NAVIGATE
RESPONSE
A WITT O'BRIEN'S COMPANY

Cyber Concerns in the Maritime Industry

navigateresponse.com

ASTARA
COMPANY LIMITED

Cyber Security
- what are the real issues?

William Egerton
Chief Cyber Officer

#ResilienceandRecovery

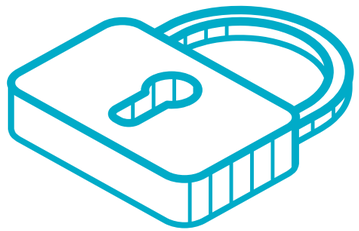
Bill Egerton, Chief Cyber Officer

- FCO – UNISYS-PWC
- OLIVE – DS&S – GD – AEGIS
- INDEPENDENT CYBER ADVISORY
- THE STANDARD SYNDICATE 1884
- LINGUIST, NOT TECHNICAL

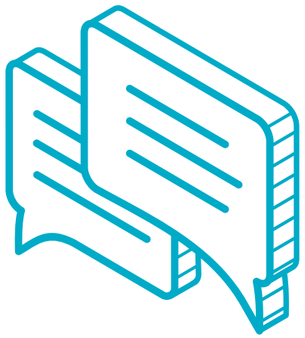
Why me, here, today?

- EMERGING THREATS? THEY ARE ALREADY HERE.
- WHAT DOES MATCH FIT LOOK LIKE

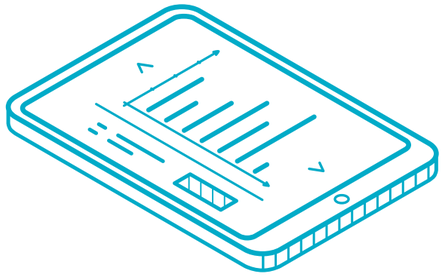
ASTARA
COMPANY LIMITED



Insurance



Advisory



Analytics

3 CYBER ATTACK ON MARITIME ENTERPRISES ARE INCREASINGLY COMMON – BUT THE CYBER ATTACKERS DON'T CARE WHO...

Common factors

The cyber threat is agnostic as to industry sector

↓

All are spending more on security as a result

↓

It is not a case of if, but when

#ResilienceandRecovery

4 INCREASING CYBER THREATS IN THE MARITIME SECTOR

Ransomware = no1 cyber insurance claim

» 41% ransomware
» 27% fund transfer
» 19% business email compromise
  » Source Coalition H1 2020 report (US Cyber Insurer)

OFAC

» Warning: are you funding terrorism?

EU/UK/US

» Do you understand cyber regulatory framework
» Potential impact on ticket to trade (IMO and ship's certification and ticket to trade)

Digitisation

Automation / autonomous shipping

5 WHY ARE WE SEEING THE INCREASING INCIDENTS?

- Lack of leadership commitment
- Lack of investment, or investment in the wrong things
- Unmanaged customers & your supply chain

