Caught in a cyber crisis?

Get ready to catch your digital fire hose.

In the heat of the crisis

orange™ Cyberdefense

Jan De Bondt
Director Audit & Business Consultancy

Steven De munter
Business Consultant Cyber Security

Role of each team lead. What is key in the middle of the crisis.

How to deal with the top management "nervosity"

Strategy of mitigation

How to create a cyber crisis cell, how to rebuild IT infrastructure, how to build a good recovery plan

What minimum tools should we have? What to do in case of an incident?

What is the ultimate solution to prevent all attacks? :)

How can you anticipate a crisis? How can you determine which scenarios are most likely for your organization?

How to manage cyber crisis management if the teams you are working with are in remote locations?

Which steps should a ransomware crisis plan contain?

I'd like to hear their approach to the cyber crisis and which actions they've taken to prevent this from happening again

As we currently have a relatively good level of technical security, I would be more inclined to hear about training, awareness campaigns and other more social aspects of Cybersecurity. As for a cyber crisis per say, I think knowing more about fall back solutions would be most interesting.

Do you have any advice on secure platforms that could be used in IT crisis situations, that allow for storage of essential documents, and that offer a way to communicate internally, when our normal IT systems are not available?
- Do tabletop crisis management exercises make sense? If yes, do you have some tips on how to set them up?

Where do I start - is it useful to have a disaster time frame table?

How to start when attacked...

What to do when our data is hijacked

how to quickly detect them, can we have managed help in resolving the hack, what about protection on AI threats

How to use AI to our advantage in cyber crisis management.

What size should a practical crisis management plan have as you can't prepare for every scenario.

On what basis will an incident be classified as a risk? On what basis are mitigating measures chosen?

Cyber Insurance - useful, necessary or best covered by internal and external sourcing?
- What is the best option to recover from a ransomware? Extra segregated data center? Segregated cloud solution?

How to handle hackers who are asking ransom to decrypt data? Follow-up cyber incident after a first resolution.

How to detect all the 'entrances' of the hacker and be sure you can start solving

How do you do tabletop exercise - how do you keep a rather complex incident response plan in the minds of every engineers even if they are not specifically assigned a security role - how do you appoint a second incident commander that might not have the right IT mindset

Is Cyber crisis management to be approached in the same way for both IT and OT environments?

How does everything tie into a full digital transformation

How to deal with a ransomware attack

For entities recently hit by crisis (ransomware or other): do you see that typically incidents are related to a known weakness/risk (possibly too complicated to mitigate on a short term) or was the root cause something entirely different and up until the crisis unknown to the organization? Alternatively, the root cause may not be known, even after investigation. If so, how do you tackle the uncertainty?

Provide a step-by-step plan to show how the risk management priorities are reflected in the plan to secure the highest risks in a crisis.

How do I convince my management to free up budget for trainings and assessment on information security? One of them will join the event!

How are the other companies dealing with cyber security incidents (crisis)?
Also in the context of NIS - NIS2 ...

How to be well prepared to recover from a Cyber Attack

How to define a practical action plan based on priority, risks and situation?

How do I prevent and deal with a cyber crisis in a holistic and value creating way.

Shared experiences. "I wish I knew"

How to use AI to our advantage in cyber crisis management.

What is the relation between OCD CSIRT and CCB. Because when you are an essential

What strategy is used to re-integrate cleaned equipment after a breach?

How to organize a disaster recovery "test scenario" with different department on an efficient way (like fire drill is done)

How to keep calm during the crisis

How to minimize downtime during a cyber crisis management. What's the average downtime for the last big cyber crises?

How to keep the technical experts busy as much as possible while keeping open communication lines towards the business (and beyond, like the board, press)

Managing the crisis IT vs/with business. Plan of action, responsibility, and communication.

do you have templates / checklists that help us to be better prepared for a security crisis?

How to involve your entire organization in a "cybersecurity-diet", so thay all coworkers are on the same level?

How can the maritime infrastructure be protected optimally with the upcoming use of IOT-devices in an increasing landscape of cyber-threats.

Do you have a general drill down scheme/ scenario to follow for a successful recovery ?

How to define a cyber crisis management framework that is in line with NIS Directive?

For those who experienced a cyber crisis, which control/mitigation was crucial and was not identified in upfront?

Which assessment methodology to use to identify if a breach should be reported to the authorities (or not).

Who is involved in the Cyber Crisis Management Team. and who does what.

Trends in cyber defense
What is a good cyber resilience/business continuity plan.

Since a "cyber crisis" has a potentially severe impact on business, should cyber crisis management not be an integral part of your business continuity strategy? How would this reflect in your business continuity plans?

