Attention - SCADA security awareness

EU SANS SCADA Security Summit, 2008-09-09

Corporate Information Security Expert, E.ON Nordic
Gitte Bergknut

The big question – How do we get Top Managements attention?

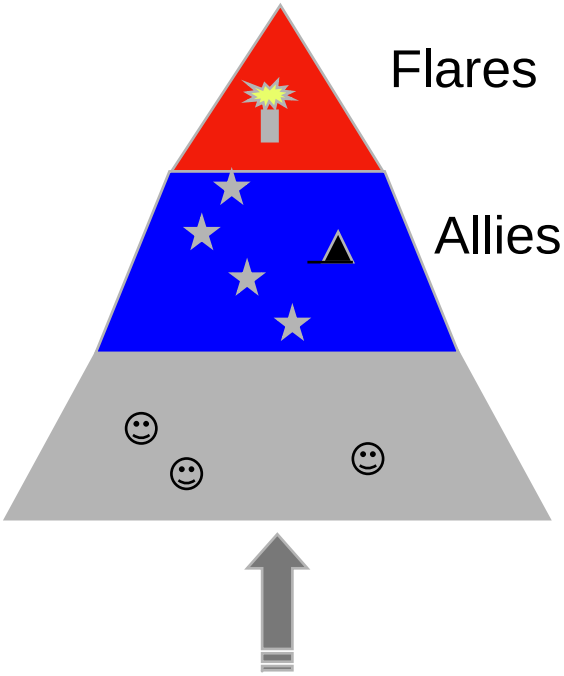
Step One To achieve that is – You need to know what You are d

- You got to know – What to achieve
- You got to know – Why it is important
- You got to know – How to get there present a plan
- And be prepares to prove and strengthen Your arguments

Before You try to get attention!

Next step - Get the message out in the organization. Spread the word – everywhere and every possible time but work Your way upwards and adjust Your language on the way.

Start to ring the bell!



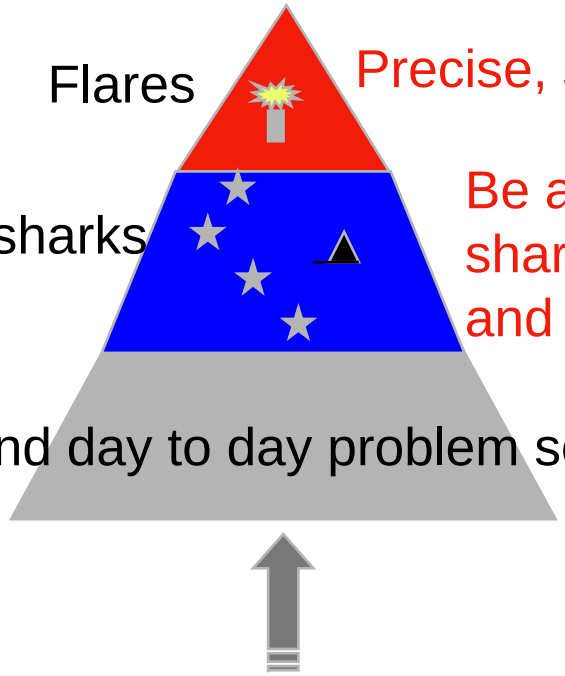
Flares

Allies and sharks

Staff and day to day problem solvers

When You ring the bell adjust the language and form of the message on the way

Shake the ground a little!



