27th ANNUAL FIRST CONFERENCE

BERLIN

14 - 19 JUNE 2015

UNIFIED SECURITY:
IMPROVING THE FUTURE

27th ANNUAL FIRST CONFERENCE BERLIN 14-19 JUNE 2015

I'm Sorry to Inform You…

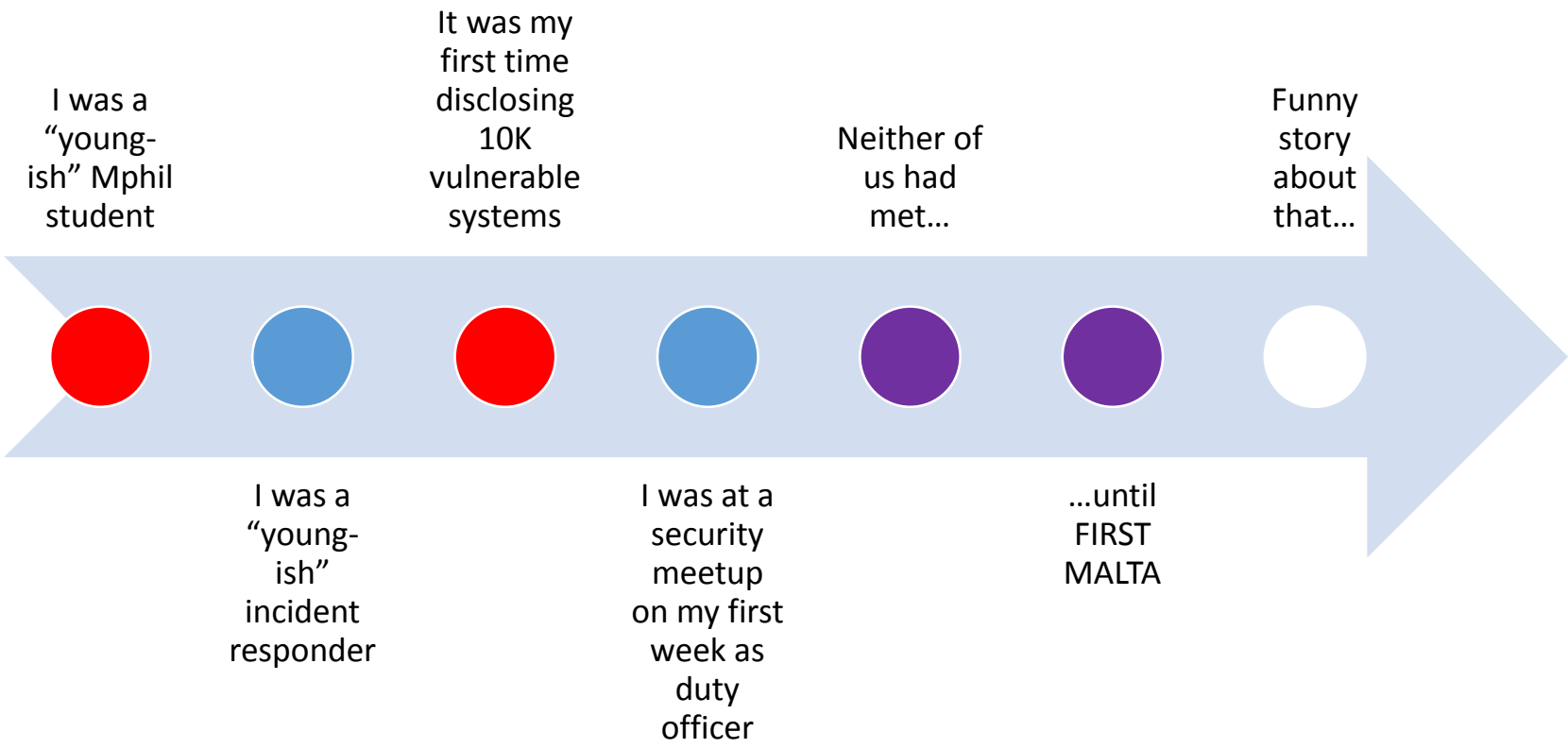
Dr. Marie Moe
@MarieGMoe

SINTEF

Éireann Leverett
@blackswanburst

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

How we met…

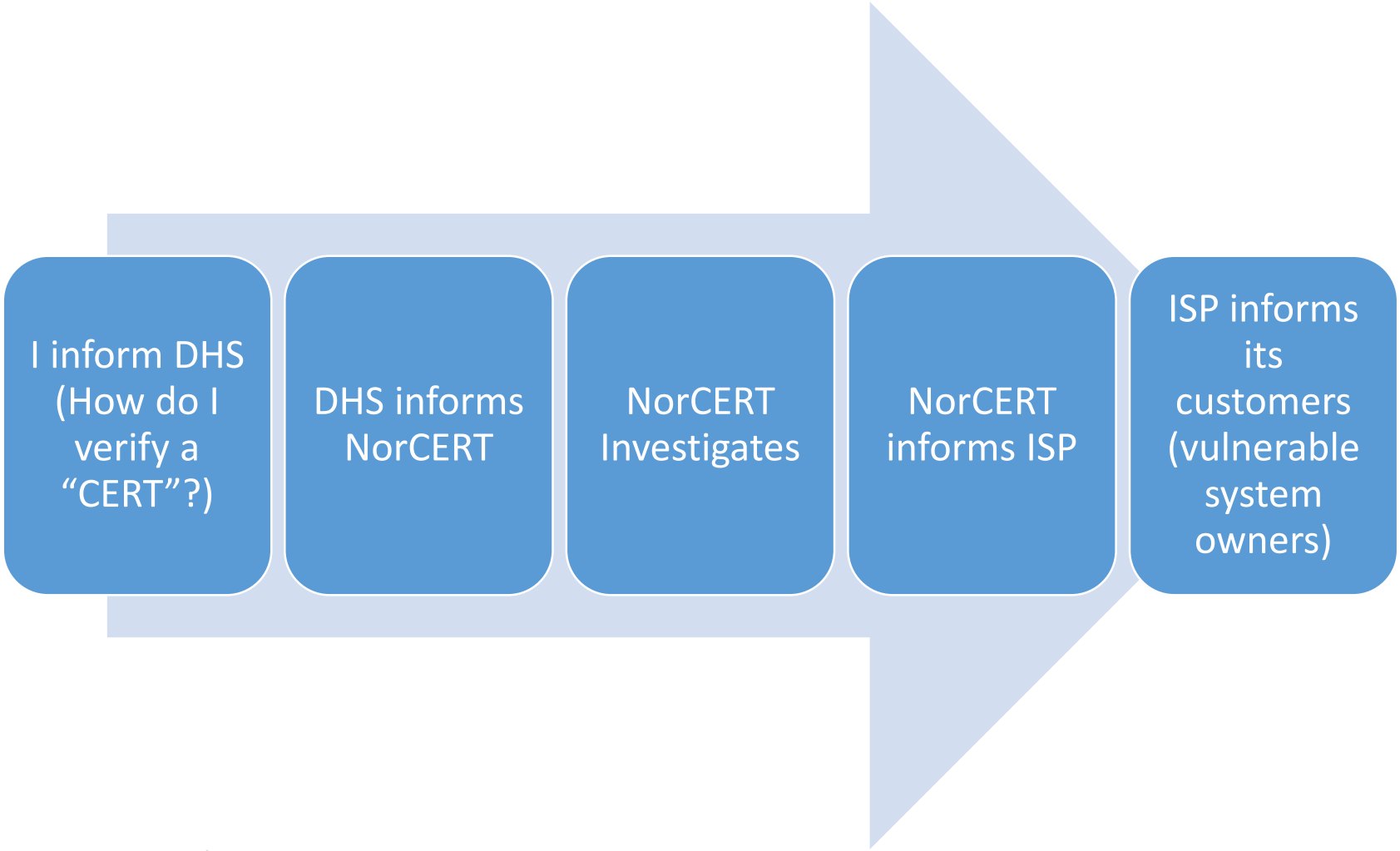

I was a "young-ish" Mphil student
I was a "young-ish" incident responder
It was my first time disclosing 10K vulnerable systems
I was at a security meetup on my first week as duty officer
Neither of us had met…
…until FIRST MALTA
Funny story about that…

Trust. Why do I trust him?

How did I come trust her?

- Face to Face contact
- Willingness to use strong cryptography in emails
- She provided feedback (where others didn't)
- Independent verification of facts
- Yearly communication
- Working futher incidents
- Core question:
  - How do I know this info doesn't flow straight to the offensive national team?

