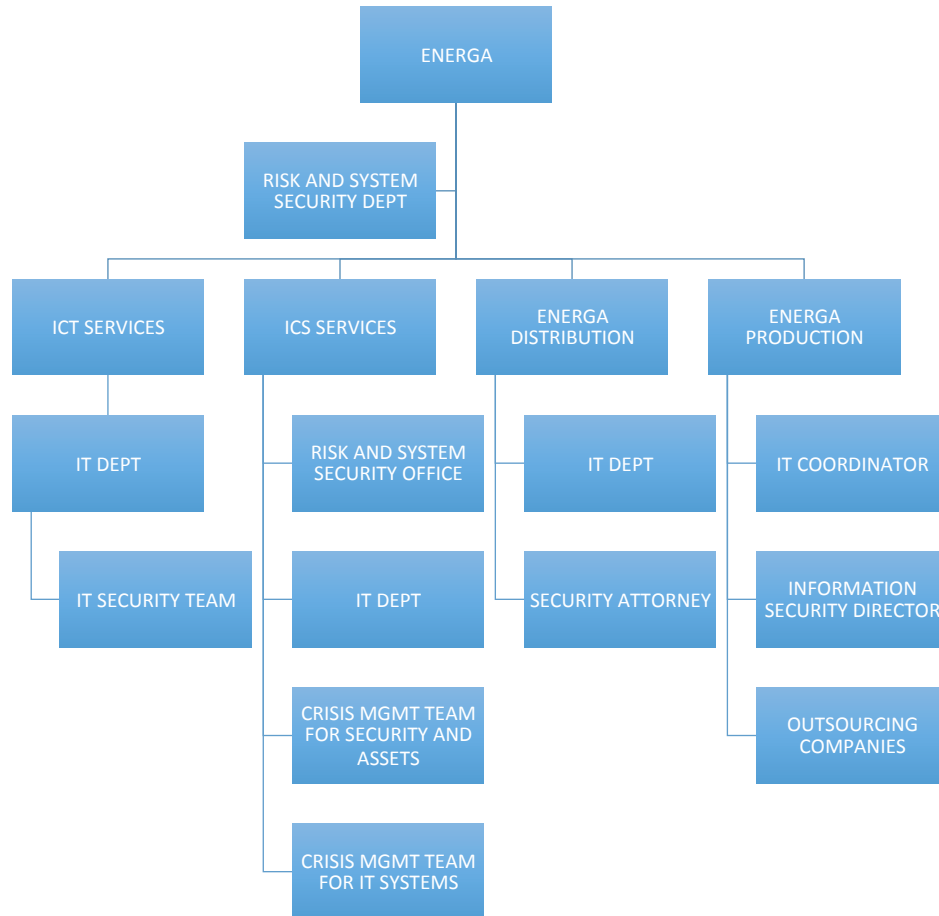
Heterogeneous ICT environment

- ICT
- OT
 - Various ICS systems
 - Outsourcing
 - Remote access
- 2 SIEMs
- 2 SOCs (?) / NOCs
- 2 Teams



Challenge #4

Distributed security roles



Challenge #5

Internal politics

- The first question was:
 - Where in the organizational structure the CERT will be situated?



#Background

#Methodology

#Challenges

#BestPractices



#Background

#Methodology

#Challenges

#BestPractices



Best Practice #1

Use their knowladge about crisis management

- They work in crisis management situations almost all the time
- Recognize the existing processes and try to find specific things for cybersecurity



Best Practice #2

Ensure ICT and OT technical competences

- Do not build only coordination center without technical knowledge
- You do not need your technical knowledge operationally but you must understand to incident and have common language and esteem for technical partners
- Ensure access to technical tools – e.g. SIEM
- Do not propose IPS in OT environment
- Make simple port scanning



Picture: <http://tenabla.com/>



Best Practice #3

CSIRT SERVICES are your foundations

- You learn the organization
- They learn a CERT concept
- Make a survey

What services do you serve?

What services you would like to serve?

