Information Security Incident Management:

Planning for Failure

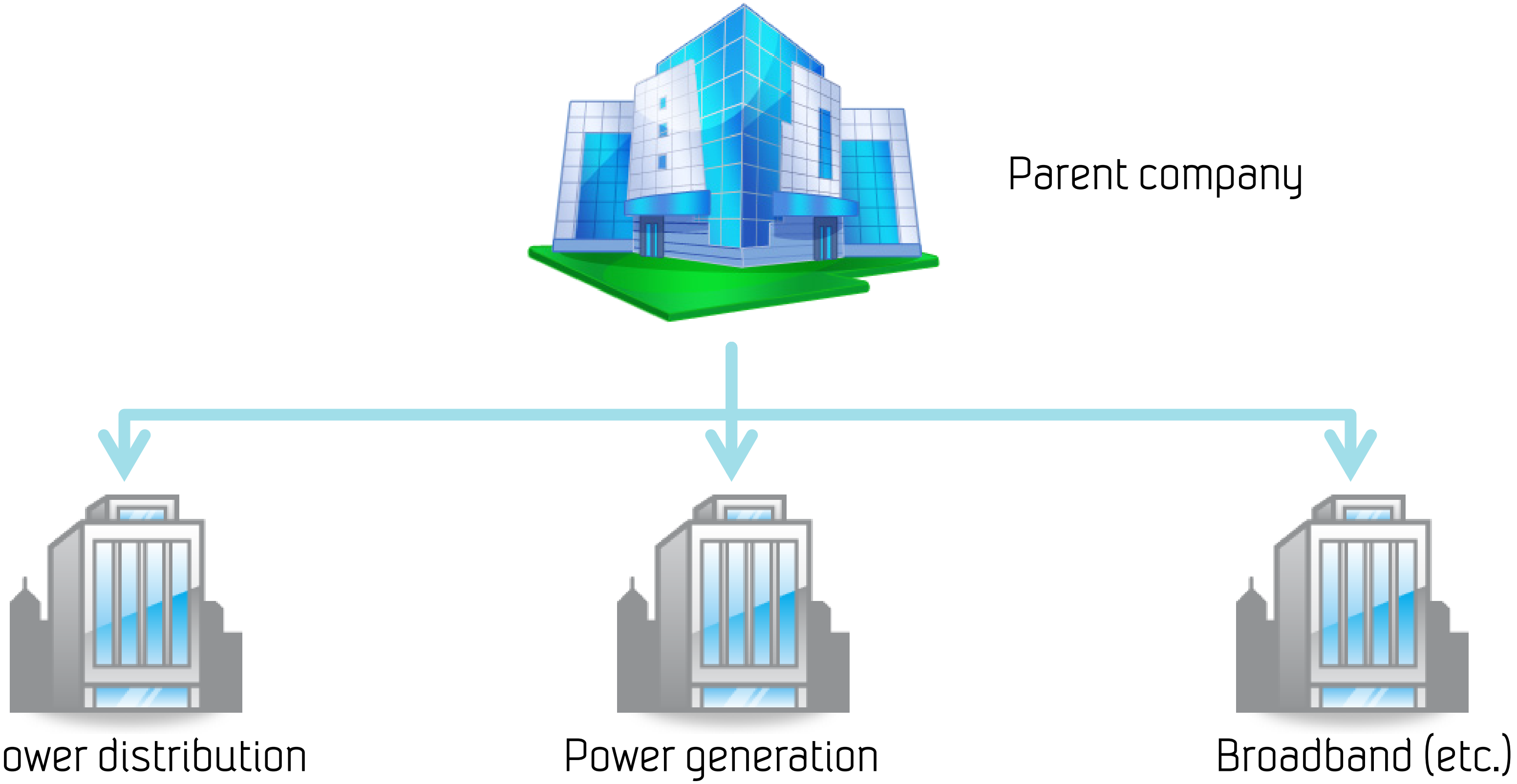
(in Power Distribution Companies)