2010-2011


I inform DHS (How do I verify a “CERT”?)
DHS informs NorCERT
NorCERT Investigates
NorCERT informs ISP
ISP informs its customers (vulnerable system owners)

In retrospect

I should have included vulnerabilities

- I was uncomfortable sending both IPs and vulnerabilities to one country for distribution
- So I just sent IPs to ICS-CERT
- That mean Marie couldn’t have much traction
- Since she didn’t have evidence of vulnerability
- She had to redo that work

In the future I’d trust more

Informing by proxy.

I used ICS-CERT/DHS in 2011

- They shared with 52 certs

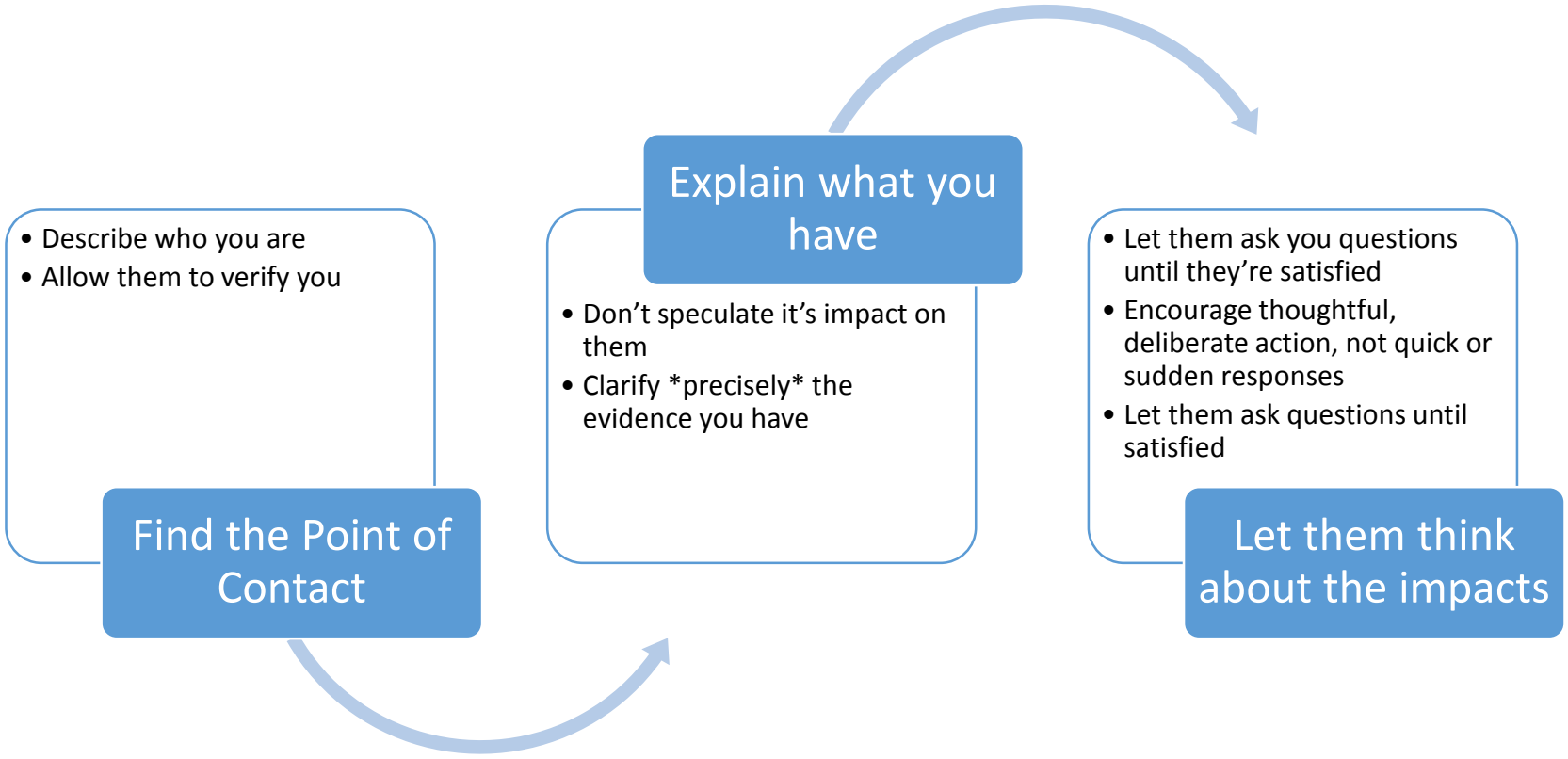
I worked with 12 certs in 2012

- Codesys Vulnerabilities (detailed later)

Basic Process

- Send them an email about what you have
- Attach GPG key and sign email
- Offer them data
- When they respond, send it to them encrypted

How do you approach companies?



Who in the organisation should you be speaking to?