Flares

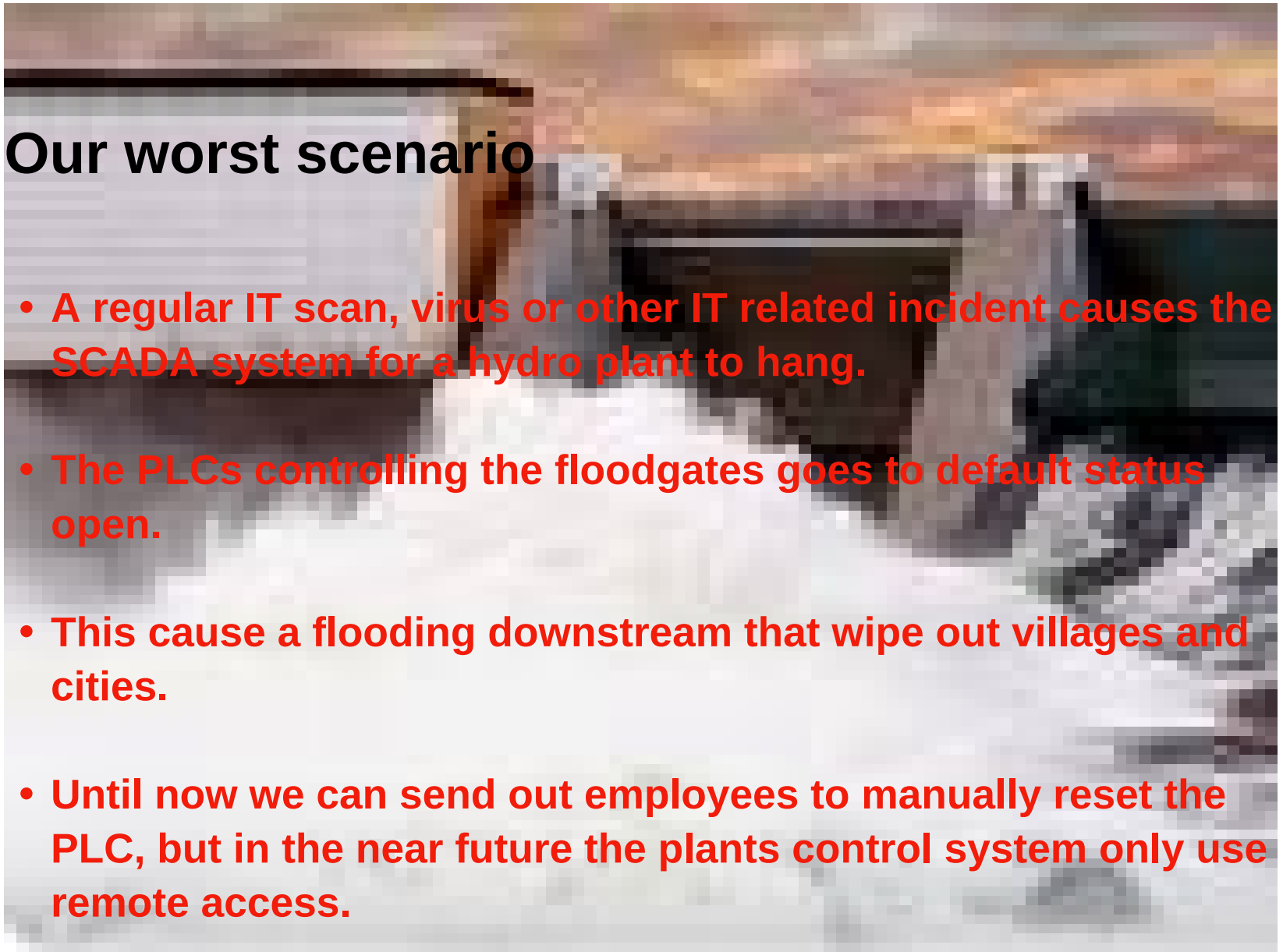
Precise, short, strategic and repeated regularly

Allies and sharks

Be aware find your allies and watch out for the sharks. Extend your message fill it with details and references to reliable sources

Staff and day to day problem solvers

Precise, short and hands-on



Our worst scenario

- A regular IT scan, virus or other IT related incident causes the SCADA system for a hydro plant to hang.
- The PLCs controlling the floodgates goes to default status open.
- This cause a flooding downstream that wipe out villages and cities.
- Until now we can send out employees to manually reset the PLC, but in the near future the plants control system only use remote access.

SCADA system and security ?

- From the GAO report, May 2008, security study regarding TVA.

