BUSINESS CONTINUITY MANAGEMENT

CISO-29: Tabletop excercise

11 september 2019

HUISHOUDELIJKE MEDEDELINGEN

Uw Telefoon Op Stil

Uw badge aan het eind inleveren

Registratie bij binnenkomst en na afloop (voor o.a. (C)PE punten)

Volgende reguliere bijeenkomst: dinsdag 24 september 2019 18:00 – 22:00 uur:
Security Eco-Systemen: Best of breed security v.s. ECO Security oplossingen
(m.a.w. losse deeloplossingen versus security suites)

Volgende CISO bijeenkomst: donderdag 31 oktober 2019 16:00 tot 18:30 uur:
CISO-30: Security Architecture - Is dit echt nodig?

PROGRAMMA

16.15 – 16.20	INTRODUCTIE EN WELKOM DOOR ANDRÉ BEERTEN
16.20 – 16.50	INTRODUCTIE IN CYBER CRISIS MANAGEMENT: - CYBER CRISIS MANAGEMENT TECHNIEKEN - CYBER CRISIS MANAGEMENT PROCEDURES - CYBER CRISIS MANAGEMENT ORGANISATIE
16.50 – 17.20	OEFENING 1: TONEELCOMMISSIE
17.20 – 17.55	KOFFIE/THEE PAUZE
17.55 – 18.20	OEFENING 2: CYBER CRISIS
18.20 – 18.45	EVALUATIE

CRISISMANAGEMENT??

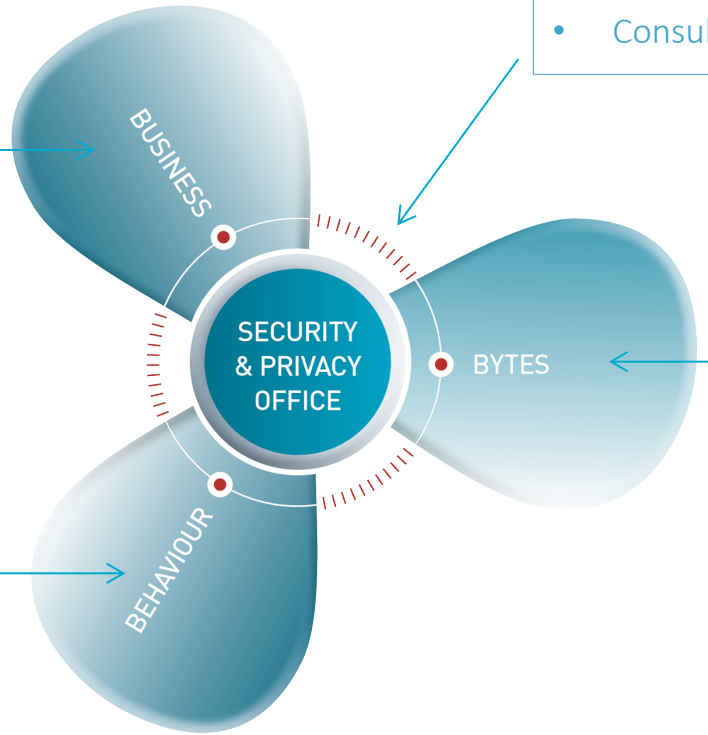
UW BEGELEIDER VANDAAG:

Marcel Paschedag

NORTHWAVE: BUSINESS, BYTES, BEHAVIOUR

- Security & Privacy Office as a Service.
- Assessments & Audits
- Consultancy

- Plans & Procedures
- Cyber Resilience
- GDPR implementation
- ISO27001 implementation



- SIEM/SOC Services
- Red Teaming
- Penetration testing
- CERT services & Forensics

- Awareness programs
- Training
- Exercises

OBJECTIVES

1. INTRODUCTION TO CYBER CRISIS MANAGEMENT THEORY & TECHNIQUES
2. CREATE UNDERSTANDING OF A CRISIS MANAGEMENT ORGANISATION AND STRUCTURE
3. CHANCE TO EXPERIMENT IN A CYBER CRISIS MANAGEMENT CONTEXT
4. IMPROVE RESPONSE THROUGH LEARNING ABILITY → MAKING ‘MISTAKES’ = GOOD ☺


WHY BOTHER WITH CRISIS MANAGEMENT?

WHY ARE WE HERE?