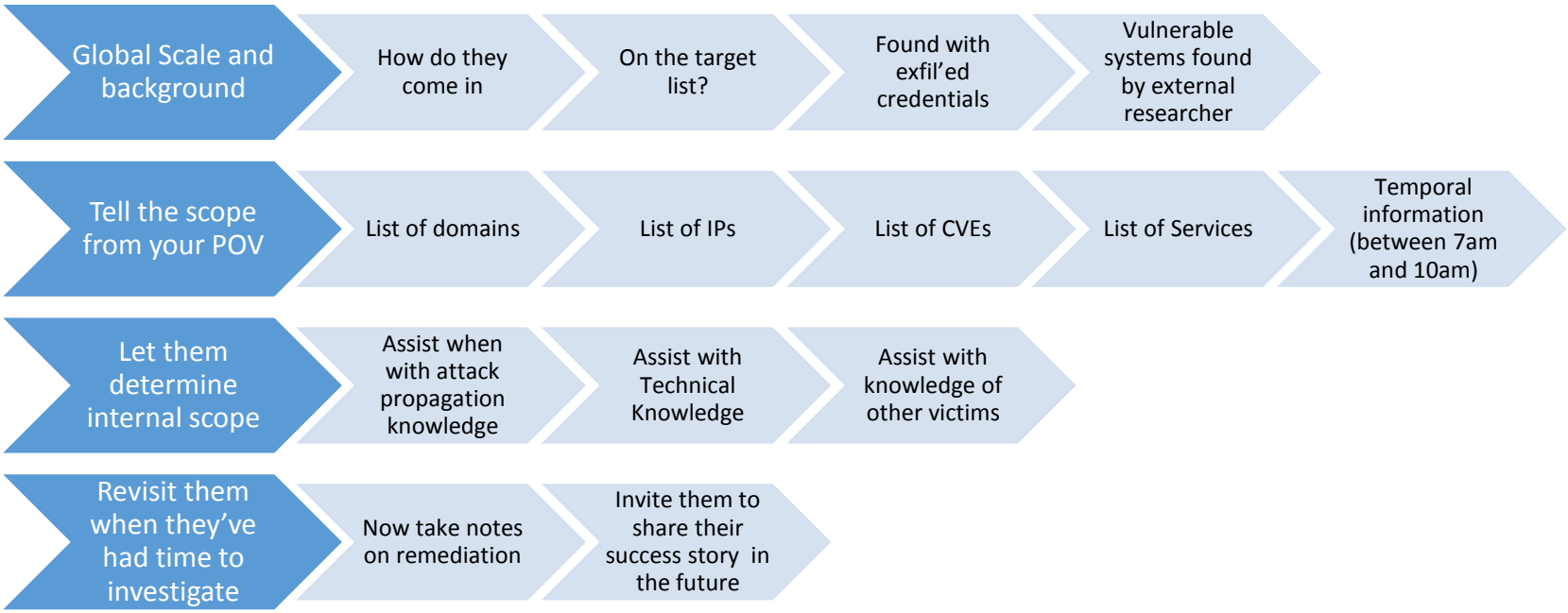
Ideal:

- Understands Technology
- Understands Security
- Has some level of responsibility for technology
- Previous Trust relationship established
- A CSO, CISO, or DFIR pro

Not Ideal:

- A support team
- A CRO
- An engineer
- A PR person
- A lawyer

How do you explain vulnerabilities and exposure?



One time during an incident: ‘assisted scope discovery’

