28th ANNUAL FIRST CONFERENCE

SEOUL

JUNE 12 - 17, 2016

GETTING TO THE SOUL OF INCIDENT RESPONSE

Does it pay to be cyber-insured

Dr. Marie Moe
Research Scientist, SINTEF ICT, @MarieGMoe SINTEF
Mr. Eireann Leverett
Founder and CEO, Concinnity Risks, @blackswanburst @concinnityrisks

28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016

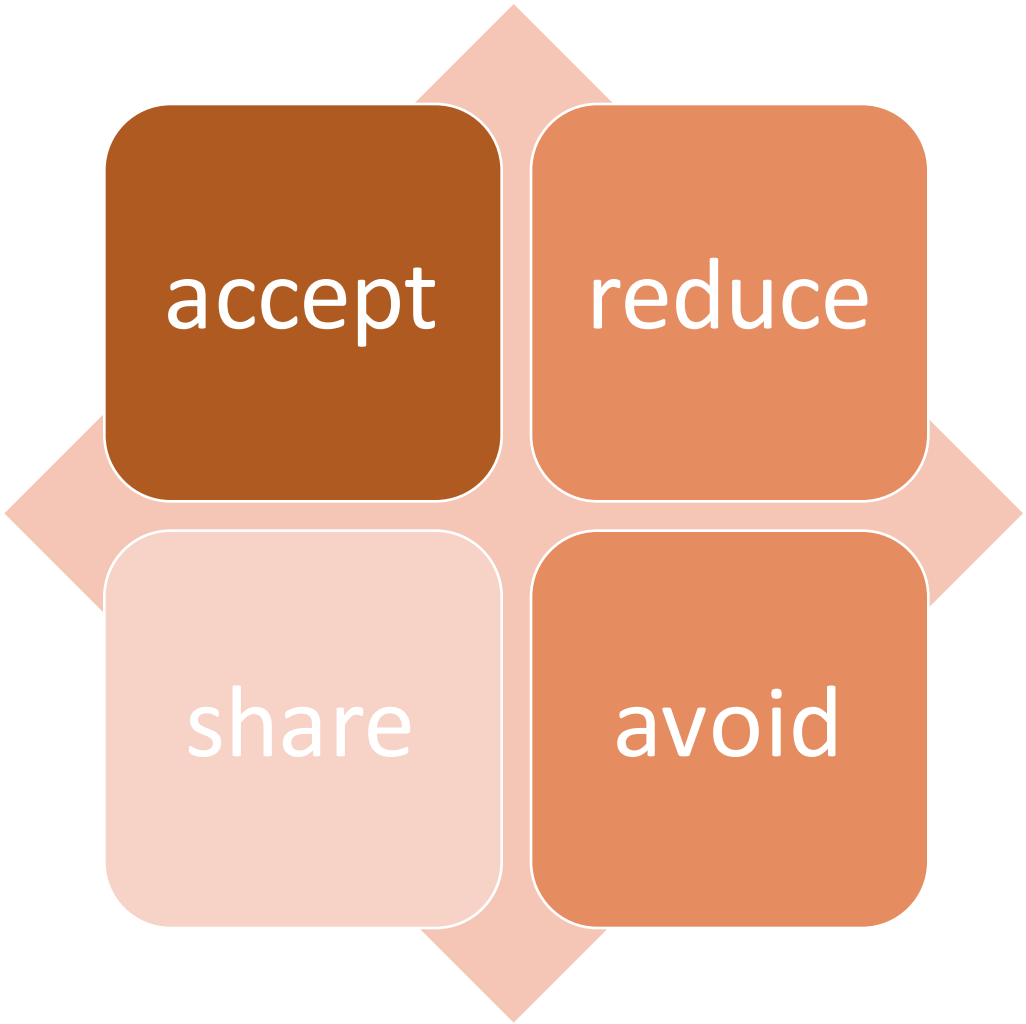
Key issues

- Where do insurance companies best fit in to the incident response lifecycle?
- How can CERTs collaborate with insurance companies to mitigate and minimise costs of cyber incidents?
- What language do CERTs need to speak to interact efficiently with insurers?
- Why modelling is important

