INTERNATIONAL
NUCLEAR SERVICES

INTERNATIONAL NUCLEAR SERVICES

Cyber Security in Marine Nuclear Transport Systems

PROUD OF OUR BRITISH HERITAGE

Contents:

1. What are we protecting?
2. Why do we need Cyber Security?
3. How do they do it?
4. Cyber incidents and threats – why it should be important to you
5. The dangers of removable media
6. A simple methodology
7. Conclusion

INS
INTERNATIONAL NUCLEAR SERVICES

INTERNATIONAL NUCLEAR SERVICES

INS is a wholly-owned subsidiary of the NDA with over 40 years experience of irradiated fuel management and nuclear material transportation.

Our vision:

Delivering specialist nuclear services with pride

Our mission:

- Supporting the NDA mission
- Delivering Growth

2,000+
casks of nuclear materials moved

5,000,000+
sea miles travelled

20
high level waste returns

12
MOX shipments

NEW DISPOSAL ROUTE
established for UK sealed sources from hospitals, universities and industry

NEW WORK STREAMS
supporting NDA at Springfields and Capenhurst with the Ministry of Defence

SIGNIFICANT PACKAGING DESIGN
and licensing input to support Dounreay Exotics Consolidation Project

PLUTONIUM TITLE TRANSFER AGREEMENTS
concluded with German, Spanish and Dutch customers over last three years

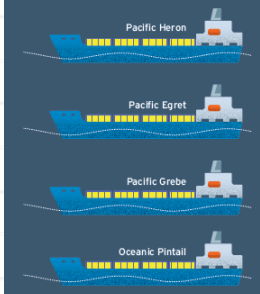
PROVISION OF PACKAGE ENGINEERING
and licensing services to RWM, Springfields and Capenhurst

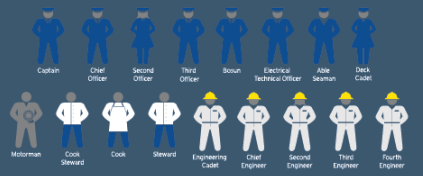
INS HAS PROVIDED END-TO-END TRANSPORT SOLUTIONS FOR MATERIALS INCLUDING:

- PLUTONIUM
- HIGHLY ENRICHED URANIUM
- MOX FUEL
- VITRIFIED HIGH LEVEL WASTE
- SPENT FUEL

10 CATEGORY 1 HIGH-SECURITY SHIPMENTS SINCE DECEMBER 2015 (IN PARTNERSHIP WITH THE CIVIL NUCLEAR CONSTABULARY)

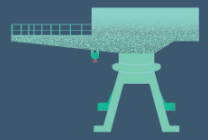
4 SPECIALIST NUCLEAR VESSELS





178 SEAFARERS

LONGSTANDING PARTNERSHIP WITH CIVIL NUCLEAR CONSTABULARY



A DEDICATED NUCLEAR MARINE TERMINAL

LOCATIONS IN THE UK AND OVERSEAS

PROUD OF OUR BRITISH HERITAGE

What are we protecting?

- The cargo, vessel and people aboard

- Sensitive Information

- The environment

- Our reputation

INS INTERNATIONAL NUCLEAR SERVICES

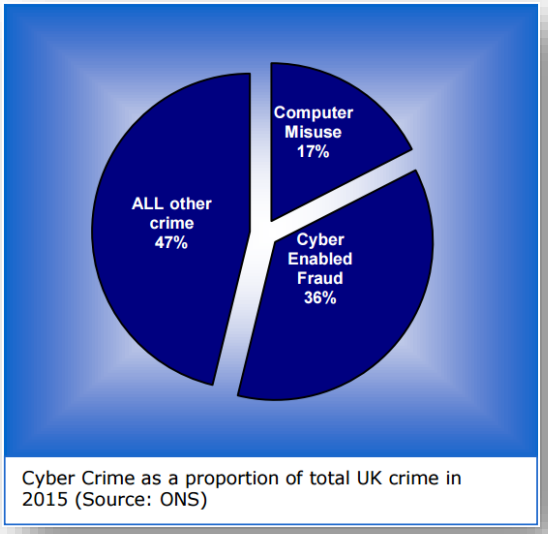
Headline Questions

- Is it possible to create an Uncontrolled Radiological Release (URR) by means of a cyber attack on an INS vessel?
- Is it possible to create operational difficulties through a cyber attack on an INS vessel?

INTERNATIONAL NUCLEAR SERVICES

Why do we need Cybersecurity?

