Different Steps for Dealing with Cyber Attacks on a Country Level
Do’s and Don’ts

Miguel De Bruycker

Managing Director
Legal Basis

• R.D. 10/10/2014

Create a national policy and capabilities with existing actors

Coordination

Laws, standards, guidelines

Ensuring crisis management
Plan for incident response

- @Home
  - Awareness – notification – help

- @Work
  - Prepare – support – guide (insurance)

- @Critical Infrastructure
  - Warn – detect – handle
What you should know before any incident

We are not all equally sexy

Some of us need more & better protection

It’s better to detect yourself

All intrusions leave traces

Intrusions remain undetected for a long time

Advanced protection & detection
Lessons learned

- The CEO handles the incident
- Evaluate risks fast and continuous
- IT gets the fame, not the blame
- Have a full time communication manager
  - Communicate after surgery
  - If you talk … you pay
- Make a non-public top level final report
E + R = O

(Event + Response = Outcome)

*The Success Principles* by Jack Canfield
ENISA

Strategies for Incident Response and Cyber Crisis Cooperation

Think

Out of the box ...
Resilience of National Cyber Interests

The greatest enemy of knowledge is not ignorance, …

Cyber weapons are not like nuclear weapons…

The auditor is not a bloodhound …
Cyber Threats

The greatest enemy of knowledge is not ignorance, it is the illusion of knowledge

Malicious actions

Impact of these actions

Knowing the actors with intentions and abilities

Stephen Hawking
Early warning & information sharing

The next step after information sharing is making it actionable
Cyber Security Diplomacy

Cyber weapons are not like nuclear weapons…

They are more like biological weapons
Common characteristics

- Risks of development & warehousing
- Controlled use is impossible
- Attribution issues, remain intact after usage
- Target advantage, reproduction takes a relative small effort
- Expiration date

Justifiable use

Diplomacy

Not unthinkable or outlawed
Cyber Security Norms

The auditor is not a bloodhound,

he is a watchdog

International Cyber Security Norms

Accredited auditors

Certified technology and networks
Cyber Security Norms / Standards

• Baseline Cyber Security Norms
  • Home user
  • Industry
  • Critical infrastructure (all sectors)

• International standards

• Audits & certifications
E + R = O

*The Success Principles* by Jack Canfield

Questions?

Info@ccb.belgium.be