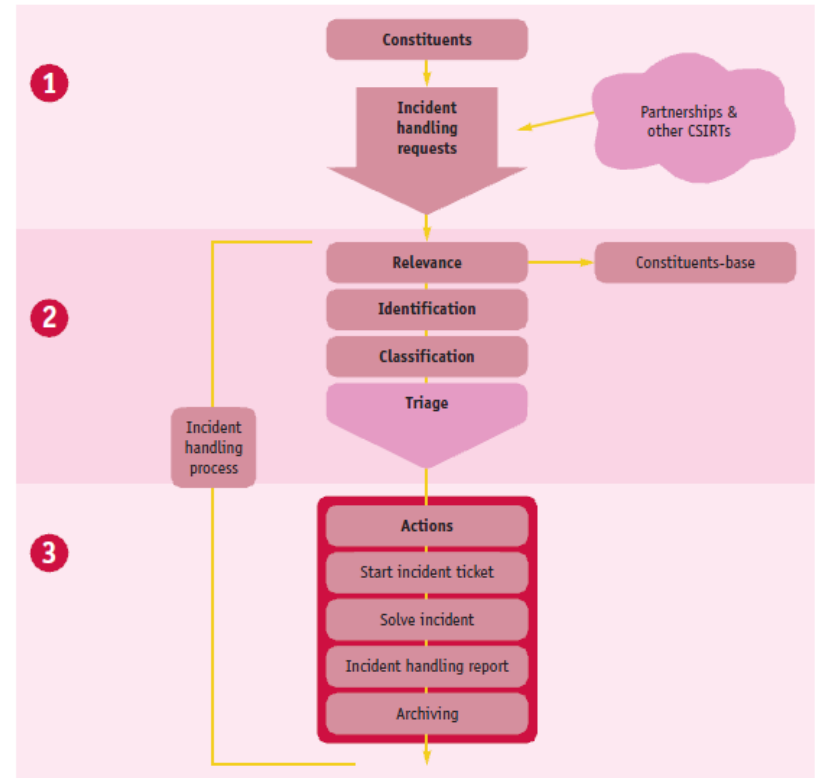
What services your constituency need?



Best Practice #4

Work with workflows

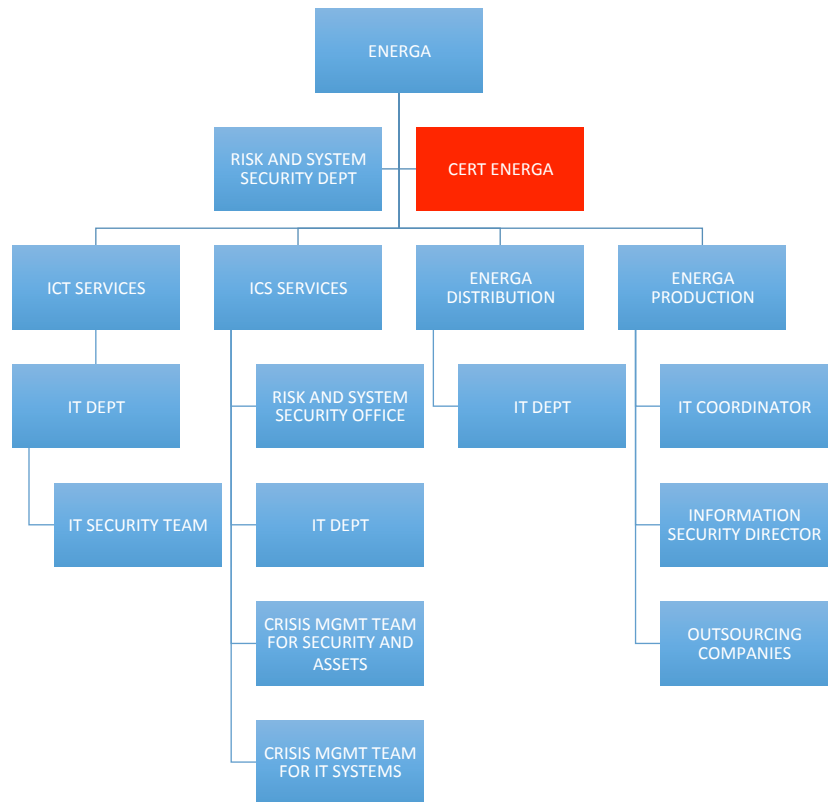
- In sophisticated organizational structure this is the best to identify parties and tasks
- Take main types of incidents and work with them
- Use graphics rather than text