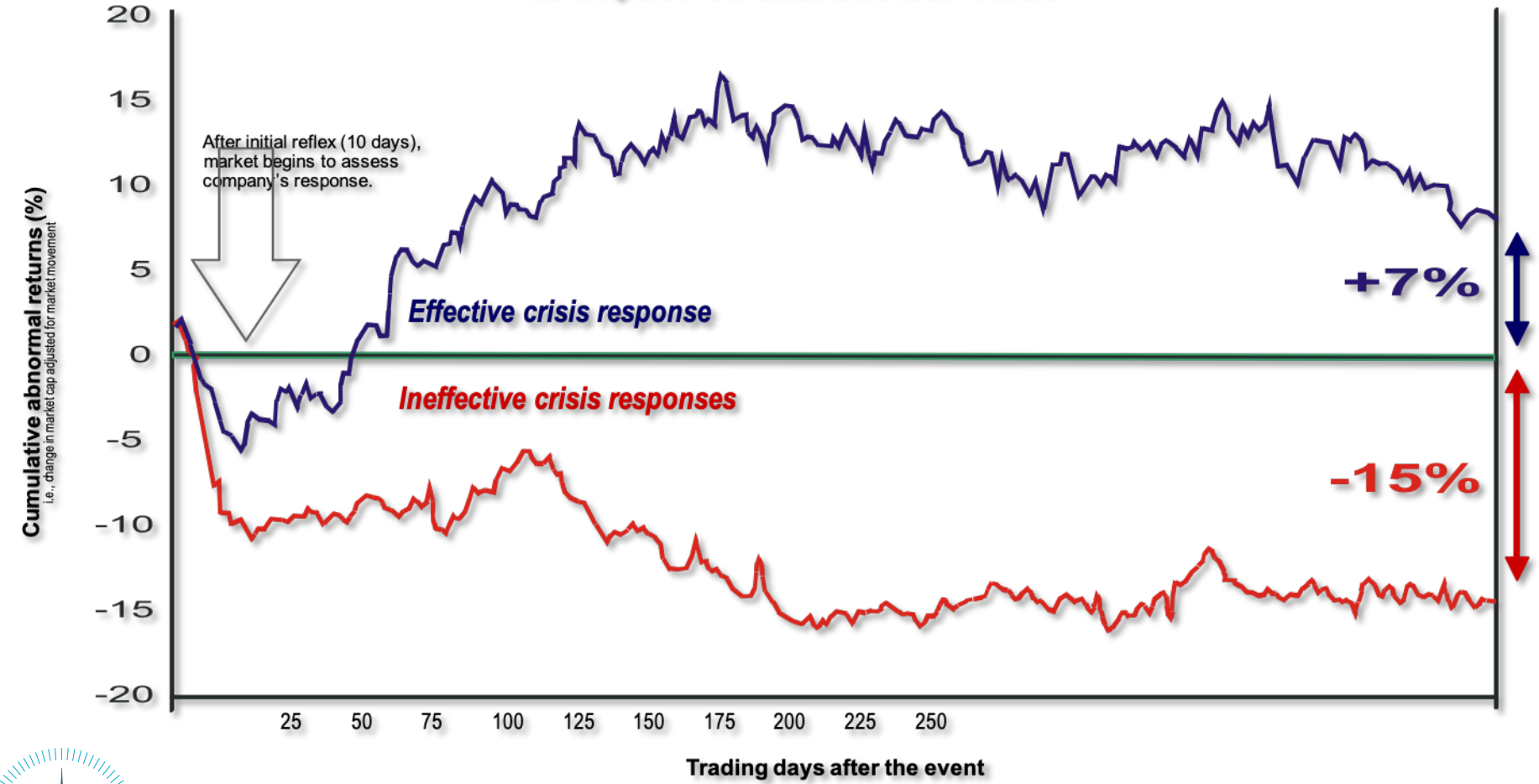
“When anyone asks me how I can best describe my experience of nearly forty years at sea, I merely say uneventful……I never saw a wreck and have never been wrecked, nor was I ever in a predicament that threatened to end in disaster of any sort”.

E.J. Smith, 1907

On 14 April 1912, the RMS Titanic sank with the loss of 1,500 lives.