The power of Cyber Crisis Management

3 keys to success

Prioritize

Rebuild

Communicate

The power of Cyber Crisis Management

3 keys to success

Prioritize

- Incident severity assessment
- Identify critical assessment
- Resource allocation
- Legal and regulatory considerations

The power of Cyber Crisis Management

3 keys to success

Rebuild

- Containment
- Eradication
- Recovery
- Security enhancement
- Incident documentation

The power of Cyber Crisis Management

3 keys to success

Communicate

- External communication
- Media and public relations
- Post-incident review

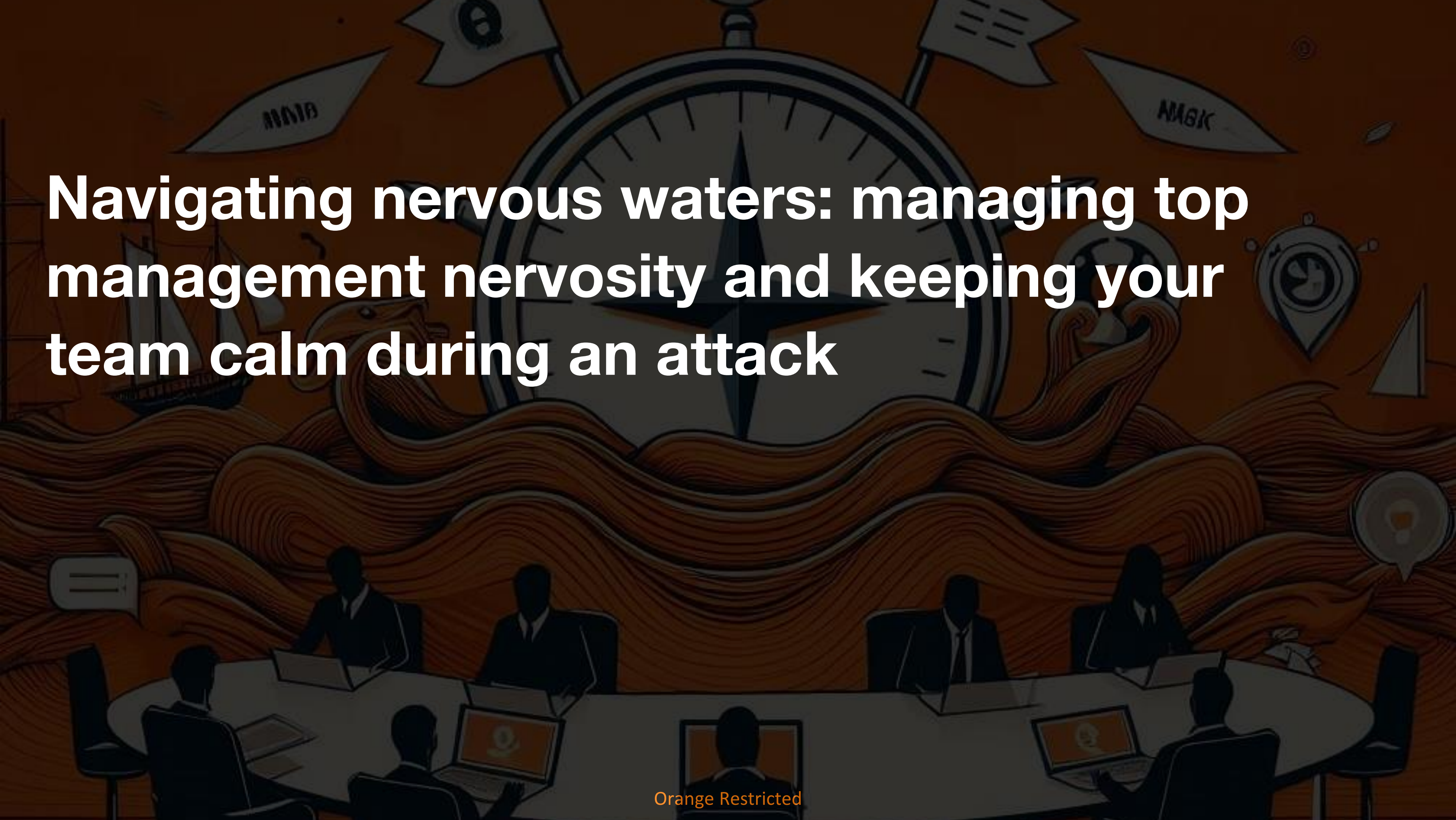
The power of Cyber Crisis Management

3 keys to success

Prioritize

Rebuild

Communicate



Navigating nervous waters: managing top management nervosity and keeping your team calm during an attack

Part 1: How to deal with top management nervosity

- Open and honest communication
- Provide data-driven insights
- Be flexible and adaptive
- Celebrate success/learn from fails

Part 2: How to keep your team calm

- Preparation is key
- Transparent communication
- Appoint crisis leaders – provide support
- Learn from the experience

Fighting fire from different fronts – remote teams

Fighting fire from different fronts – remote teams

- Remote team preparation
- Clear communication
- Continuous improvement

Fighting fire from different fronts – remote teams

Q&A and selfie time

Steven De munter
Business Consultant Cyber Security

Jan De Bondt
Director Audit & Business Consultancy