Best Practice #5

Recognize a structure of regulations

- Use an umbrella document to introduce CERT in the organization
- Focus on regulations relate to incident response but not the whole security
 - Find existing regulations
 - Add regulations
- Try to put CERT as high as possible
 - Separation of IT and CERT -> **MUST**
 - Separation of IT security and CERT -> recommended



Best Practice #6

Use this time to introduce metrics

- Number of incidents
- Classification
- Reaction times
- etc

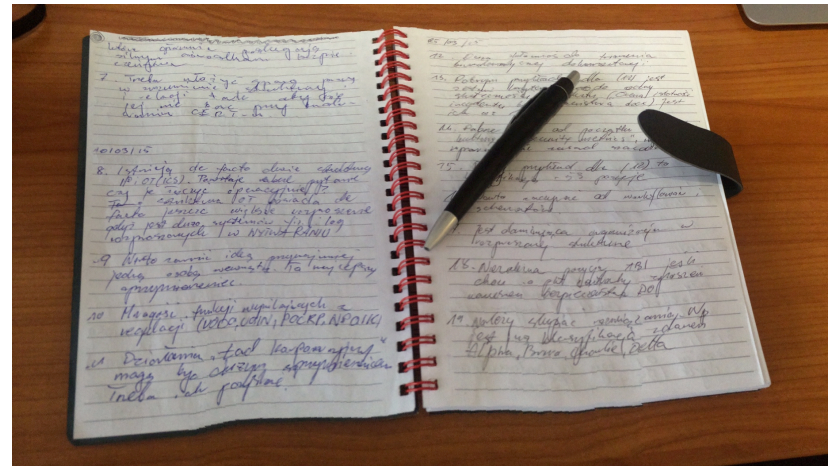
Incident Class <i>(mandatory input field)</i>	Incident Type <i>(optional but desired input field)</i>	Description / Examples
Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by unauthorized local access.
	Unprivileged account compromise	
	Application compromise	
Availability	DoS	In this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYN- a. PING- flooding or e-mail bombing (DDoS: TFN, Trinity, etc.). However, availability can also be affected by local actions (destruction, disruption of power supply, etc).
	DDoS	
	Sabotage	
Information Security	Unauthorised access to information	Besides local abuse of data and systems, the security of information can be endangered by successful compromise of an account or application. In addition, attacks that intercept and access information during transmission (wiretapping, spoofing or hijacking) are possible.
	Unauthorised modification of information	Besides local abuse of data and systems, the security of information can be endangered by successful compromise of an account or application. In addition, attacks that intercept and access information during transmission (wiretapping, spoofing or hijacking) are possible.
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (eg, the use of e-mail to participate in illegal profit chain letters or pyramid schemes)
	Copyright	Selling or installing copies of unlicensed commercial software or other copyright protected materials (Warez)
	Masquerade	Types of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.