Client thought only email had been compromised

I suggested it might be box that contained email

Client then thought single windows box was infected

Suggested looking at where profile had roamed

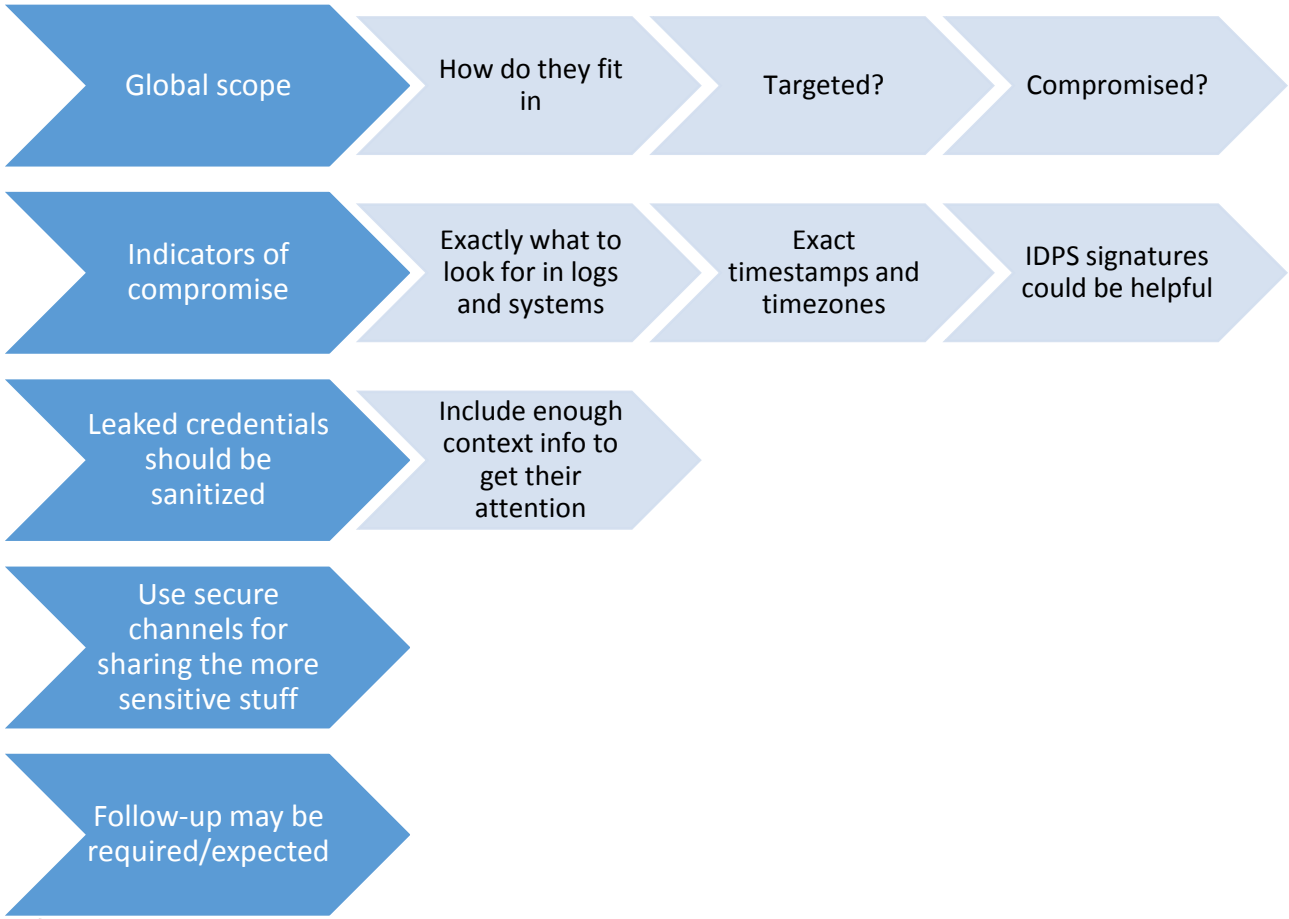
Turned out to be wrong, but useful

Forensics on a disk suggested exfiltration of data

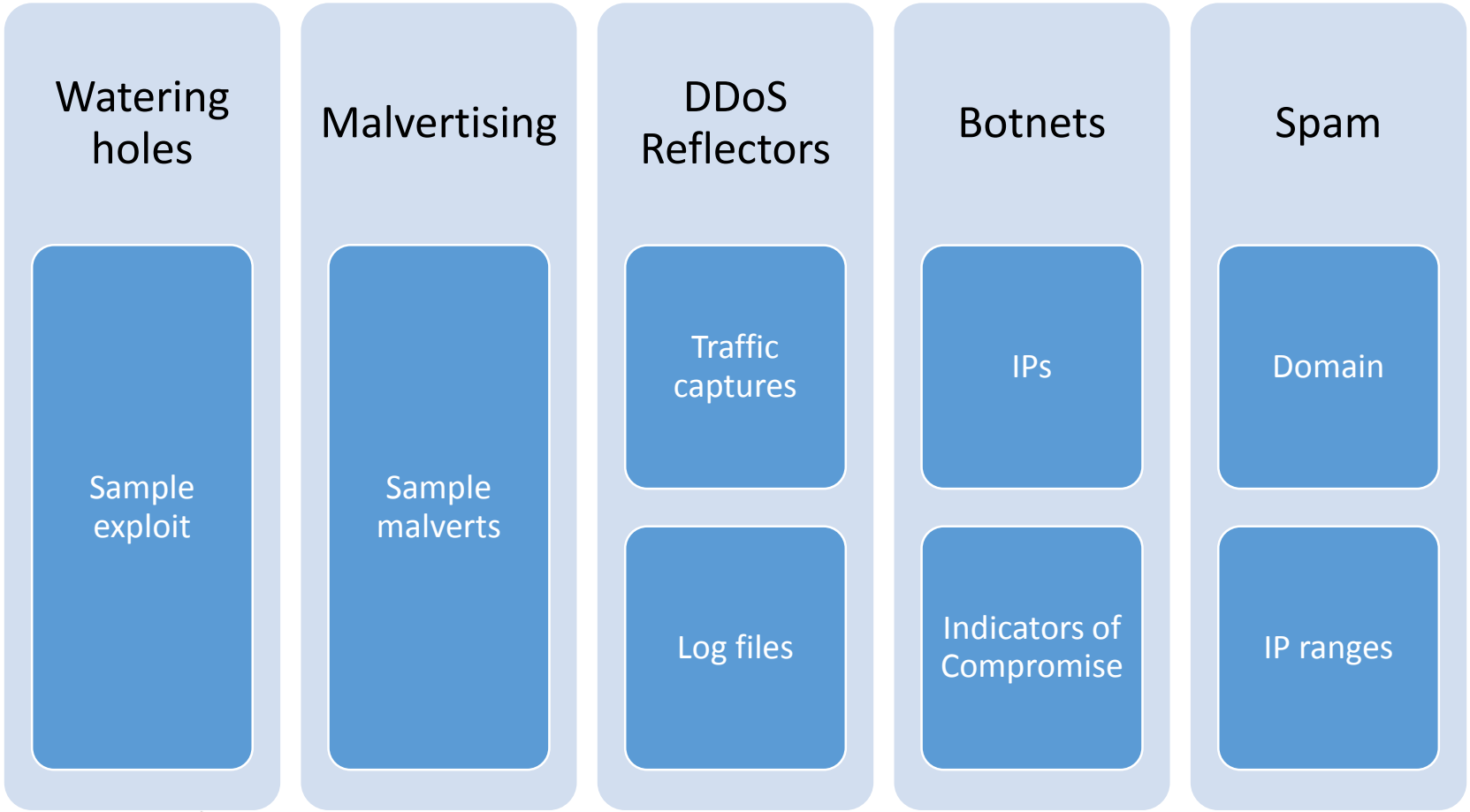
Knowledge of IODINE allowed me to suggest DNS traffic examination in openflow

Got a handle on volume of exfiltrated data

How do you tell them they're owned/infected?



How do you tell them they're causing someone else harm?



The CodeSys Story

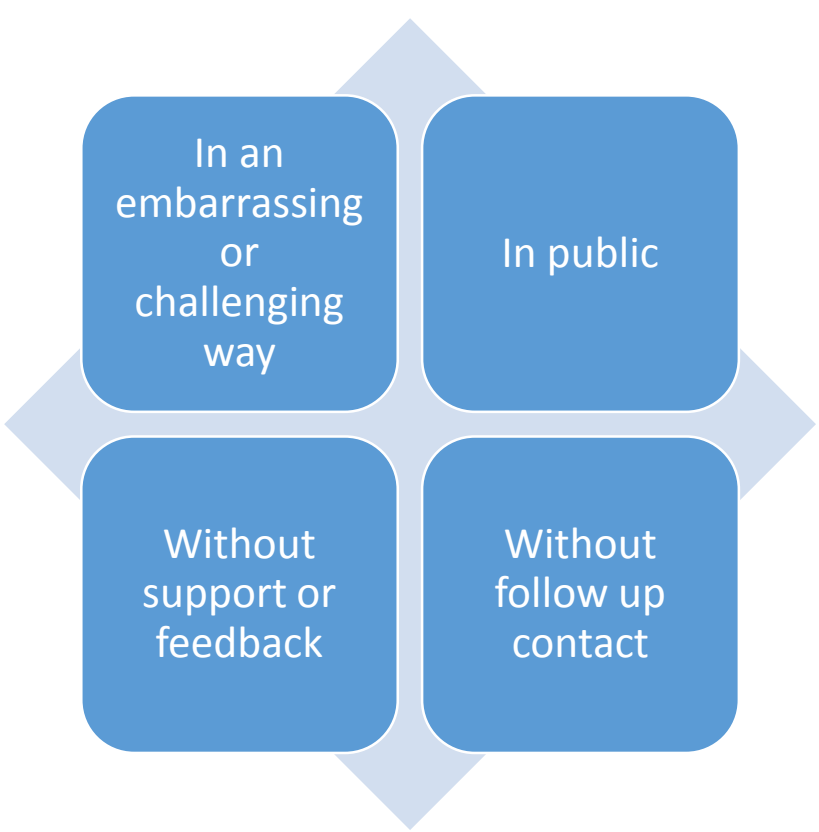
1. Ten Autonomous Systems containing the largest number of vulnerable I