Myths and Facts

They won't pay out	• They already have. *cough* German Steel Mill *cough*
Cyber war/nation state/APT is excluded	• If you can't attribute, how can they?
It steals my security budget	• It should come from your POST incident budget • You do divide budget into PRE and POST, right?
They don't know anything	• They hire us, as the market grows • They're not fire, auto, or aircraft experts either • They progress the art of security at higher abstraction

Traditional risk management



You know this story already:

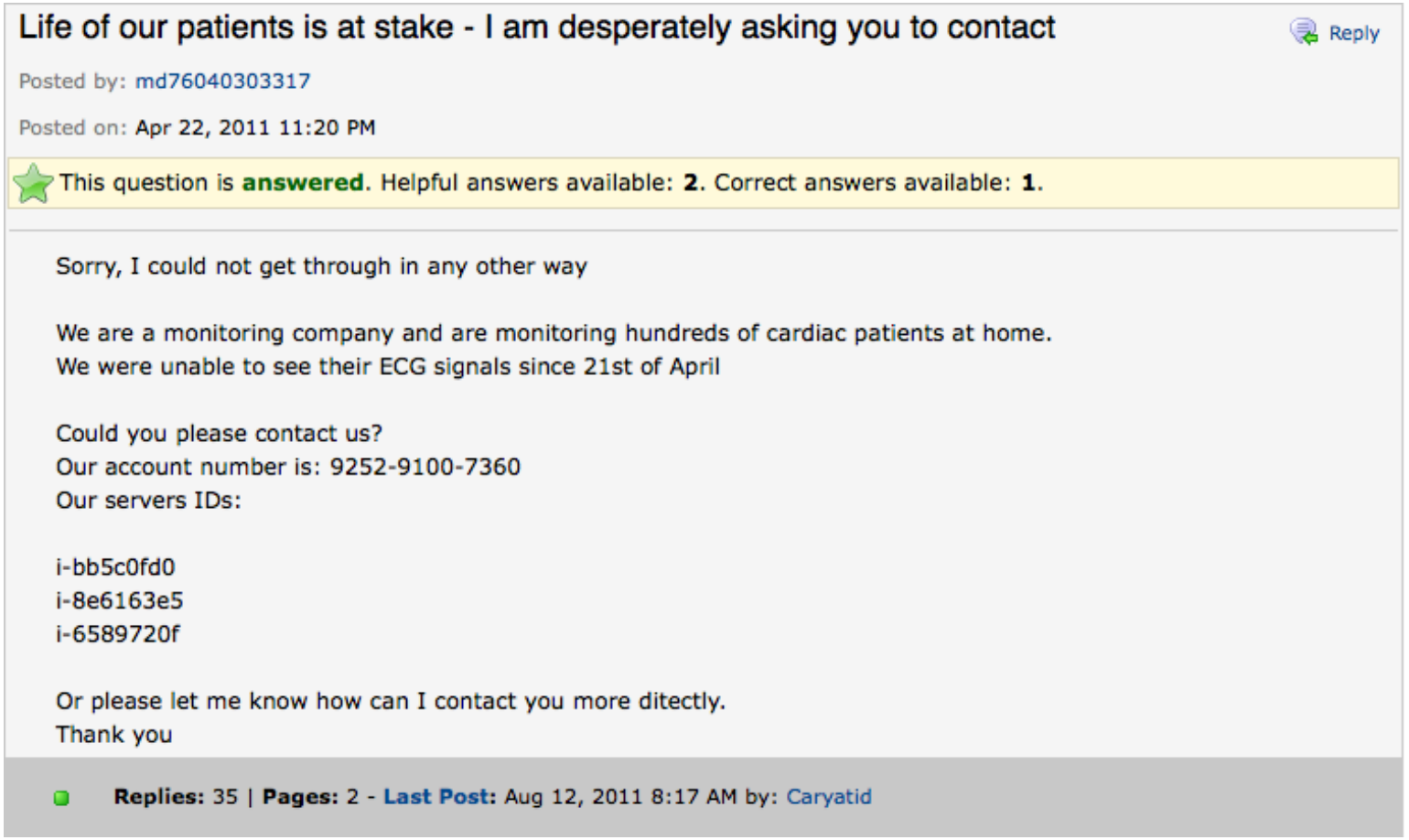
- **too much acceptance,**
- **a little reduction,**
- **a pinch of avoidance**
- **hardly any sharing.**

So let's play what if…

What if we share: cyber-insurance

Cyber:	Traditional
•Breach •DDoS •Business Interruption •Contingent Business Interruption •Financial Fraud •Ransom/Ransomware •OT (physical damage in engineering lines)	• Material Damage • Directors and Officers • Commercial General Liability • Construction • Life • Event cancellation

Example: Cloud outage



Life of our patients is at stake - I am desperately asking you to contact

Reply

Posted by: md76040303317

Posted on: Apr 22, 2011 11:20 PM

This question is **answered**. Helpful answers available: **2**. Correct answers available: **1**.