- The percentage of Cybercrime in the UK is now more than 50% of overall crime
- 39% of recently surveyed ship operators admitted to being compromised in the last 12 months.
- Barrier to entry into Cybercrime is reducing all the time. Cybercrime as a Service (CaaS)
- Ransomware and Phishing campaigns are becoming more targeted and more successful every year
- Automation = cyber risk



Cyber Crime as a proportion of total UK crime in 2015 (Source: ONS)

INS INTERNATIONAL NUCLEAR SERVICES

How do they do it?

Breaching a system is like breaching a castle…

Stage 1 - Reconnaissance

Stage 2 - Plan + Choose vulnerabilities

Stage 3 - Intrusion

Stage 4 - Lateral Movement

Stage 5 - Privilege Escalation

Stage 6 – Data exfiltration and destruction of evidence.

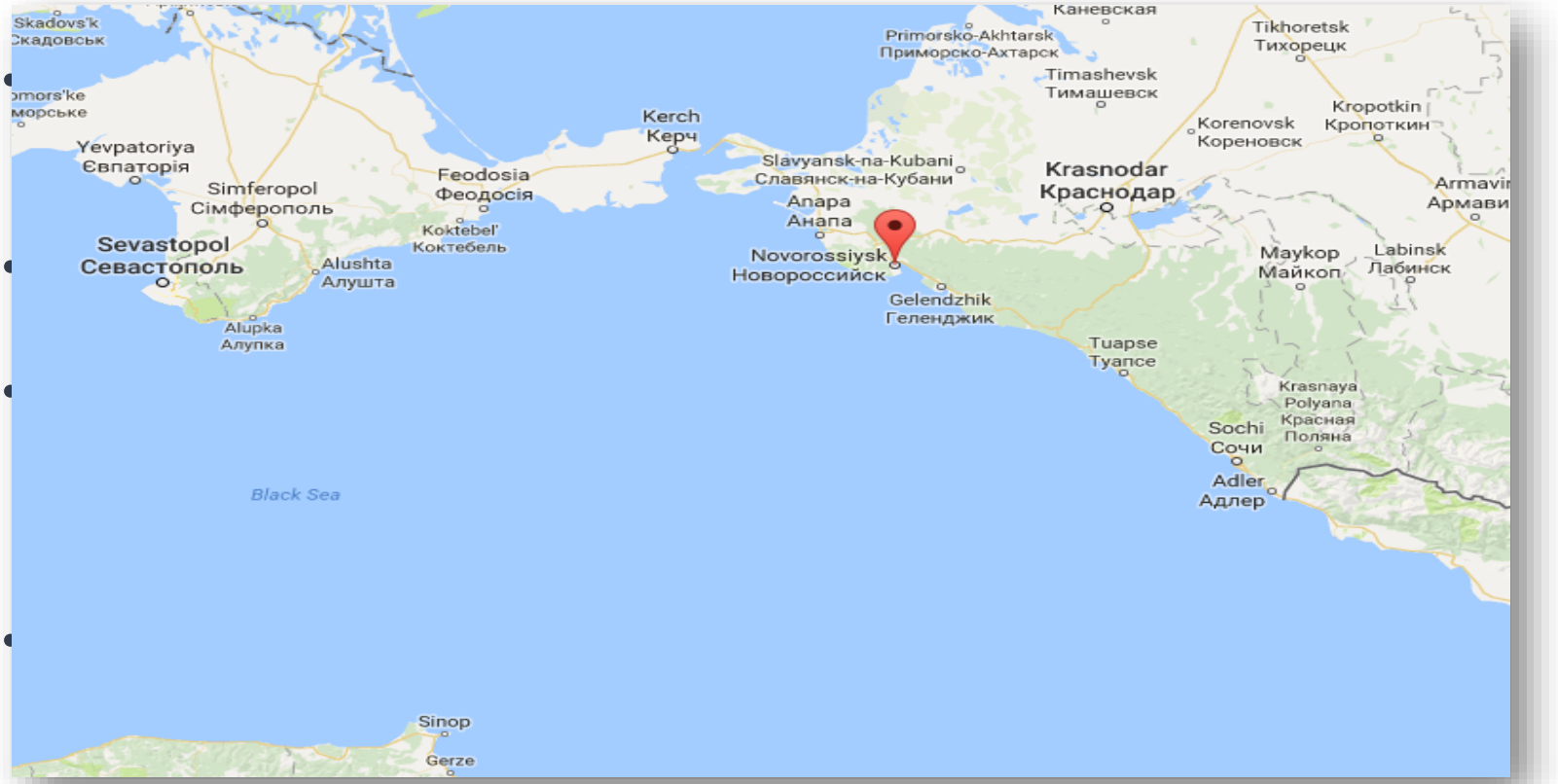
INS INTERNATIONAL NUCLEAR SERVICES

The White Rose of Drachs

INTERNATIONAL NUCLEAR SERVICES

Black Sea GPS incident

- Issues in June 2017 off the coast of Novorossiysk, Russia.