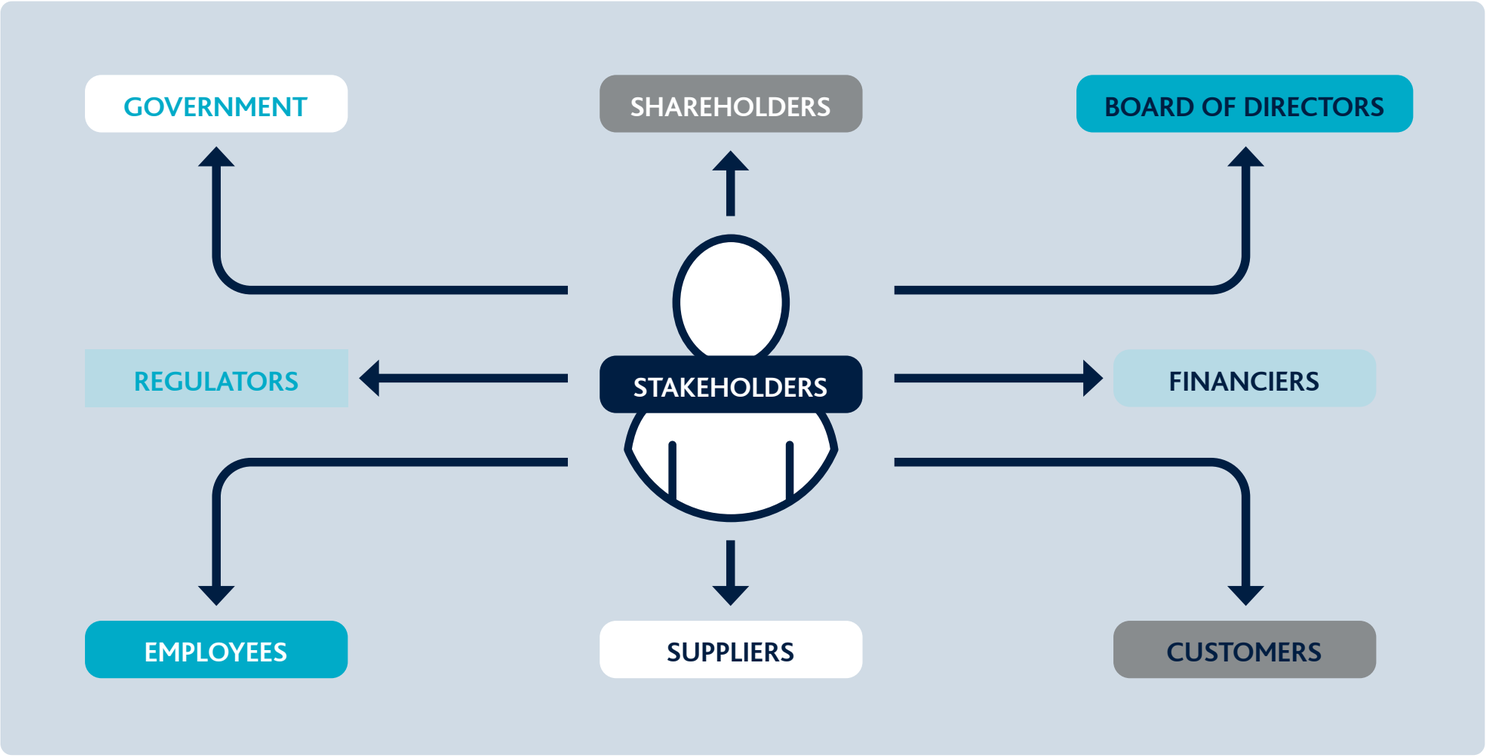
The attack vector is a demonstration of the sector's failure to deal with the issues of which they are already aware

6 THE WHY IS IMPORTANT BECAUSE WE KNOW THE ATTACK VECTORS

- Ransomware – unpatched software
- Money diversion – process fail
- Rapid unplanned network propagation – segregation
- IPR theft – poor security or vetting
- Network fail – complex and robust access control
- Supplier fail – they fail, you take the hit

What is the corporate rationale that puts us in a place where some or all of the above exist simultaneously? We know the cure…

7 WE ALSO KNOW WHERE THE LOSSES ARE FELT..... BUT IT IS NOT INEVITABLE IF YOU INVEST IN CYBER



#ResilienceandRecovery

8 SO, WHAT DOES MATCH FITNESS LOOK LIKE?

» **Be aware** – risks, vulnerabilities, poor behaviours

» **Be responsible** – CEO down

» **Be trained** – policies, guidance, procedures and plans

» **Be human** – think how your users work

» **Be ready** – all the time

» **Be unforgiving** – breaches and poor behaviour are NOT excusable

» **Be empirical** – do not rely on luck or sentiment – make sure you get the data you need

» **Be humble** - there is no monopoly of knowledge

9 THESE ARE THE CHARACTERISTICS OF GOOD.....

- Realise you are vulnerable and that you might have been lucky so far
- Understand that you have to manage the risk dynamically
- Recognise you need to invest
- Be aware that your people are key to your success – and failure
- Senior management is publicly committed to the issue
- Be ready to move at pace to fix the issue
- Make people responsible. But give them the tools to do the job