Maria B. Line, Inger Anne Tøndel, and **Martin Gilje Jaatun**

Martin.G.Jaatun@sintef.no

Background

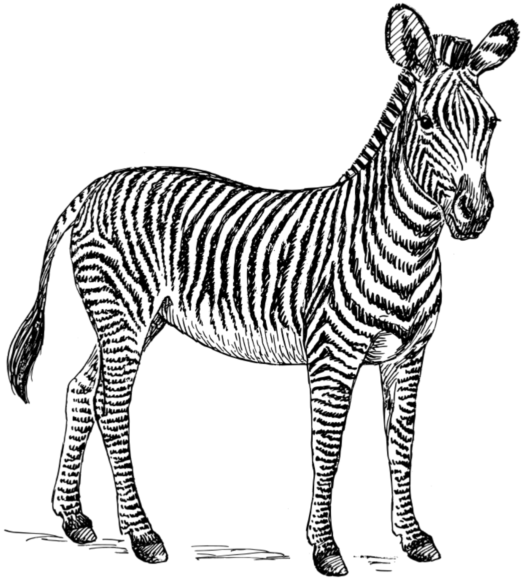
- Interviews with 6 power distribution service organisations (DSOs)

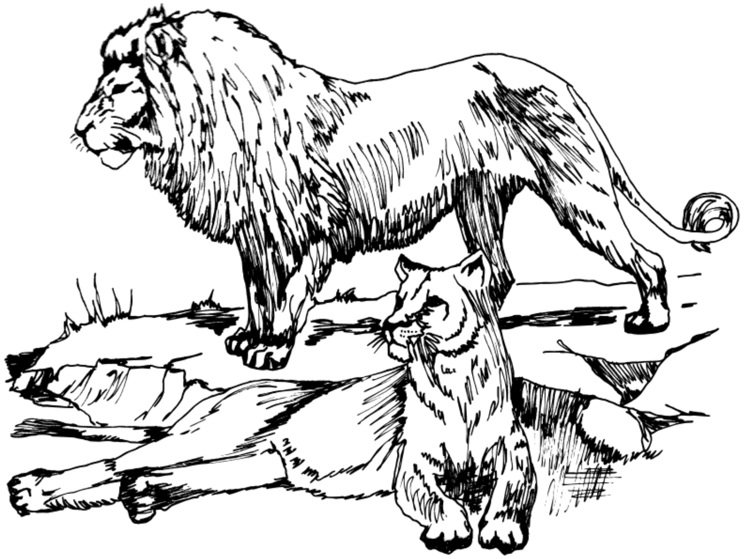


Introduction

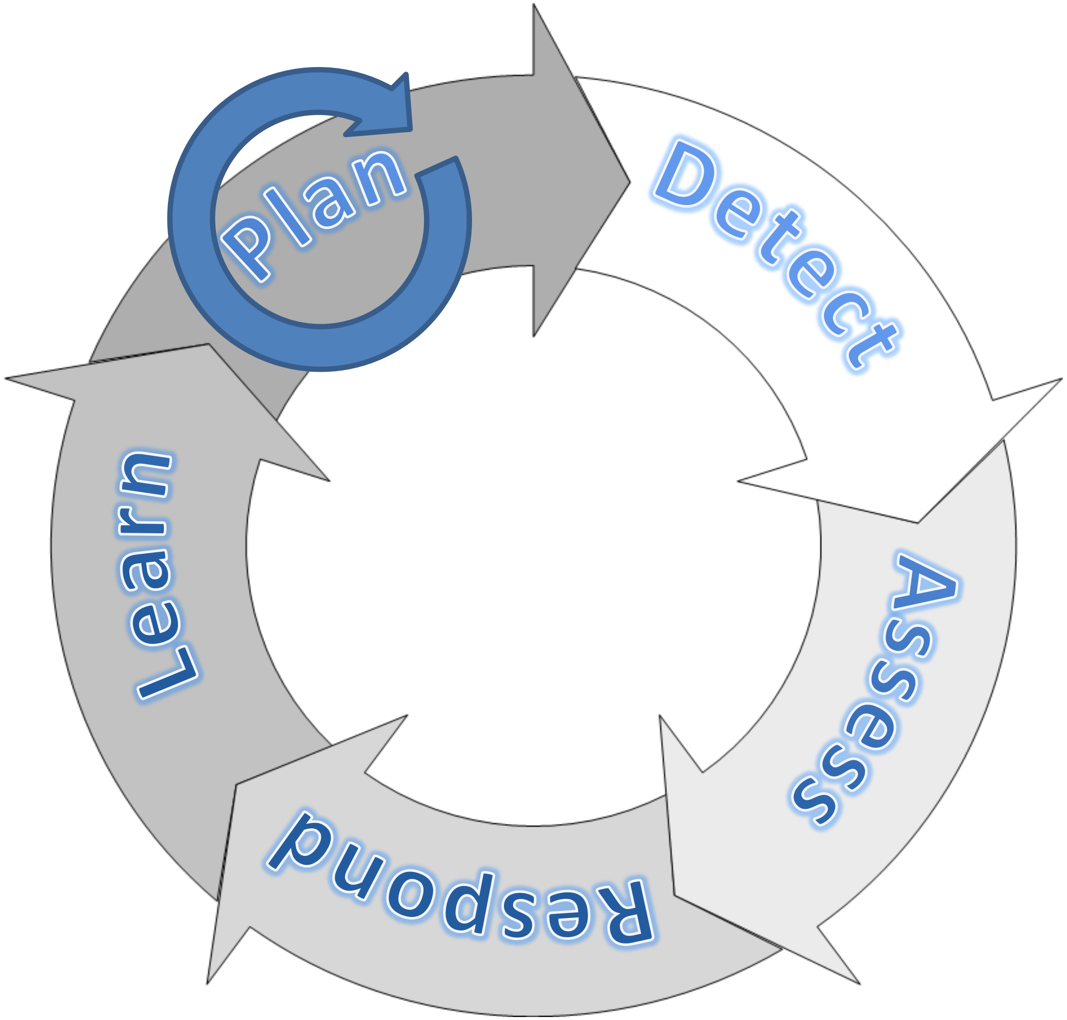
- IT is permeating Industrial Control Systems
  - COTS components
  - Increased interconnection

IT & ICS: Lions vs. Zebras?





ISO/IEC 27035 Incident Handling Cycle



Research Questions

- How are power distribution companies planning & preparing for incidents?
- What differences exist between IT & ICS?

Interviewees

DSO	IT Manager			IT Security Manager			Sec%	Ctrl Op
	Parent	Branch	Outsrc	Parent	Branch	Outsrc		
A			X		X		5%	(x)
B	Y			Y			100%	(x)
C	Y	X						(x)
D	X				Y		10-20%	(x)
E	X				X		100%	(x)
F						X	50%	(x)