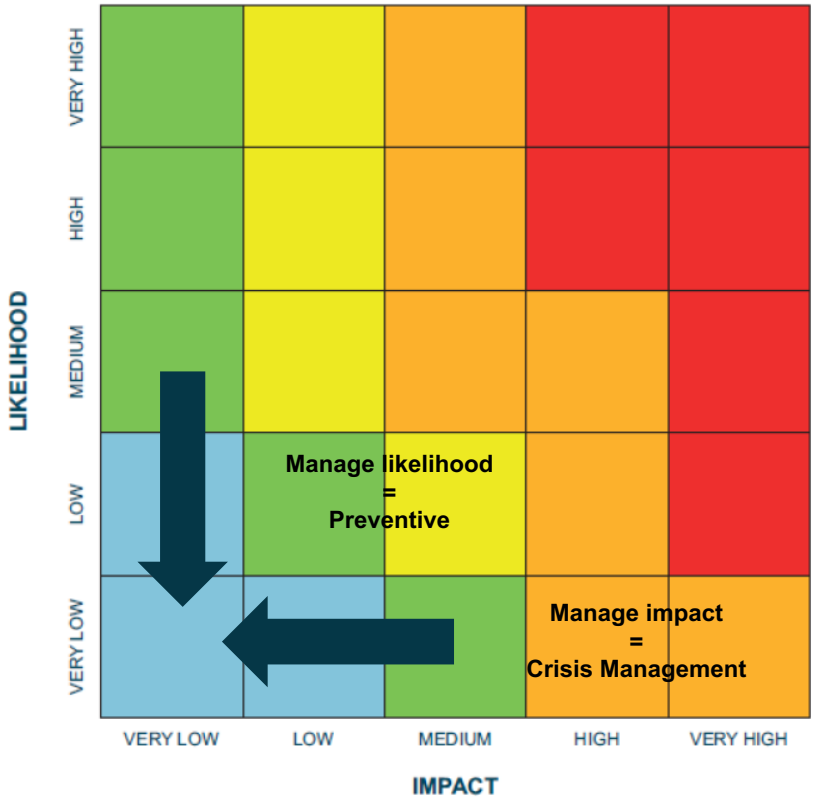
(One of which was its Master, Captain E.J. Smith)

The impact on shareholder value



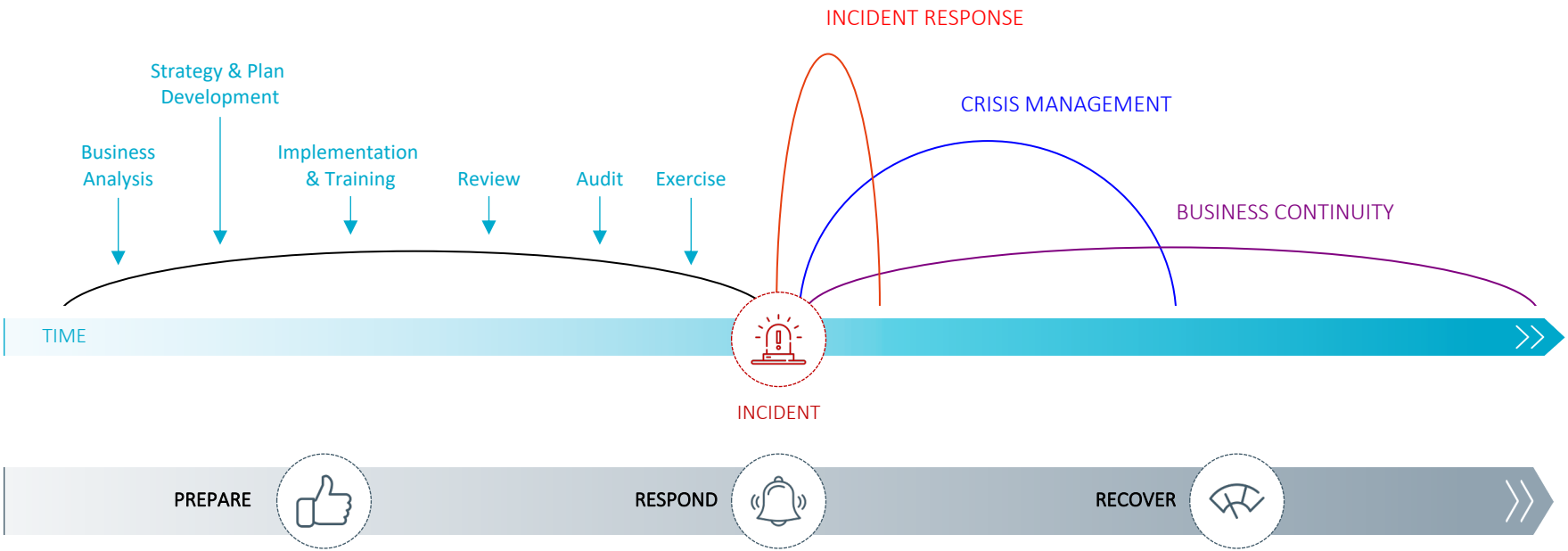
Source: "The Impact of Catastrophes on Shareholder Value," Rory F. Knight & Deborah J. Pretty, Templeton College, University of Oxford, p. 3.