PLCs Found	ASN	CC	Registrar	AS Name
9	6327	CA	arin	Shaw Communications Inc.
9	6830	AT	ripencc	Liberty Global Operations B.V.
12	5610	CZ	ripencc	Telefonica Czech Republic, a.s.
21	28929	IT	ripencc	ASDASD-AS ASDASD srl
25	12605	AT	ripencc	LIWEST Kabelmedien GmbH
28	3269	IT	ripencc	Telecom Italia S.p.a.
28	3303	CH	ripencc	Swisscom (Switzerland) Ltd
43	1136	EU	ripencc	KPN Internet Solutions[2]
43	286	EU	ripencc	KPN Internet Backbone
44	3320	DE	ripencc	Deutsche Telekom AG

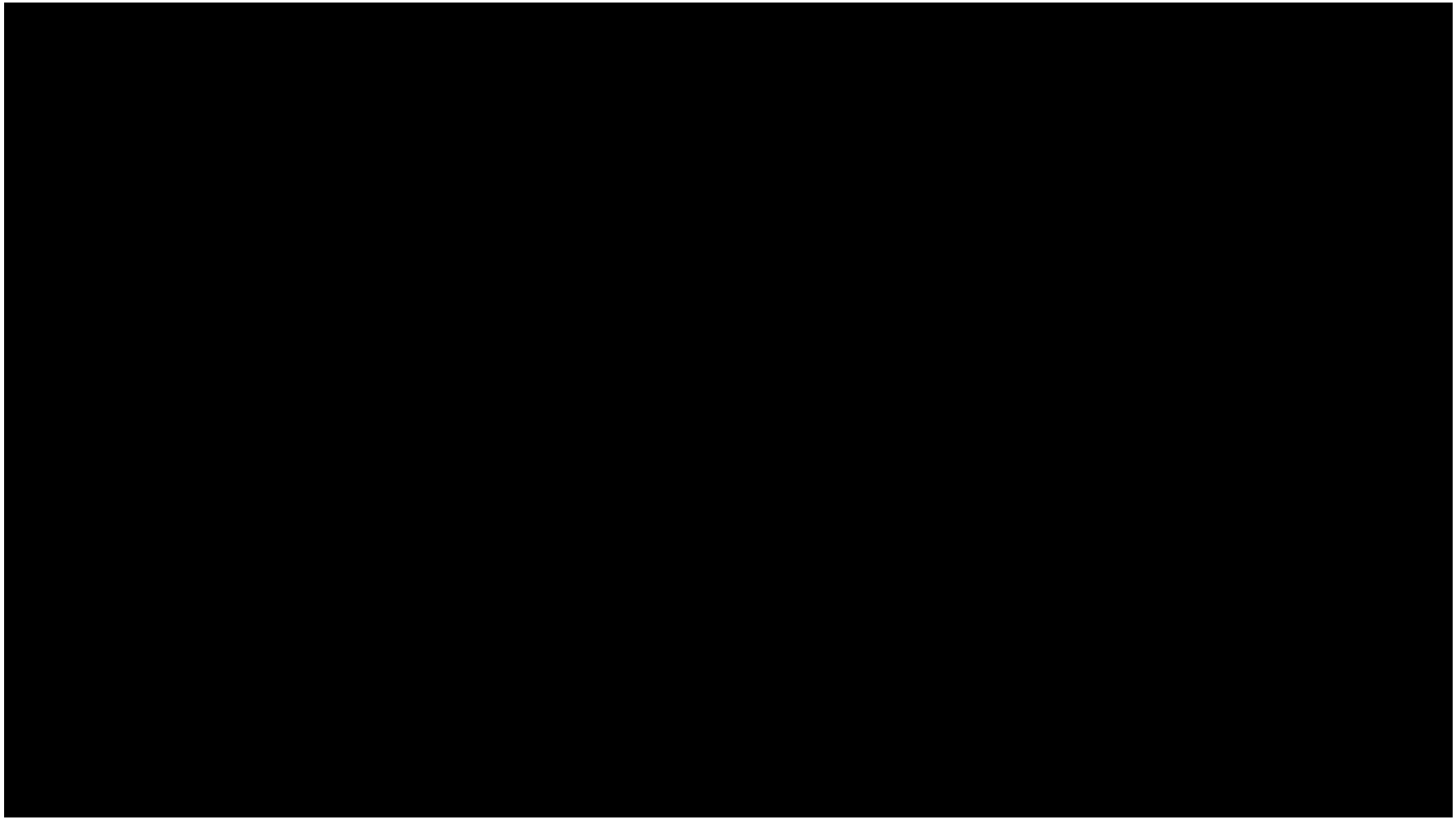
Table 2. Ten Countries containing the largest number of vulnerable PLCs

PLCs Found	Country Code
21	CA
21	ES
29	CZ
33	AT
33	US
38	CH
60	PL
64	NL
80	DE
81	IT

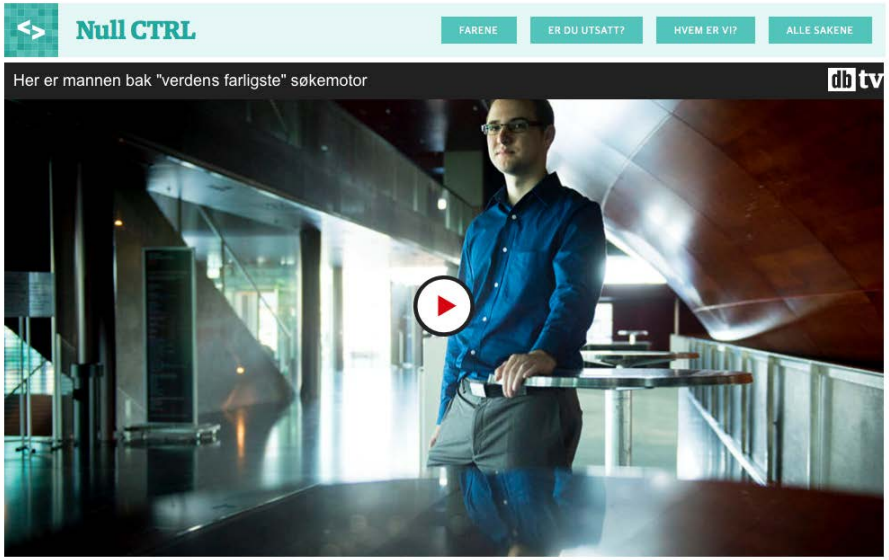
How not to do it.