Compromise of on-board systems…

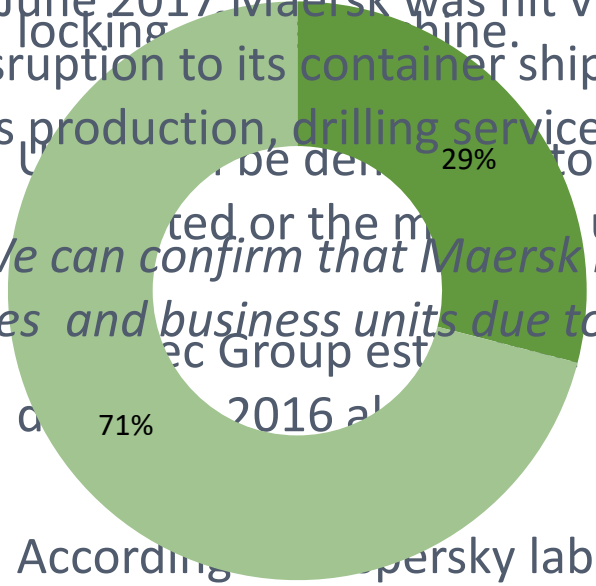
- In 2016 an 80,000 Tonne tanker was delayed significantly when its Electronic Chart Display was compromised, as it docked in an Asian port.
- Malware was accidentally spread to the system via an employee with an infected USB.
- The employee was unaware of the malware residing on the USB.
- When attempting to update the ships electronic charts with the USB, it was ultimately spread into the system.
- The malware had to be removed and an investigation launched before the ship was allowed to set sail.

Ransomware

- Ransomware is a strain of malware designed to incapacitate client machines either through encryption of the file system or permanent locking of the machine.
- User will be demanded to pay a Ransom to get the file system decrypted or the machine unlocked.
- Sophos Group estimates Ransomware generated over one billion dollars in 2016 alone.
- According to Kaspersky labs in Q3 2016 a business was hit with a ransomware attack every 40 seconds.
- The success rate of Ransomware attacks is alarmingly high, Given the security measures most organisations have in place.

In June 2017 Maersk was hit via this exact method, causing significant disruption to its container shipping, port and tug boat operations, oil and gas production, drilling services and oil tankers.

"We can confirm that Maersk IT Systems are down across multiple sites and business units due to a cyber attack" – Maersk (Twitter 2017)



INTERNATIONAL NUCLEAR SERVICES

Indirect attacks - Cargo System

- Australia's customs and border protection cargo system was compromised by hackers in 2012.
- The attack allowed drug traffickers to see which of their containers had been marked as suspicious.
- This crucial information allowed them to change their trafficking operation, to utilise different routes and methods to successfully get drugs into the target countries.
- Allowed criminals to evade law enforcement.
- Cargo systems have been targeted by pirates and drug traffickers previously. Highlighting the need to secure these systems.

INS INTERNATIONAL NUCLEAR SERVICES

Indirect Attacks – INS Context

INTERNATIONAL NUCLEAR SERVICES

Tangential attacks – Your context

- Do you know all the computer systems and networks which belong to you? (and those that don't that you rely on!)
- Do you know how connected they are to each other?
- Do you whether any are connected to the internet?
- Do you know who or what connects to them and why?
- Do you know the consequences of a cyber attack on any of your systems?
- Do you care?

INS INTERNATIONAL NUCLEAR SERVICES

The dangers of removable media…

- USB's are the digital mosquito.

Carrying Malaria ?

Not carrying Malaria ?

Navigational chart ?

Ransomware ?

- If you don't know the provenance of a USB, do not trust the USB

INS INTERNATIONAL NUCLEAR SERVICES

How should we respond?

- Leadership and competence
- Discovery
- Risk Appetite and Risk Management
- Culture

INS INTERNATIONAL NUCLEAR SERVICES

Conclusions

- The cyber threat is pervasive, innovative and growing
- If a system is connected, automated and has human interaction, the cyber vulnerabilities are high
- You must act if you wish to maintain the Confidentiality, Integrity and Availability of your systems and data
- A risk-based and business-focussed approach is probably most appropriate
- Good security culture is vital and central to mitigating cyber risks

INS INTERNATIONAL NUCLEAR SERVICES