10 WHY DO INCIDENTS CONTINUE TO INCREASE IN FREQUENCY / SEVERITY….?

Because we let them

» If we did ‘cyber’ properly, 90% of breaches **WOULD NOT HAPPEN**

It is not just IT

It is manageable

Do the basic hygiene well and start from there

#ResilienceandRecovery

NAVIGATE
RESPONSE
A WITT O'BRIEN'S COMPANY

Cyber Concerns in the Maritime Industry

navigateresponse.com

DATA PROTECTION ADRIFT

GDPR IN A NUTSHELL

COVERS EU DATA SUBJECT PERSONAL DATA - *ANY INFORMATION* THAT ALLOWS FOR IDENTIFICATION "DIRECTLY OR INDIRECTLY"

- **Examples:** name, ID number, location data, IP Address, health information, etc.
- Not just sensitive information -- much broader than US privacy standards

APPLIES TO CONTROLLERS AND PROCESSORS OF DATA

- Need not be an EU/EEA ship/company - if it targets EU individuals (employees, customers), the GDPR applies

Examples of data processing:

- Processing crew data for HR/Finance/legal compliance (e.g., Maritime Labor Convention)
- **CCTV** / Voyage Data Recording of crew on ships
- Intra-company data sharing / third-party sharing with port agents, P&I clubs, authorities

GDPR IN A NUTSHELL

SEVEN BASIC PRINCIPLES

- Must be lawful, fair & transparent
- Limited in purpose
- Data Minimization
- Accurate
- Storage Limitation
- Integrity & Confidentiality
- Accountable

WHAT'S A LAWFUL BASIS?

* Consent*
* Performance of a contract
* Legal obligation
* Legitimate interest of the controller

PENALTIES AND FINES FOR NON-COMPLIANCE

- Penalties can be as high as 4% of worldwide turnover
- Regulators have already targeted the transportation industry

IMPORTANT CONSIDERATIONS

EMPLOYEE & SUPPLIER DATA

DATA BREACH

THIRD PARTY RISK

DATA TRANSFERS

FINES IN THE INDUSTRY

- **ENTIRELY SHIPPING & TRADING S.R.L. (DEC 2019)**

  Fined 10,000 EUR by Romanian DPA

  Multiple violations, including lack of lawful basis for processing CCTV and biometric data of employees

- **AEGEAN MARINE PETROLEUM NETWORK INC. (DEC 2019)**

  Fined 150,000 EUR by Hellenic DPA

  Insufficient Technical & Organizational Controls

- **ALLSEAS MARINE S.A. (JAN 2020)**

  Fined 15,000 EUR by Hellenic DPA

  Illegal installation and operation of CCTV. The company also violated principles around transparency & accountability.

HAS YOUR FIRM SUFFERED A DATA BREACH?

DID YOU REPORT IT?

1. WE'VE BEEN LUCKY (NO BREACH)
2. YES, BUT WE DIDN'T REPORT
3. YES, AND WE NOTIFIED OUR REGULATOR
4. I CAN NEITHER CONFIRM OR DENY (OR DON'T KNOW)


Healthcare
$7.1M
Energy
$6.4M
Financial
$5.9M
Pharmaceutical
$5.1M
Technology
$5.0M
Industrial
$5.0M
Services
$4.2M
misc.Entertainment
$4.1M
Education
$3.9M
Transportation
$3.6M
Communication
$3.0M
Consumer
$2.6M
Retail
$2.0M
Hospitality
$1.7M
Media
$1.7M
Research
$1.5M
Public
$1.1M
$0
$2,000,000
$4,000,000
$6,000,000
$8,000,000
$10,000,00
AVERAGE DATA BREACH COSTS BY INDUSTRY
IBM SECURITY, COST OF A DATA BREACH REPORT