Sorry, I could not get through in any other way

We are a monitoring company and are monitoring hundreds of cardiac patients at home.
We were unable to see their ECG signals since 21st of April

Could you please contact us?
Our account number is: 9252-9100-7360
Our servers IDs:

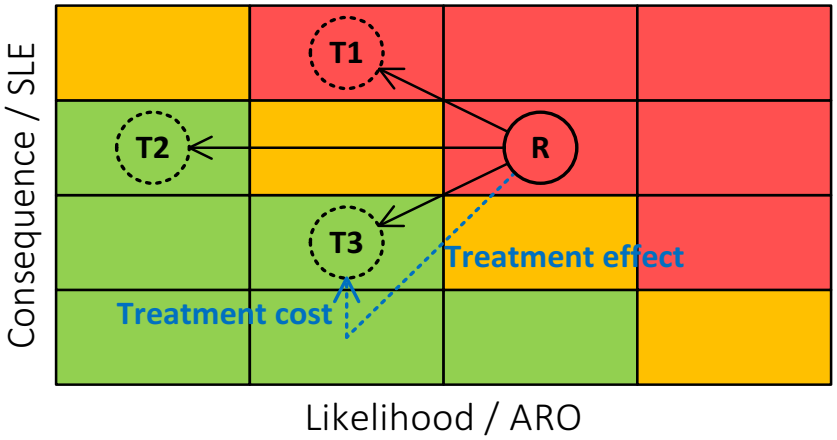
i-bb5c0fd0
i-8e6163e5
i-6589720f

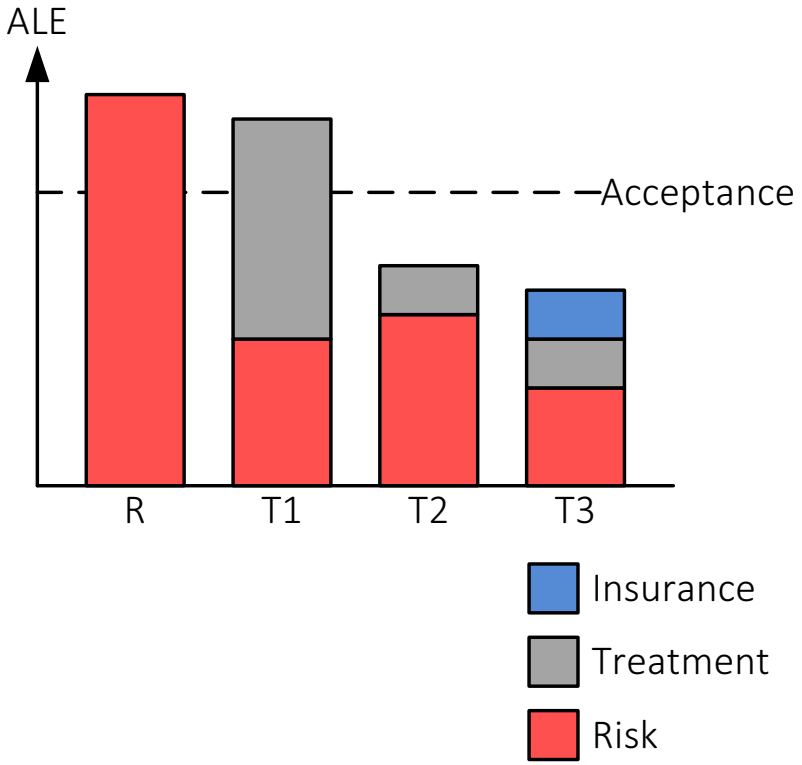
Or please let me know how can I contact you more ditectly.
Thank you