The shock effect 1



The Null CTRL article series



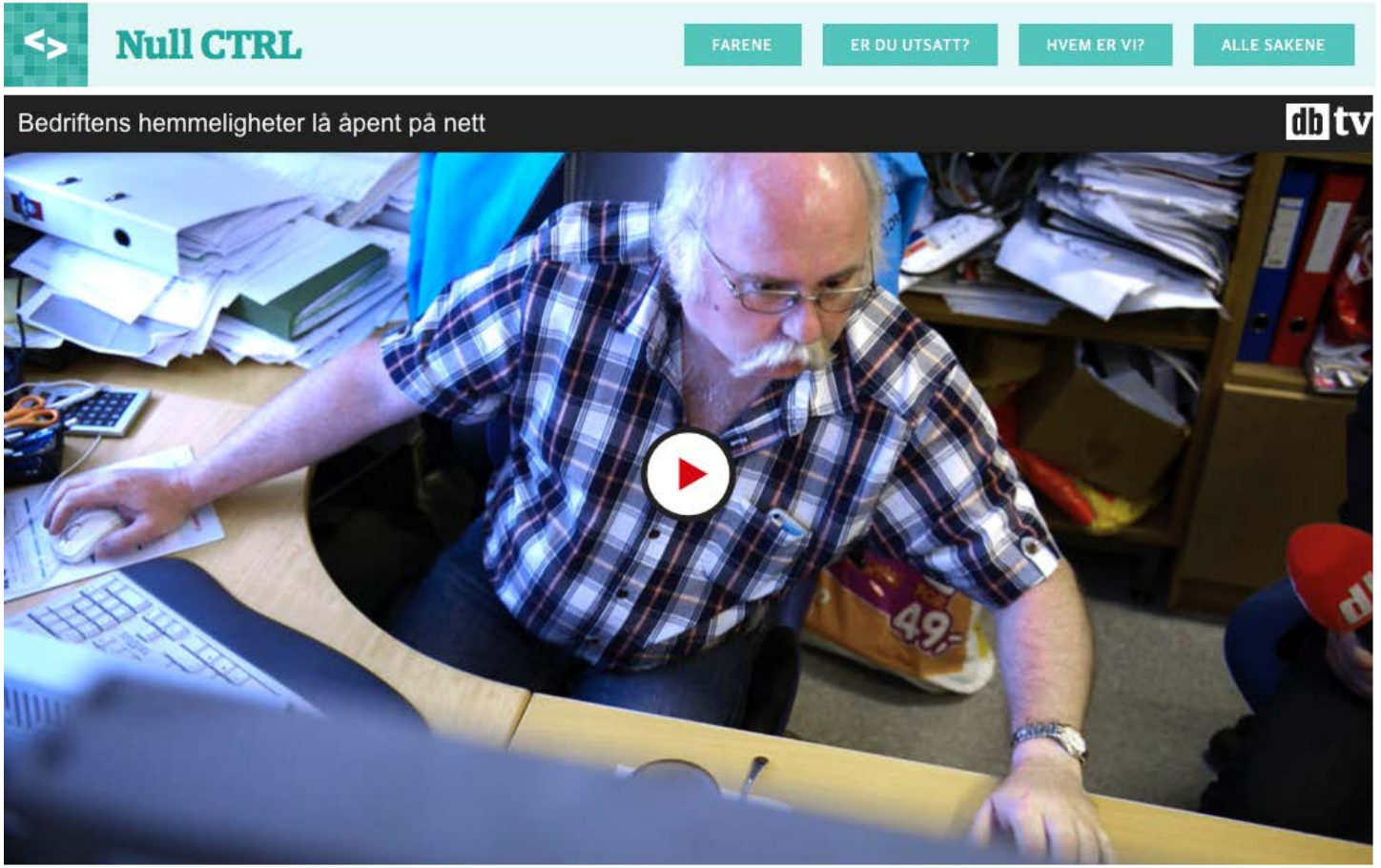
RAISING AWARENESS John Matherly created the search engine Shodan. He believes he is on the side of good, combating poor security and raising awareness. Video: Øistein Norum Monsen/Dagbladet

Journalists warned system owners and Norwegian NSA of 2500 critical data flaws

How two journalists set out on a mission to test the data security in the whole of Norway.

Source: http://www.dagbladet.no/2014/01/06/nyheter/nullctrl/shodan/english/english_versions/30861347/

The shock effect 2



Source: http://www.dagbladet.no/2013/10/14/nyheter/innenriks/nullctrl/datasikkerhet/29071043/

Havex/Dragonfly/Energetic Bear

August 28, 2014

Hundreds of Norwegian energy companies hit by cyber-attacks

Share this article:

Approximately 300 oil and energy companies in Norway have been hit by one of the biggest cyber-attacks ever to have happened in the country, a government official is reported to have claimed.