WIDER CONTEXT – RISK MANAGEMENT



CYBER RESILIENCE

When Murphy strikes….



A CRITICAL DIFFERENCE

INCIDENT OR CRISIS

WHAT IS AN INCIDENT? – DEFINITION

An information security incident is a **violation of security policy, user policy or a breach of IT security standards**. Such an incident (potentially) **harms the security** of resources or an information source and has a **negative impact (on business)** in one or more of the following areas:

- *Confidentiality*
- *Integrity*
- *Availability*

Usually can be solved in a regular proces, placed in the normal organisation, under normal managementcontrol

WHAT IS A CRISIS? – DEFINITION

An inherently **abnormal**, **unstable** and **complex** situation that represents a **threat** to the **strategic objectives**, **reputation** or **existence** of an organisation, requiring intense **coordination** and **communication** with internal and external (sometimes unexpected) **stakeholders**

WHAT IS A CRISIS?

Key characteristics:

- Threat to the organisation
- Element of surprise
- Short decision time
- Rapidly changing environment

- Not the strongest or fittest survive.....

=> but the ones most capable of adapting

HOW DIFFERS AN INCIDENT FROM A CRISIS: WHAT TO PROTECT?

PEA

PEOPLE ENVIRONMENT ASSETS

PEARS

REPUTATION STAKEHOLDERS

A LOT TO DO…

- Manage the decisionmaking process
- Manage behaviour
- Manage internal and external communication
- Manage content or subject matter
- Manage (personal) resources
- And so on