Best Practice #7

Keep asking and implement answers

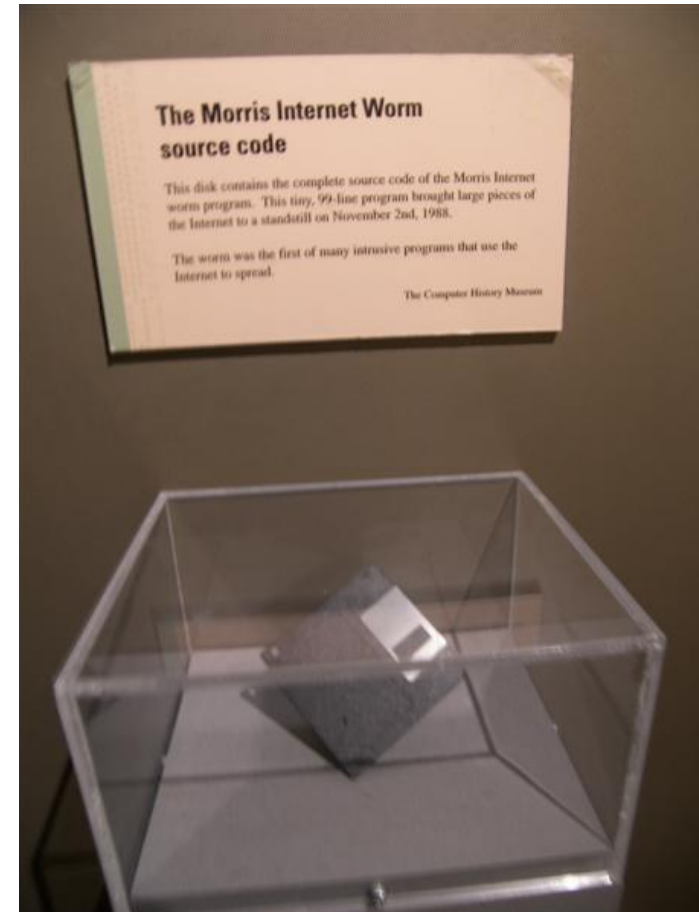
- Prepare the final document backbone at the very beginning and feed it with your findings all the time
- Give an open access to your partners at organization side
- Document all Q&A as the special chapter
- Start your project diary



Best Practice #8

Have friends of your idea

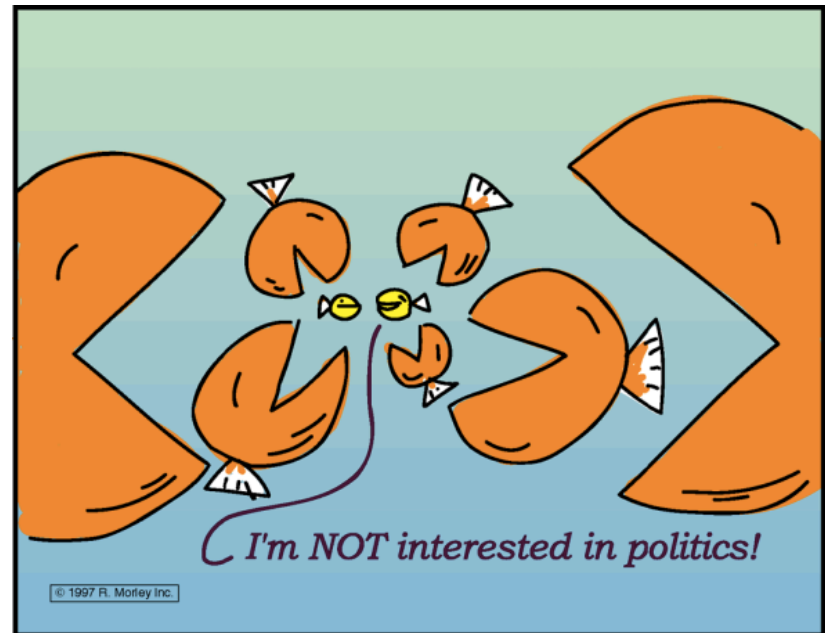
- Tell nice stories about CERT
- Inspire by the picture of future CERT in the organization



Best Practice #9

Avoid politics

- Just listen them
- Do not change your pragmatic plan
- Do not write the most important document yourself
 - They will do it better
 - They know the organization wording
 - They will learn more about what they are building



Best Practice #10

Build the external contacts

- Build the external contacts from the very beginning
 - Sectorial
 - Country level
 - International level
- Explain how these communities work
- Start to share information – having live cases during the process only can help you



Best Practice #11

Understand the organization

Beer Trusted Party 😊



Thank you!

Questions?

mirosław.maj@cybsecurity.org

mirosław.maj@comcert.pl