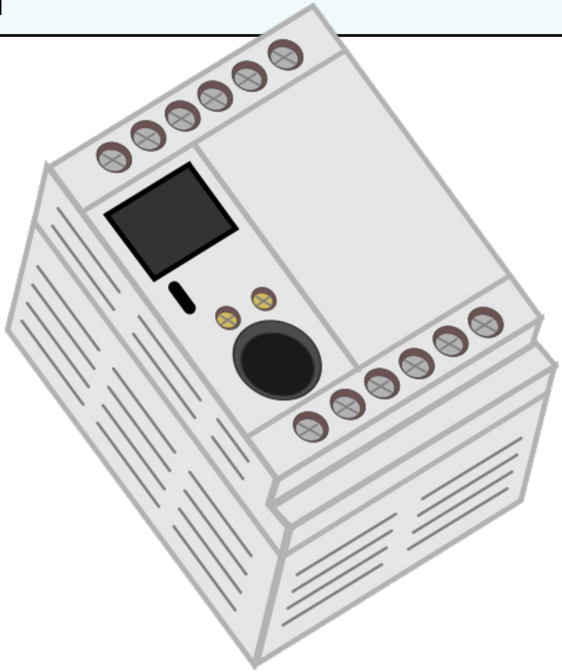
X: Only administrative system

Y: Both IT and ICS

(x): Only ICS

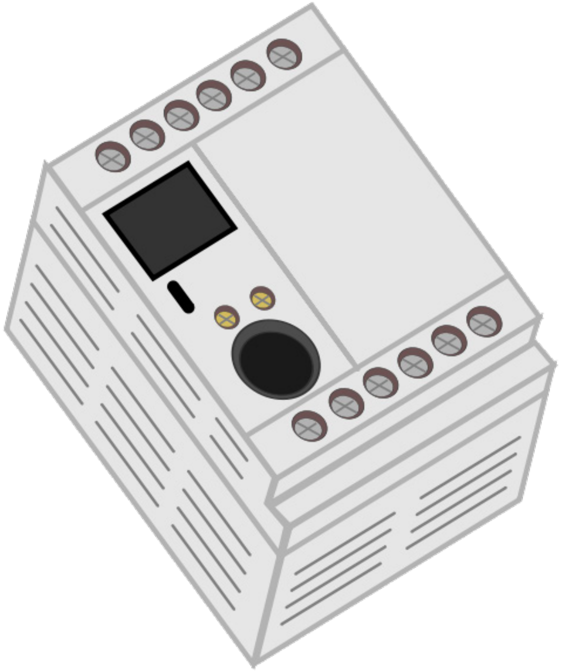
Dependency on IT

IT /IT Sec	Control Room Managers
100 %	100%
Cannot dig, maintain or invoice	2-3 days on manual without loss of power production



What is an incident?

IT /IT Sec	Control Room Managers
Uniform view	No clear definition ("not defined here")
Consistent examples	Wide variation in examples
Happens weekly	Has never happened



ICS incidents

- Mainly concerned with the consequences for power supply

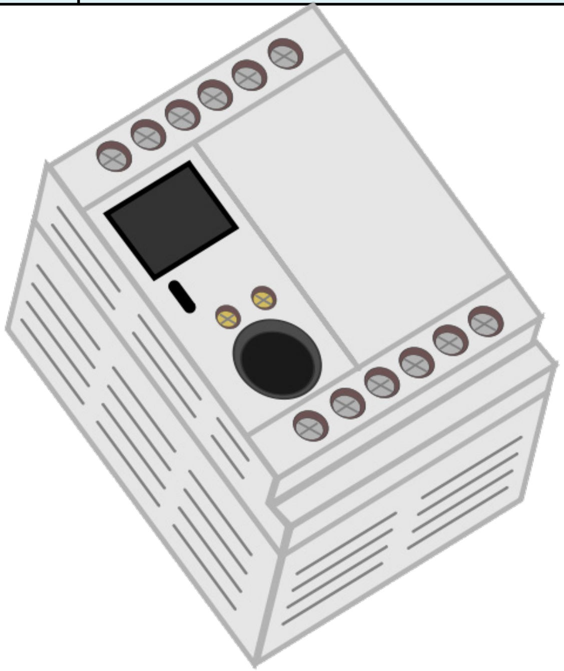
Worst case scenario

Worst case, cont.