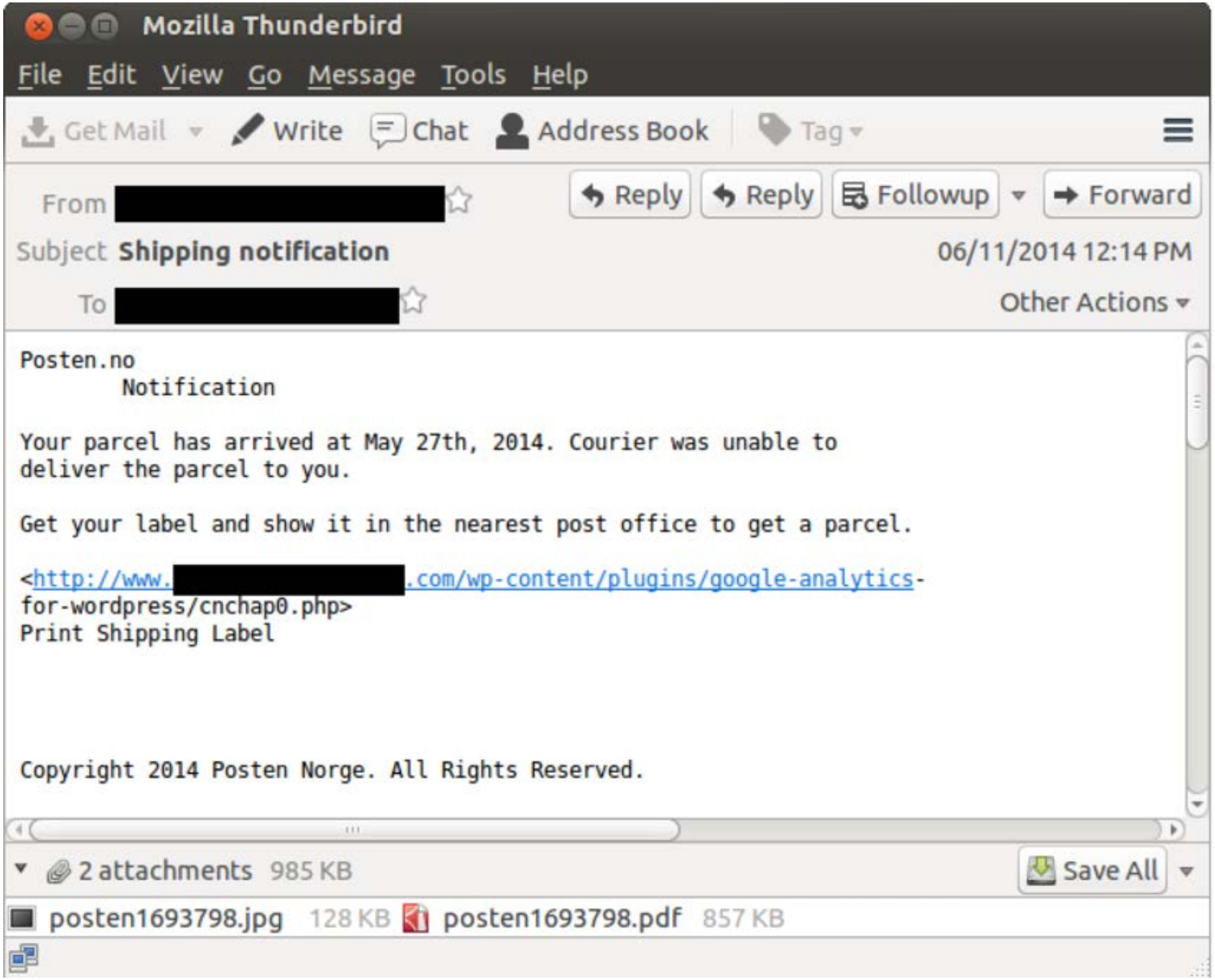
As first reported by The Local and Dagens *Næringsliv*, the National Security Authority Norway (Nasjonal Sikkerhetsmyndighet – NSM) detailed how 50 companies in the oil sector were hacked and how another 250 have been warned that they may have been hit too.

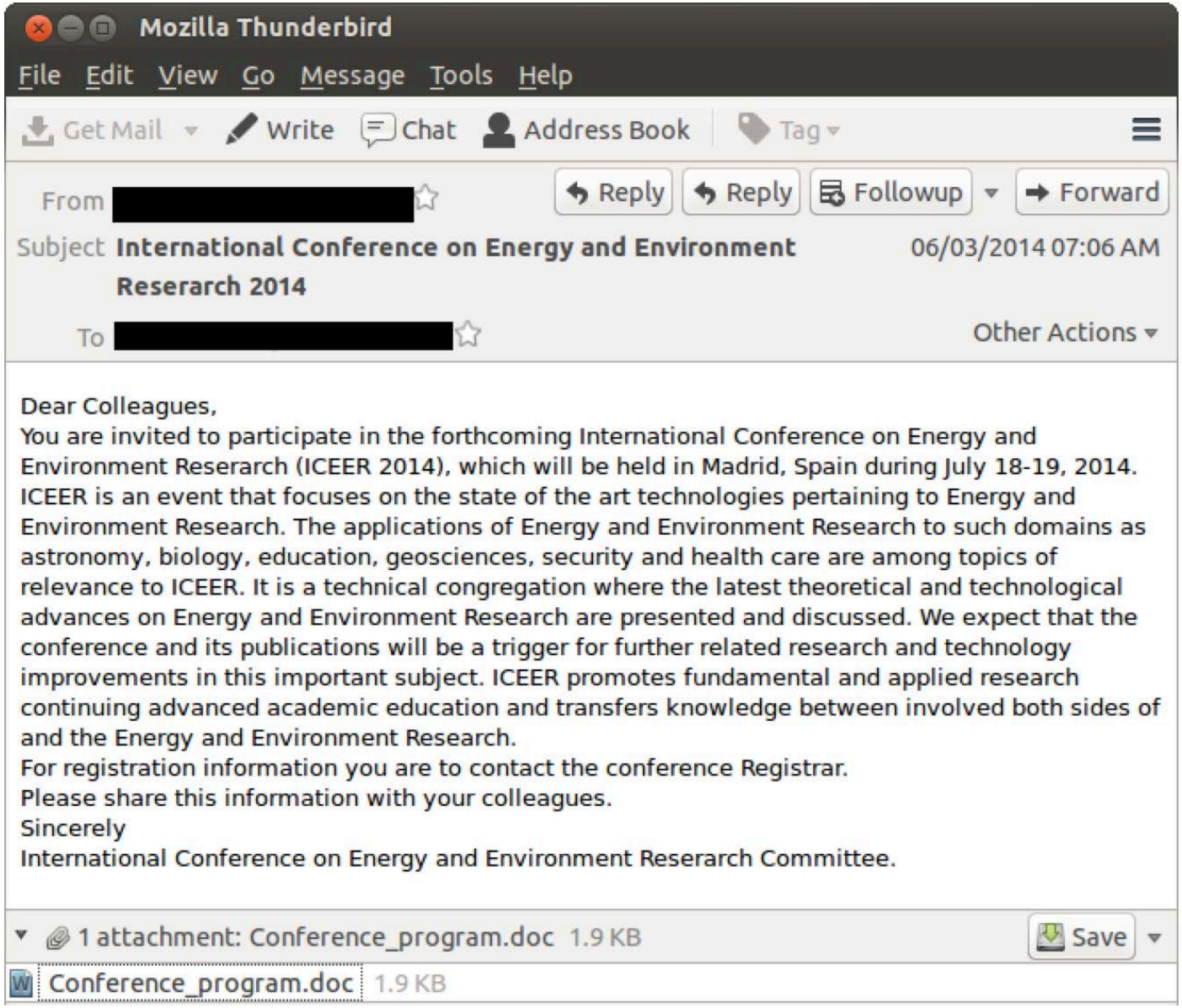
NSM is Norway's prevention unit for serious cyber-attacks and, like CERT-UK in Great Britain, warns companies about the newest threats. It took part of the CyberEurope2014 exercise in June.

The companies themselves haven't been named – although NSM is investigating whether the computer systems at Statoil, Norway's largest oil company, were targeted. Technical details are also few and far between at this moment in time.