Replies: 35 | **Pages:** 2 - **Last Post:** Aug 12, 2011 8:17 AM by: Caryatid

Source: https://forums.aws.amazon.com/thread.jspa?threadID=65649

Cyber-insurance in risk management





- SLE: Single loss expectancy
- ARO: Annual rate of occurrence
- ALE: Annualized loss expectancy

Exclusions matter

- Without “cyber exclusions” traditional insurance covers cyber losses.
- THINK ABOUT THAT
  - My lawyer got hit by ransomware…
  - Travelers Insurance vs Portal Healthcare Solutions…
- Let’s talk about FLEXA

Cyber Exclusions for Traditional Insurance

- NMA 2912 AND 2928
  - NMA 2912 excludes losses arising out of the "(i) *loss of, alteration of, or damage to, or (ii) a reduction in the functionality, availability or operation of*" computer systems, hardware, programs, software, data information repository, microchip, integrated circuit or similar devices in computer equipment or non-computer equipment
- NMA 2914 AND 2915
  - NMA 2914 and 2915 exclude loss, damage, destruction, distortion, erasure, corruption or alteration of electronic data, and any loss of use, reduction in functionality, cost, expense of whatever nature resulting from that loss of data. Data is defined in the clause, and is said to include software.
- CL 380
  - CL380 is the widest of the exclusions, and is in common usage in upstream energy policies. It excludes all loss, damage and liability directly or indirectly caused by, contributed to by, or arising from, the use or operation "*as a means for inflicting harm*" of any computer, computer system, computer software program, malicious code, computer virus or process or any other electronic system.
- ADVANCED CYBER EXCLUSION CLAUSES BEING DRAFTED

Why should CERTs care about cyber-insurance?

- A common interest in detection, response and prevention of loss
- A new strong stakeholder in the threat intelligence and info sharing “market”
- Outsourcing of risk
- Outsourcing/collaboration on CERT services
- Business opportunities in partnering with insurance companies

How do insurers choose their customers?

Key risk factors

- Key information to collect
- Key measures to monitor
- Accumulated risk
- Catastrophic event risk

Constraints

- In-house competence
- Available data
- Building customer base

Making compro-mises

- Efficient processes vs trust in data
- 3rd parties vs in-house capacity
- Baseline requirements vs sales

Speaking different languages/ Learning to collaborate

They need your data to make models

- This brings down the cost

We need some of their cash and enthusiasm

They need our:

- Training
- Services
- Data
- History
- Collaboration

We need their patient market interventions

They need our expertise when evaluating the risk of their customers

Interfaces in other teams

They might give you work

Or might take work from you

We get more time to work on emerging threats

They reward mitigation toolsmithing

They need threat intel and “near miss” data

Cost effective

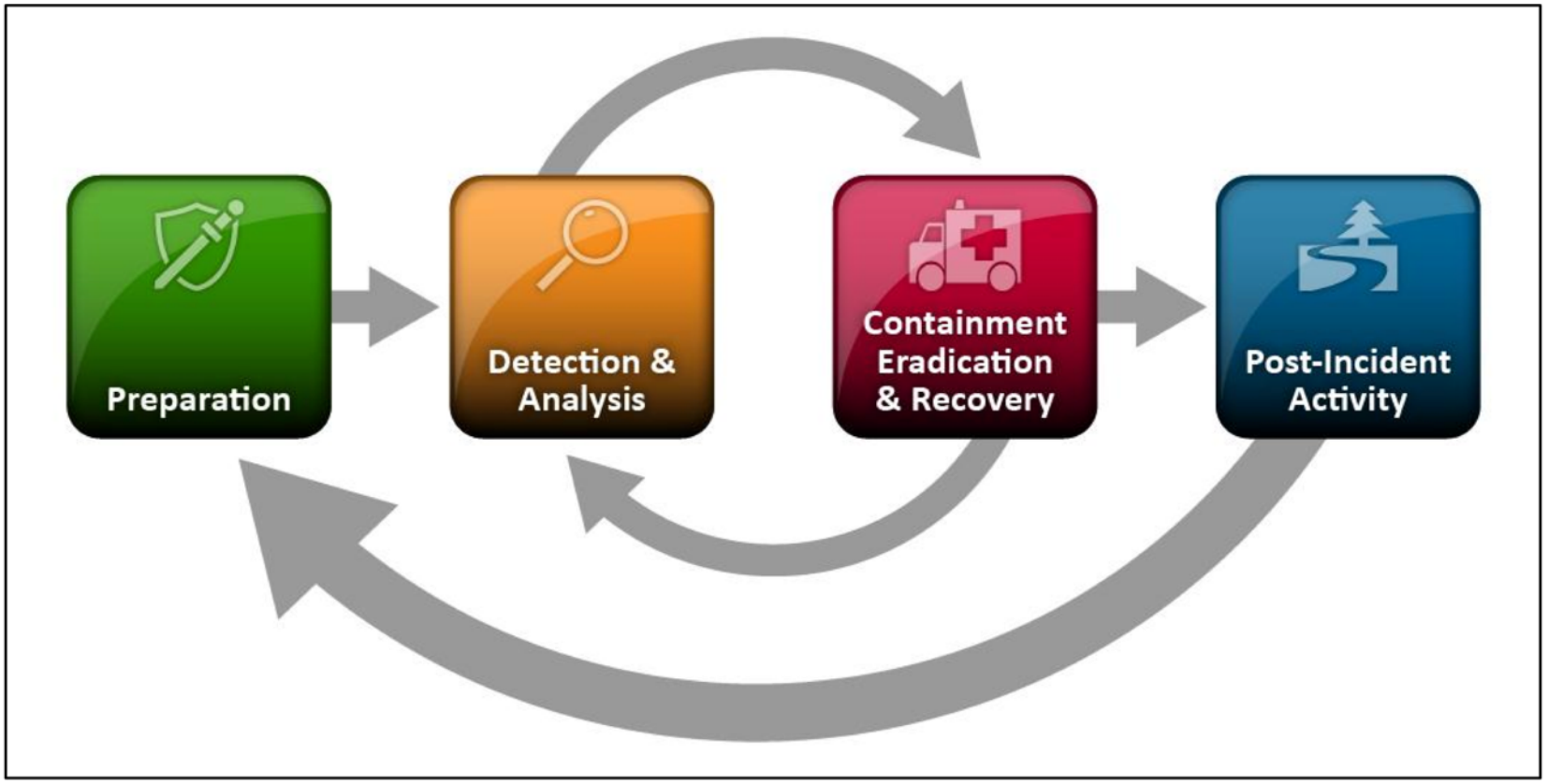
Initially through Marie and Eireann

Ideally they deal with boring incidents

Our DFIR innovations get valued!