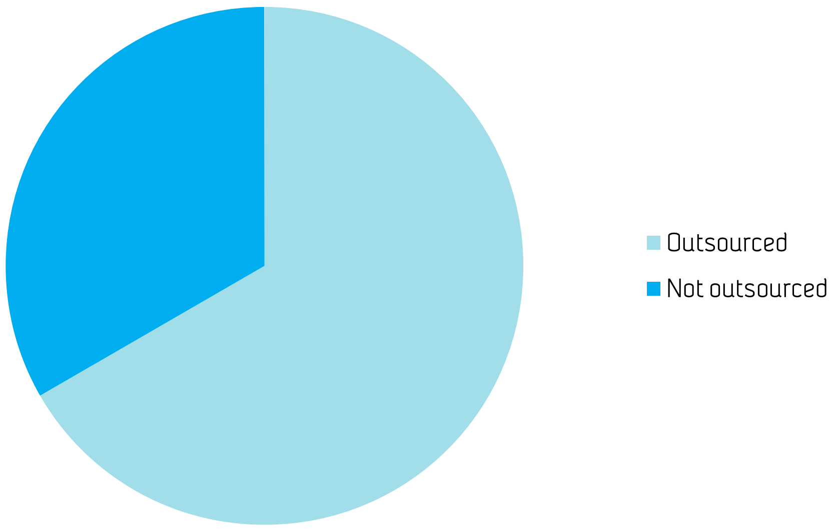
- IT and IT Sec personnel also considered loss of customer data
- Worst case is compounded by combinations of incidents
    - Remember: Murphy was an optimist!

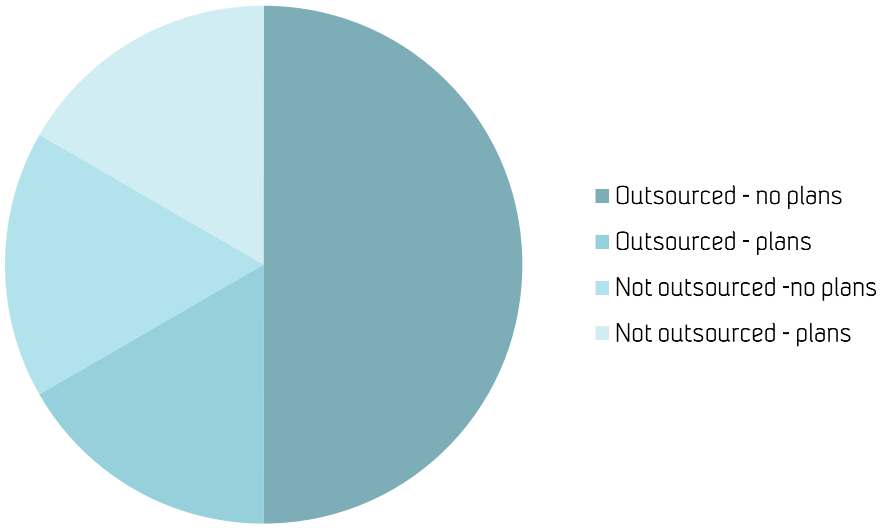
Documentation of plans

Outsourced IT		Not outsourced		Control Room Managers
Have plans	No plans	Have plans	No plans	Too complex to have plans
1	3	1	1	
	(2 in progress)		(1 in progress)	Plans are seldom used



More on the distribution





Plans, cont.

- In many cases, responsibilities were left unspecified
  - Especially when IT services were outsourced
- Plans that *do* exist do not cover ICS