Reputation on the line…


External stakeholders get involved…

ANOTHER CRITICAL DIFFERENCE

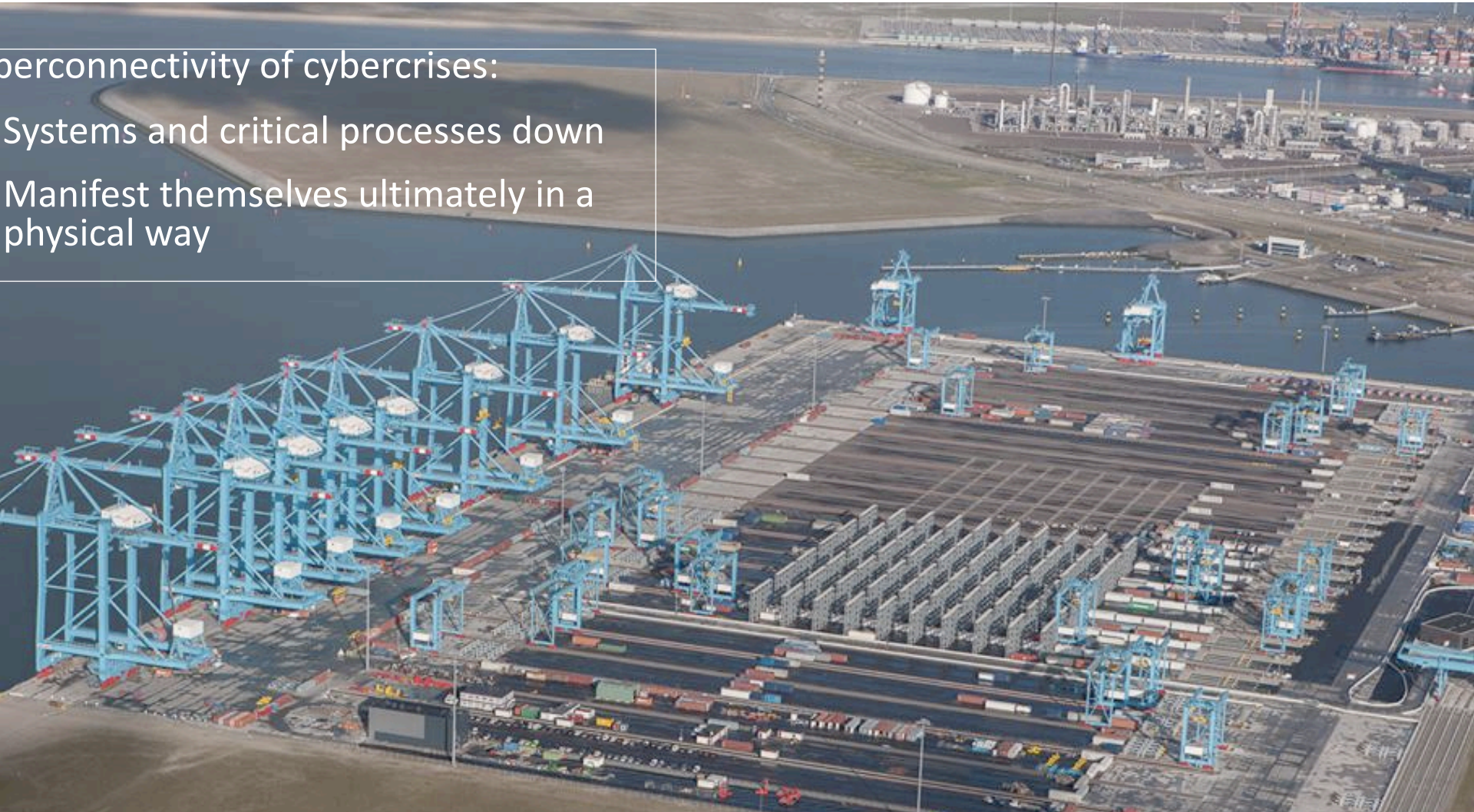
JUST CRISIS OR CYBERCRISIS

DIFFERENT TYPES OF CRISIS

Focus on source of the incident

CRISIS CHARACTERISTICS

Element	Description
Unexpected	Is outside the regular (incident) process
Confusion	Incomplete and/or conflicting information, while decision-making is necessary, without knowing all the facts
Uncertainty	Major risks and the outcome of a crisis is impossible to predict
Speed	Incidents follow each other rapidly, are unpredictable
Stress	Time pressure and impact of decisions
Control	Difficult to recover once you lost the initiative
Media	Big chance of publicity
Stakeholders	Communication is a challenge


berconnectivity of cybercrises:
Systems and critical processes down
Manifest themselves ultimately in a physical way

HOW DOES A **CYBER** CRISIS DIFFER?

Element	Description
Speed	A cyber crisis manifests itself even faster than a regular crisis
Hyper connectivity	Through hyper connectivity, a cyber crisis can have consequences for all vital processes
Crisis organizations	The crisis organizations themselves may also severely affected in their functioning
Source determination	Determining the source and attribution are difficult
Unknown vulnerability (‘zero-day’)	In the digital domain, a crisis may occur because use is made of a up to that moment unknown vulnerability

CRISIS MANAGEMENT PITFALLS

1. **Tendency to manage the incident, not the crisis**
2. Plans out-of-date, unknown or unread
3. Multiple changes to decisions, conflicting decisions and instructions
4. Duplication of efforts
5. Inadequate or absent leadership / Limited decision-making capability
6. Difficulty in establishing and managing communications effectively
7. **Lack of engaging stakeholders**
8. Personality clashes or a failure to listen
9. **Group Think**
10. Lack of resources
11. Externally visible chaos and panic
12. Fatique – nourishment, rest

CRISIS MANAGEMENT BEST PRACTICES

1. Assess information
2. Make decisions
3. Take actions and communicate
4. Isolate problem from day-to-day business
5. Tiered response
6. Global consistency
7. Escalate according to predefined criteria
8. Clear roles and responsibilities
9. Manage stakeholders
10. Be honest, reasonable, and above all, humane

This can only be achieved when… PREPARED

CRISIS STRUCTURE

ELEMENTS OF THE CRISIS RESPONSE PROCESS: **RACER**

Report
- Crisis management team becomes aware of situation

Assess
- Is this an incident or crisis?
- What is the impact on the Company?

Convene
- What team manages the issue?
- Where and how does the team meet?

Execute
- Team works through a structured decision making process

Resolve
- When does team assess the crisis is over & review?