Build interfaces today with insurers

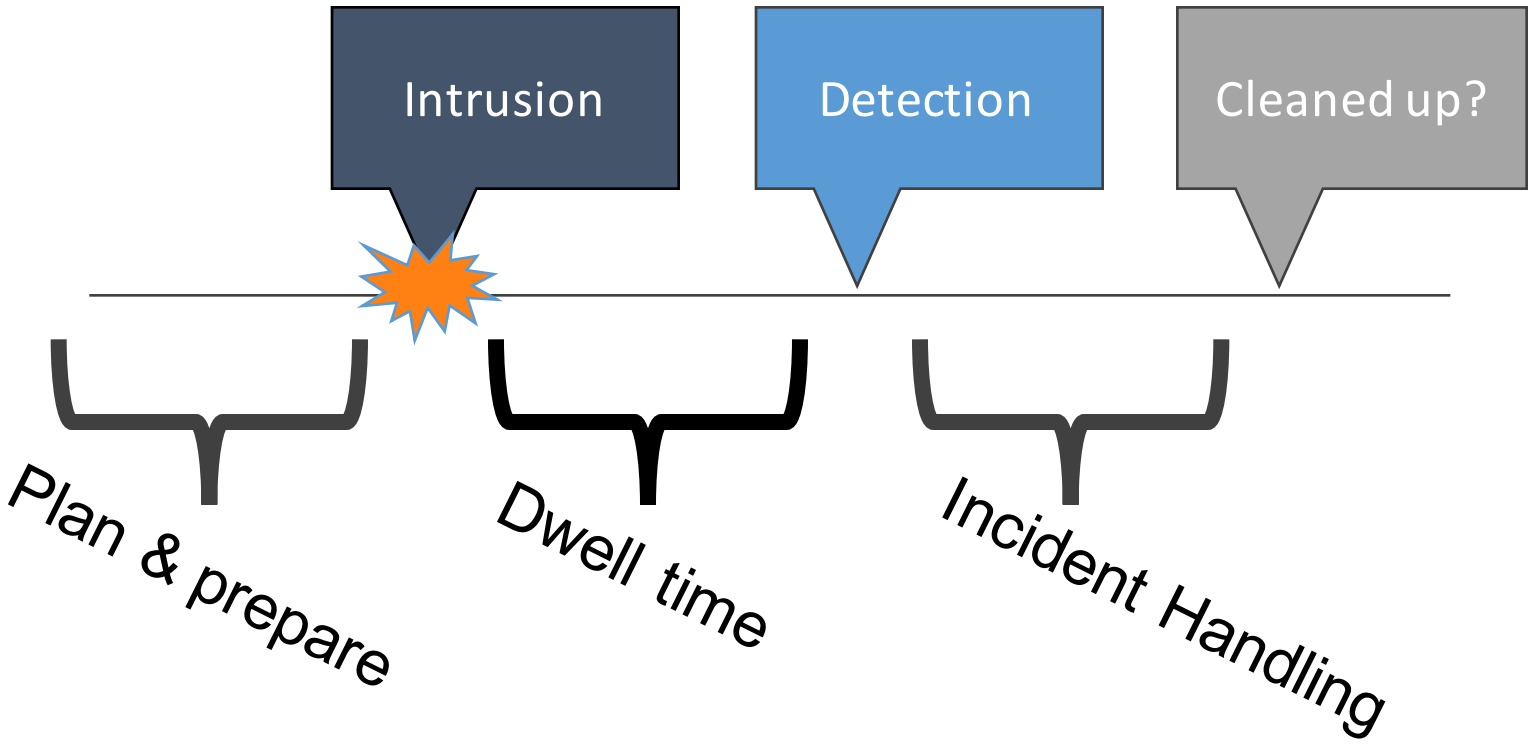
The incident response life cycle



NIST SP 800-61, Revision 2

Where does cyber-insurance come in to play?

Where do we want it to come in to play?	• Triggered for large incidents? • A feed of incidents to work?
Data sharing?	• Public Private Partnership management? • Risk Models?
Market interventions	• Test Lab creation? • Standards management?


Intrusion
Detection
Cleaned up?
Plan & prepare
Dwell time
Incident Handling

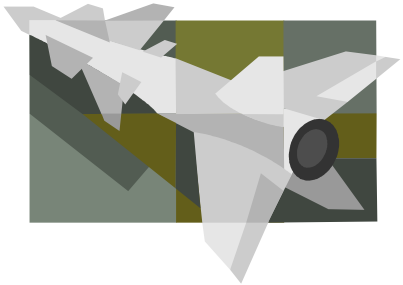
When to report?

- Think about two reports: insurance and CERT
- Most reporting happens after an incident has been detected
  - Insurers offer rapid-response services to quickly assess a possible intrusion after detection
- What about undetected intrusions?
  - Reporting of near-misses and prevented incidents gives valuable threat intelligence
  - Customers may be reluctant to disclose their vulnerabilities
  - Can insurers provide incentives?

How to calculate the cost of an incident?

Defender

a) Cost of preparing to respond
b) Cost of response (b > a)
c) Loss (c >> a+b)
d) Cost of insurance (d > a+b)
e) Insurance payout (e < c)



Attacker

a) Cost of preparing and executing attack
b) Profit (b >> a)
c) Penalty (c << a+b)

When does it pay to be cyber-insured?

- When the cost of insurance is lower than the expected loss
- When insecurity is great and unpredictable
- When the consequences are catastrophic
- When the victim does not have enough resources to handle the consequences

Cyber-insurance as risk control strategy

- Risks can be controlled by:
  - Avoidance
  - Mitigation
  - Acceptance
  - Termination
  - *Transfer or share*

- What is the benefit of risk transfer?

Conclusions

- It’s here, and paying out
- You might as well meet them, understand them, learn from them, and teach them
- Watch those exclusions
- Some incidents could be referred to insurers!
- Or costs reclaimed?!?

Questions?

Dr. Marie Moe

@MarieGMoe
marie.moe@sintef.no

Mr. Eireann Leverett

@blackswanburst, @concinnityrisks
eireann.leverett@cantab.net