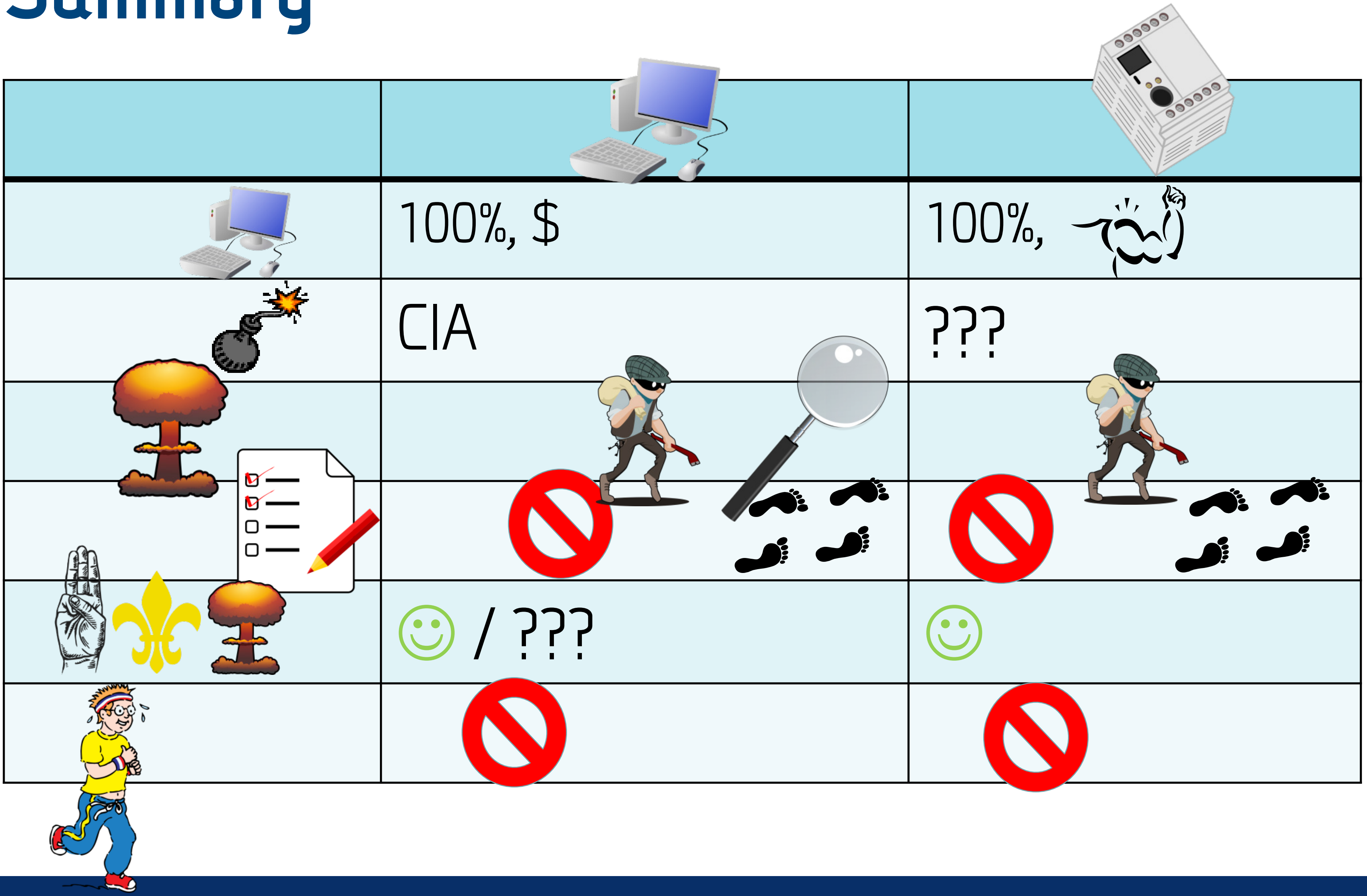
Exercise is good for you

- … and yet no DSOs report that they perform information security training exercises
  - Some regular emergency training is also relevant for IT sec
  - Even if they have never performed training, many DSOs believe they will manage an incident if it happens (optimistic bias)

The nice thing about standards

- … if you do not like one, you can always find another!
- None of the interviewees mentioned ISO/IEC 27035
  - …and we didn't ask them specifically
  - No other standard was mentioned either

Summary



	100%, $	100%, 💪
	CIA	???
	🚫	🚫
	☺ / ???	☺
	🚫	🚫

Research Questions Revisited

- How are power distribution companies planning & preparing for incidents?
  - If they are planning, it's generally not written down
  - Preparing is not done using exercises
- What differences exist between IT & ICS?
  - Still lions and zebras

Questions?

?

twitter.com/
SINTEF_Infosec

Infosec
Blogg

http://infosec.sintef.no

http://sintef.org/ses

Martin.G.Jaatun@sintef.no