knowligence

CAREY@KNOWLIGENCE.INFO

+353 085 104 6645

TWITTER: @PRIVACAT

HTTPS://KNOWLIGENCE.INFO

NAVIGATE
RESPONSE
A WITT O'BRIEN'S COMPANY

Cyber Concerns in the Maritime Industry

navigateresponse.com

Crisis comms for a cyber event

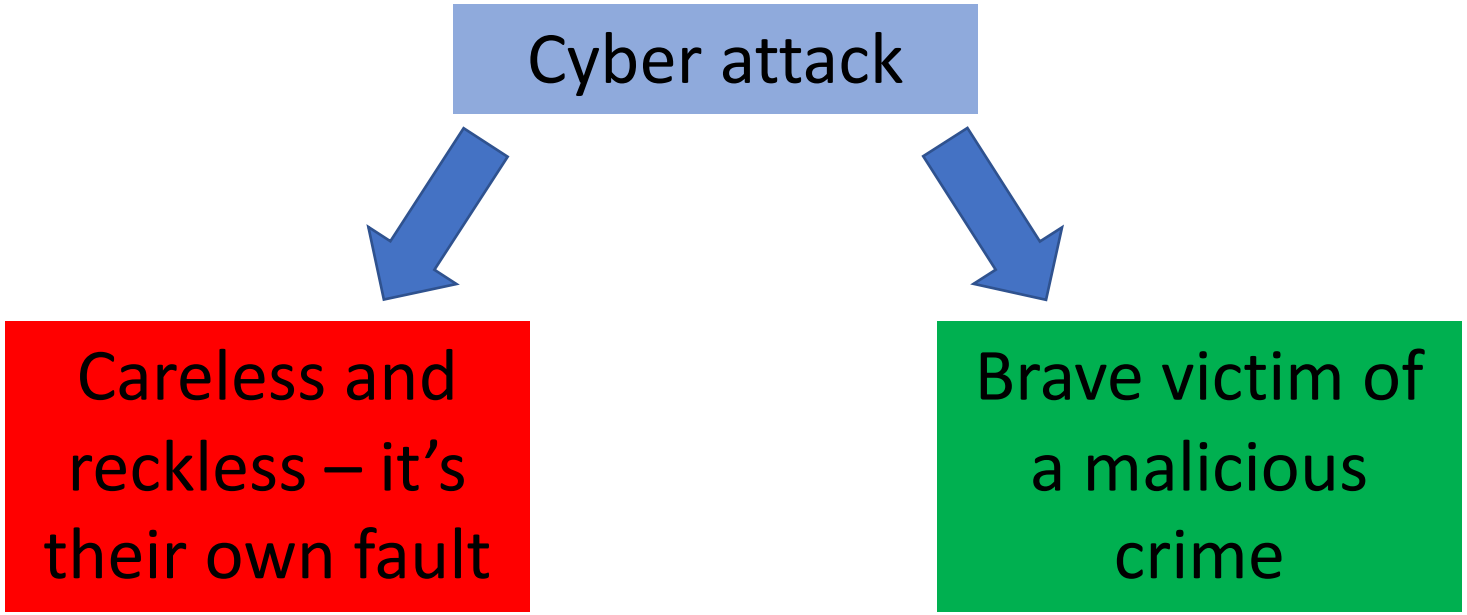
navigateresponse.com

NAVIGATE
RESPONSE
A WITT O'BRIEN'S COMPANY

October 2020

PERCEIVED AS BOTH PREVENTABLE & UNAVOIDABLE

Which frame will people view your company through?