- Remote access system was not securely configured
- System and clients was not security patched
- Lack of security security settings for key programs
- Firewalls were bypassed or inadequately configured
- Passwords were not effectively implemented
- Logging was limited
- No antivirus protection
- Lack in security in the connections between Process and Office IT network
- Etc…..
- Conclusion “TVA Needs to Address Weaknesses in Control Systems and Networks

General problems

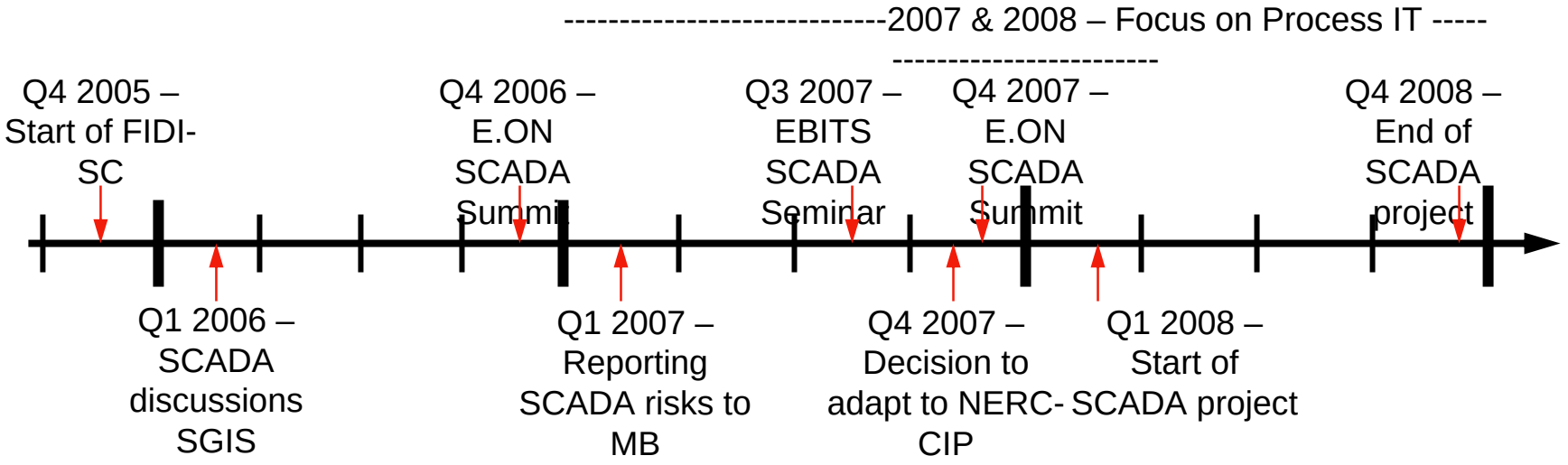
- We can not easily identify which category a computer belong to. It makes it more difficult and delay the incident management process.
- We are were of that incidents with malicious code have occurred on computers within control rooms.
- Difficult for the IT security function to get enough information about process related network and system including surroundings and connections to SCADA equipment.
- Our monitoring of the office network detect infections of malicious code and suspect behavior. We can today not detect anything of this within the SCADA environment. This could result in incomplete or incorrect handling and conclusion.
- We do not know if, an in that case which, information from SCADA system or network that have been exposed to the public.

Mitigation actions

- Create an inventory of ”SCADA” system within and outside the Industrial IT network using our standard inventory system
  - Physical and logical placement
  - Communication dependence
  - Connection to other network
  - Valid clients, different name standard
  - Existing security mechanisms, physical/logical
- Use our Incident reporting system on the intranet also for SCADA related incidents
- Installation of process IDS, alarm to existing SOC and operative personel
- Get support for regular audits at facilities
- Business representative must participate in the energy sectors SCADA security seminar

SCADA Security awareness timeline at E.ON

- Information Security Risk reporting is included in the RM process
- E.ON Sveriges Information Security process is based on best practice and has influenced E.ON Steering Group Information Security
- Active participation in and influence on best practice forums and other professional bodies and authorities are a part of the activities of the Information Security department



The Management Board decided and how are we doing?

- Inventory of ”SCADA” system within and outside the Process IT network **(CIP-002)**
  On-going
- Use present incident reporting process and tool to report Information and IT security incidents from SCADA system and Process IT **(CIP-005)**
  Implemented but training actions are on-going
- Installation of process IDS, alarm to existing SOC**(CIP-005)**
  Preparation phase
  Proof off concepts are On-going
- Regular security audits
- Participate in the energy sectors SCADA security seminar
  On-going at least 10 E.ON representatives are here today!

And we are actively participating in the VIKING research project.

Safety and confidence are built in millimeter,
but are demolished in kilometer

Security create safety and confidence,
but lack of security demolish it