ROLES WITHIN A CRISIS MANAGEMENT TEAM

Logkeeper:
Keeps a detailed log
Assists chair with time management
Room fit for purpose?
Supports on structure and directions
Communicates open items

Proces Coordinator:
Monitors crisis control process
Supports chair
Updates team members
Tunes information with other teams

Chairman:
Reports to DMA
Determines objectives
Manages group dynamics
Summarizes and reflects
Makes decisions

Communications:
Responsible for communication strategy
Monitoring (social) media
Press handling

Head of IT / CISO:
Maintenance contact with IT (security) department
Responsible for IT (security) services
Responsible for IT (security) strategy

STRUCTURED CRISIS RESPONSE – OODA LOOP

OBSERVE
Gather information from relevant sources

ORIENT
Analyze gathered information & use it to enrich your knowledge on the current incident

DECIDE
Determine the best course of action

ACT:
Follow through on your decision

NORTHWAVE CRISIS RESPONSE PROTOCOL

Crisis Response Protocol	
Observe	
Room fit for purpose en logbook	Make sure you are in the *right room* and start the *logbook.*
Roles & responsibilities	Confirm respective *roles and responsibilites.*
Raw information	What *information* is *available* about the incident?
Orient	
Facts & assumptions	What do you *know* for sure and what do you *believe* has occured?
Scenarios	Develop *worst case* and most likely scenarios. Determine the *impact*, *issues* and *risks*.
Objective(s)	Define your *desired end state* (e.g. return to business as usual) and set (sub)objectives and limitations.
Decide	
Response Options	Discuss various available and possible options and *choose* the *best option* and an *alternative*.
Act	
Action list and priority: • Action	What *actions* must we complete to achieve the chosen option? What needs to be done *now* and what can *wait*?
• Stakeholders	Identify the range of stakeholders and prioritize according to the *interest* and *influence* they have.
• Key Messages	Establish the *key messages* which must be conveyed to the stakeholders.
Repeat	*Repeat* this protocol (in principle every hour). Decide when and where the *next meeting* is.
NORTHWAVE	

[EXERCISE] This e-mail is part of an incident exercise organized by Northwave [EXERCISE]
From: Support Desk<Supportdesk@RSM.com>
Date: 21-05-2019 10:40
Subject: [Exercise] New information
All,

We have been in close contact with our IT-department regarding the suspicious mails. They've investigated the incident in the past 30-minutes and are able to give you more information regarding the phishing mails.

- At this moment, at least 15 employees have clicked on the email and filled in their credentials
- By obtaining the credentials, the attacker was able to log in to our system and might have had access to our documents and data
- It seems that the obtained credentials are used to log in on the mail server of the employee and send the malicious mail to all of his/her contacts. As a result of this, the mail is now sent to some of our clients and partners as well
- We advise you to reset the credentials of the employees that have clicked on the mail.

We keep investigating the incident and will update you if more information is available.

Kind regards,
John van der Maarel, Manager Support Desk (IT-department)

[EXERCISE] This e-mail is part of an incident exercise organized by Northwave [EXERCISE]

[EXERCISE] This e-mail is part of an incident exercise organized by Northwave [EXERCISE]
From: hackerforjustice@live.com
Date: 21-05-2019 10:20
Subject: [Exercise] Hurry up
Hi there,

It has been a while. But here I am again and my patience is over..
I will give you one more chance to pay me or this time your data will end up in the media.
At the moment, I have obtained credentials of your employees and very interesting data regarding your firm.
If the payment is not received within a few minutes, I will publish all the data on Pastebin and inform some media sources for you guys as well. This will have a huge impact for Rose, Stewart & McLaren, I can assure you.

Good luck!

Kind regards,
The Hacker For Justice

[EXERCISE] This e-mail is part of an incident exercise organized by Northwave [EXERCISE]

PASTEBIN + new paste API tools faq deals search... Guest User

Rose, Stewart & McLaren data breach

A GUEST 2019 245 NEVER

SHARE TWEET

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 0.02 KB raw download clone embed report print

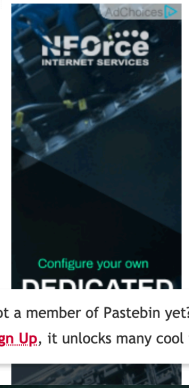
```
1. xD gaige urgaypwned
```

RAW Paste Data

```
Link for the Data: https://pastebin.com/data/Rose, Stewart & McLaren/7y43hndf8e3bd/breach/data/niewnvew
```


Public Pastes

- Untitled — 6 sec ago
- Untitled — Kotlin | 6 sec ago
- Untitled — 11 sec ago
- Untitled — 13 sec ago
- Untitled — 15 sec ago
- cec-ctl -S — 21 sec ago
- Untitled — 22 sec ago
- Untitled — 22 sec ago



HELLO Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

SUMMARY

- PREPARE
- COMPREHENSIVE APPROACH
- MANDATE
- STRATEGY
- CENTRAL DECISION MAKING
- RESILIENCE
- RECOVERY