NAVIGATE RESPONSE

THE RECENT ATTACK ON THE IMO

"The interruption of web-based services was caused by a sophisticated cyber-attack against the Organization's IT systems that overcame robust security measures in place."

https://imo-newsroom.prgloo.com/news/imo-web-services-update-02102020

NAVIGATE
RESPONSE

THE RECENT ATTACK ON CMA CGM

CMA CGM cites 'internal IT infrastructure issue' as sites go down

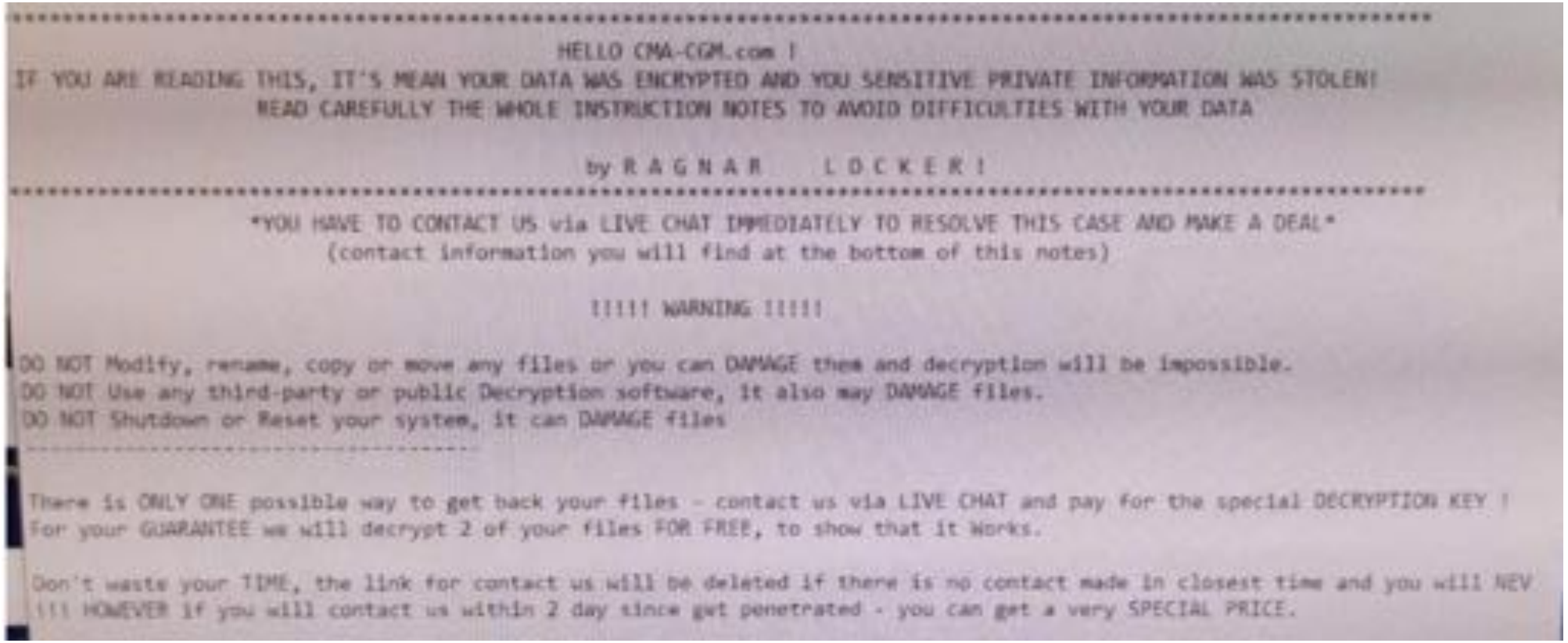
Sam Chambers · September 28, 2020 · 1 · 2,605 · Less than a minute

After initially claiming the company's booking system was disabled by 'an internal IT infrastructure issue', CMA CGM has now confirmed it was hit with a ransomware attack.

28 September 2020
https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack

NAVIGATE
RESPONSE

DETAILS WILL LEAK OUT…



HELLO CMA-CGM.com !
IF YOU ARE READING THIS, IT'S MEAN YOUR DATA WAS ENCRYPTED AND YOU SENSITIVE PRIVATE INFORMATION WAS STOLEN!
READ CAREFULLY THE WHOLE INSTRUCTION NOTES TO AVOID DIFFICULTIES WITH YOUR DATA

by R A G N A R L O C K E R !