Hundreds of Norwegian energy companies hit by cyber-attacks

Source: http://www.scmagazineuk.com/hundreds-of-norwegian-energy-companies-hit-by-cyber-attacks/article/368539/


Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Chat
Address Book
Tag
From [redacted]
Reply
Reply
Followup
Forward
Subject Shipping notification
06/11/2014 12:14 PM
To [redacted]
Other Actions
Posten.no
Notification
Your parcel has arrived at May 27th, 2014. Courier was unable to deliver the parcel to you.
Get your label and show it in the nearest post office to get a parcel.
<http://www.[redacted].com/wp-content/plugins/google-analytics-for-wordpress/cnchap0.php>
Print Shipping Label
Copyright 2014 Posten Norge. All Rights Reserved.
2 attachments 985 KB
Save All
posten1693798.jpg 128 KB
posten1693798.pdf 857 KB


Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Chat
Address Book
Tag
From [redacted]
Reply
Reply
Followup
Forward
Subject International Conference on Energy and Environment Reserarch 2014
06/03/2014 07:06 AM
To [redacted]
Other Actions
Dear Colleagues,
You are invited to participate in the forthcoming International Conference on Energy and Environment Reserarch (ICEER 2014), which will be held in Madrid, Spain during July 18-19, 2014. ICEER is an event that focuses on the state of the art technologies pertaining to Energy and Environment Research. The applications of Energy and Environment Research to such domains as astronomy, biology, education, geosciences, security and health care are among topics of relevance to ICEER. It is a technical congregation where the latest theoretical and technological advances on Energy and Environment Research are presented and discussed. We expect that the conference and its publications will be a trigger for further related research and technology improvements in this important subject. ICEER promotes fundamental and applied research continuing advanced academic education and transfers knowledge between involved both sides of and the Energy and Environment Research.
For registration information you are to contact the conference Registrar.
Please share this information with your colleagues.
Sincerely
International Conference on Energy and Environment Reserarch Committee.
1 attachment: Conference_program.doc 1.9 KB
Save
Conference_program.doc 1.9 KB

Ideas and solutions for remote maintenance.

mbNET mbCONNECT24 mymbCONNECT24

MB CONNECT LINE
remote maintenance solutions

Software Downloads

mbCHECK (EUROPE)

diagnostic program mbCHECK for mbCONNECT24 server location EUROPE
Version: V 1.1.2
MD5 Checksum: A61FCB0F09F99E57B10F663923ECD472

mbCHECK (USA/CAN)

diagnostic program mbCHECK for mbCONNECT24 server location USA / CAN
Version: V 1.1.2
MD5 Checksum: BB977F03FEF48CE28DA48199EE8CFD6F

NEWS

all News »

- Career Opportunities:IT Specialist Customer Support and Training f / m
- Career Opportunities:IT Security Specialist / IT Security Manager f / m
- MB CONNECT LINE now part of the "Cluster Mechatronik und Automation"
- Manipulationen an SPS sicher erkennen
- LUA scripting workshop for mbNET.toolbox/mbSPIDER

```
Programm was started at 10:00:34
**************************************************************************
10:00:34.0225: Start finging of LAN hosts...
10:00:34.0256: Was found 1 hosts in LAN:
01) [                44A89C]
**************************************************************************
10:00:34.025 : Start finging of OPC Servers...
10:00:34.088 : Was found 1 OPC Servers.
1) [          8544A89C\Matrikon.OPC.Simulation.1]
                    CLSID: {F8582CF2-88FB-11D0-B850-00C0F0104305}
                    UserType: MatrikonOPC Server for Simulation and Testing
                    VerIndProgID: Matrikon.OPC.Simulation
                    OPC version support: +++
**************************************************************************
10:00:34.0897: Start finging of OPC Tags...
10:00:34.0897: Thread 01 running...
10:00:36.0725: Thread 01 finished.
1)[\\SVEIN-28544A89C\Matrikon Inc (780) 448-1010 http://www.matrikonopc.com]
Saved in 'OPCServer01.txt'
```

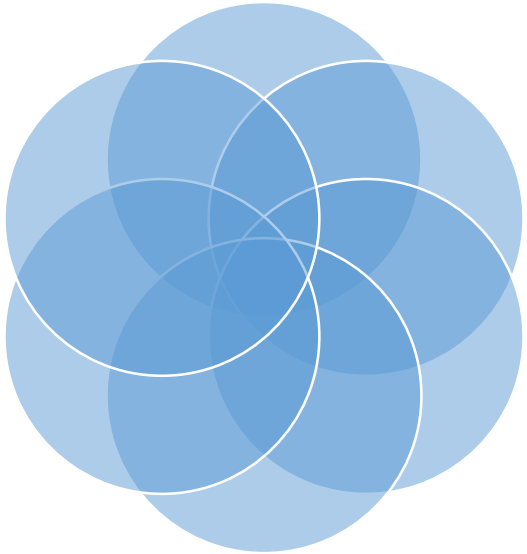
In retrospect

- Sending out physical letters was not very useful
- The crisis management personell were not always the best contact points
- The media “got it wrong”, however the effect was good nonetheless
- With the KraftCERT establishment we should do better the next time

Good Reactions

I accept the risk

Here's some more info on that attacker



Thank you, we'll pass this to the DFIR team

Thank you

That's a larger scope than we realised

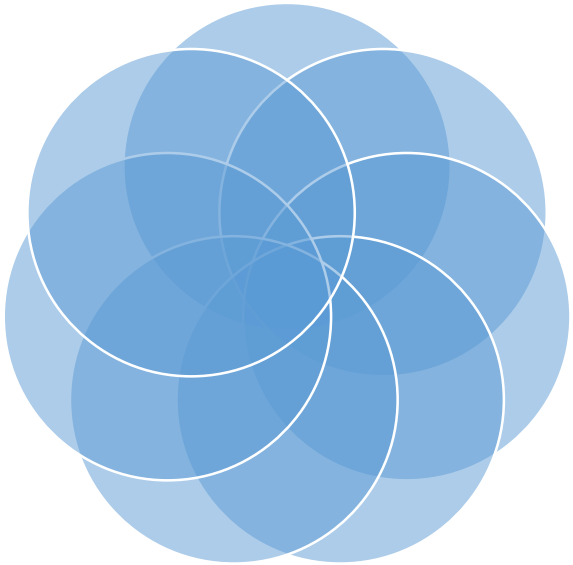
It's a honeypot

Bad Reactions

I'll sue you

We unplugged it and reinstalled the OS

You're interfering in private business



It's all hype

We are not liable for that

We followed the standards

A third party configured that

Conclusion Slide

Questions

Thank you