YOU HAVE TO CONTACT US via LIVE CHAT IMMEDIATELY TO RESOLVE THIS CASE AND MAKE A DEAL
(contact information you will find at the bottom of this notes)

!!!!! WARNING !!!!!

DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.
DO NOT Use any third-party or public Decryption software, it also may DAMAGE files.
DO NOT Shutdown or Reset your system, it can DAMAGE files

There is ONLY ONE possible way to get back your files - contact us via LIVE CHAT and pay for the special DECRYPTION KEY !
For your GUARANTEE we will decrypt 2 of your files FOR FREE, to show that it Works.

Don't waste your TIME, the link for contact us will be deleted if there is no contact made in closest time and you will NEV
!!! HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.

"Staff in Europe have been told not to use any company IT equipment, according to sources."

28 September 2020 https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack

NAVIGATE
RESPONSE

A MAJOR CASE WILL FOLLOW YOU FOR YEARS

"The Ragnar Locker attack would make CMA CGM the fourth major container shipping carrier known to have fallen victim to such a major cyber incident.

"In July 2018, Chinese giant Cosco Shipping was hit by a cyber attack that disabled its IT systems in the US.

"Maersk Line sustained a severe blow from a ransomware attack in 2017, which cost the Danish carrier up to $300m.

"Mediterranean Shipping Co suffered a shutdown from a cyber attack earlier this year."

28 September 2020
https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack

NAVIGATE
RESPONSE

Will any of this work?

DIGITAL COMMS RESPONSE

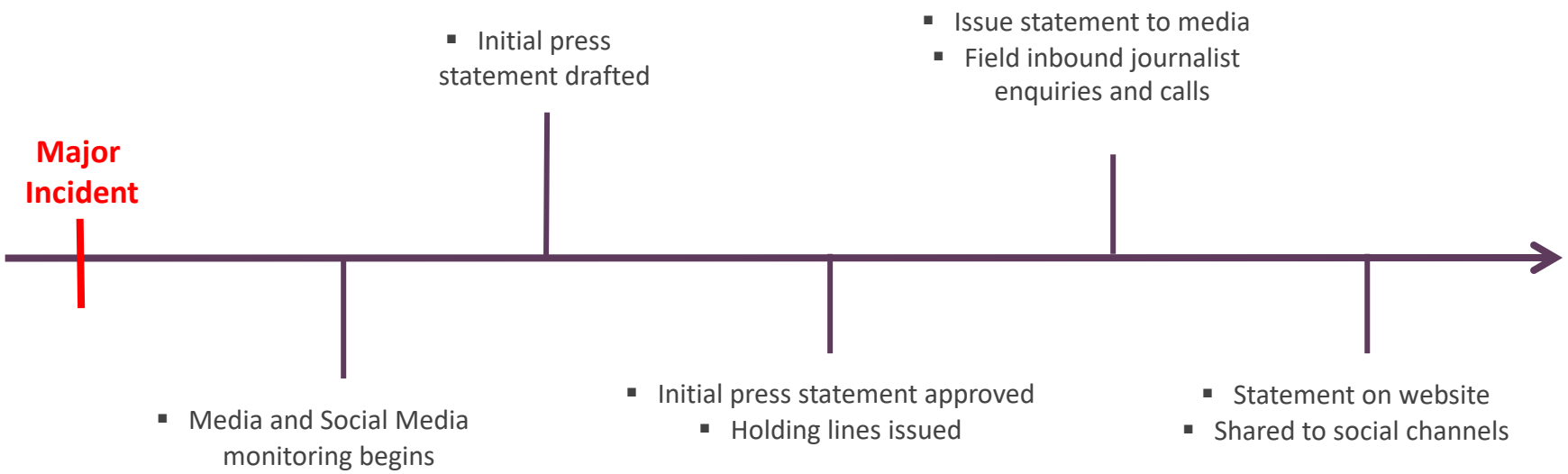
- Website – your single source of verifiable information
- Social media accounts – connect with your stakeholders
- Customer queries and email traffic – don't lose sight of the small stuff, or it will become big

NAVIGATE RESPONSE

How can you do this?

CRISIS COMMS INITIAL ACTIONS CHECKLIST

The first three hours



NAVIGATE RESPONSE

ALTERNATIVE CHANNELS

- Work with the media – friendly journalists
- Use social media (new channels if necessary)
- Candid works well – record a message on anything that's still working

NAVIGATE
RESPONSE

USE THEM FREQUENTLY

- Be predictable
- Repeat yourself until you have something new
- ALWAYS show empathy

NAVIGATE
RESPONSE

EMPATHY

- Who might feel impacted?
- Express regret
- Present solutions, but manage expectations
- Show your face – literally

NAVIGATE
RESPONSE

CMA CGM'S UPDATES

Update 10/02/2020 -- The CMA CGM Group continues to be fully mobilized to restore access to all its information systems. Our worldwide agency network is gradually being reconnected.
Mercosul and Containerships, two of the Group's subsidiaries, are once again fully operational.

We would like to thank all our customers for their trust and understanding.

Update 09/30/2020 -- The CMA CGM Group continues to be fully mobilized to restore all its information systems.
Today, the back-offices (Shared Services Centers) are gradually being reconnected to the network thus improving the bookings' and documentation's processing times.
We suspect a data breach and are doing everything possible to assess its potential volume and nature.
Our technical teams, alongside independent experts, are continuing the investigation.

Updates will be provided regularly as the situation evolves.

Update 09/29/2020 -- The CMA CGM group, hit by a cyberattack, has interrupted all internal access to its network and computer application in order to isolate the malware and take protective measures .
This malware was able to be rapidly isolated and all necessary protection measures implemented.
All communications to and from the CMA CGM Group are secure, including emails, transmitted files and electronic data interchange (EDI).
Maritime and port activities are fully operational.
The booking functionalities remain up and running.
Alternative solutions to the e-business site are available in order to support business continuity for CMA CGM Group's customers.
All of the Group's teams remain fully mobilized and we will keep you updated on the current situation.

Update 09/28/20 -- The CMA CGM Group (excluding CEVA Logistics) is currently dealing with a cyber-attack impacting peripheral servers.
IMPORTANT NOTICE / UPDATE :
The CMA CGM Group (excluding CEVA Logistics) is currently dealing with a cyber-attack impacting peripheral servers.
As soon as the security breach was detected, external access to applications was interrupted to prevent the malware from spreading.
Our teams are fully mobilized and access to our information systems is gradually resuming.
The CMA CGM network remains available to the Group's customers for all booking and operation requests.
An investigation is underway, conducted by our internal experts and by independent experts.

A new communication will be issued at the end of the day.

IMPORTANT NOTICE - 09/28/2020 - Update : 9:00 am
External access to CMA CGM IT applications are currently unavailable.
IT teams are working on resolving the incident to ensure business continuity.
For all bookings, please contact your local agency.

We will keep you posted regularly on the current situation.

https://www.cmacgm-group.com/en/news-media/global-it-update-09-29-2020

NAVIGATE
RESPONSE

HOW IT'S BEING RECEIVED

IS THIS COVERAGE FAIR?

"With updates in short supply and clients increasingly irritated at the lack of communication on the IT outage, CMA CGM has taken to answering customer questions via direct messages over Twitter in the last 24 hours."

7 October 2020
https://splash247.com/ten-days-on-and-cma-cgm-is-still-struggling-to-get-all-its-systems-back-online/

NAVIGATE
RESPONSE

ESSENTIALS TO SUCCESS

- Define the narrative and then keep control of it
- Show empathy – this isn't just impacting you
- Provide frequent updates
- Manage expectations – under promise and over deliver
- Avoid jargon, but share some details – it makes you look transparent
- Alternate communications channels – don't let perfect be the enemy of good enough

NAVIGATE
RESPONSE

THANK YOU!

October 2020

Dustin Eno dustin.eno@navigateresponse.com

NAVIGATE
RESPONSE

Questions and Answers

navigateresponse.com