KEKST CNC

Effective crisis response during a cyber breach

11 February 2020

Today's Agenda

01	Introductions
02	What is a crisis?
03	What is cybercrime and how is it different?
04	How can organisations best prepare for an incident?
05	What are the options for communications during an incident? What is proportionate?
06	Reputational recovery post a cyber incident

Introductions

Ben Curson
Partner, London/Middle East

Valentina von Lutterotti
Senior Consultant, Dubai

Who we are at-a-glance…

A leading global strategic communications firm

300

Highly experienced professionals

13

Offices globally: Europe. North America. Asia.

600

Clients across the world

PUBLICIS GROUPE

Part of Publicis Groupe, the world's third-largest communications group

…and who are you?

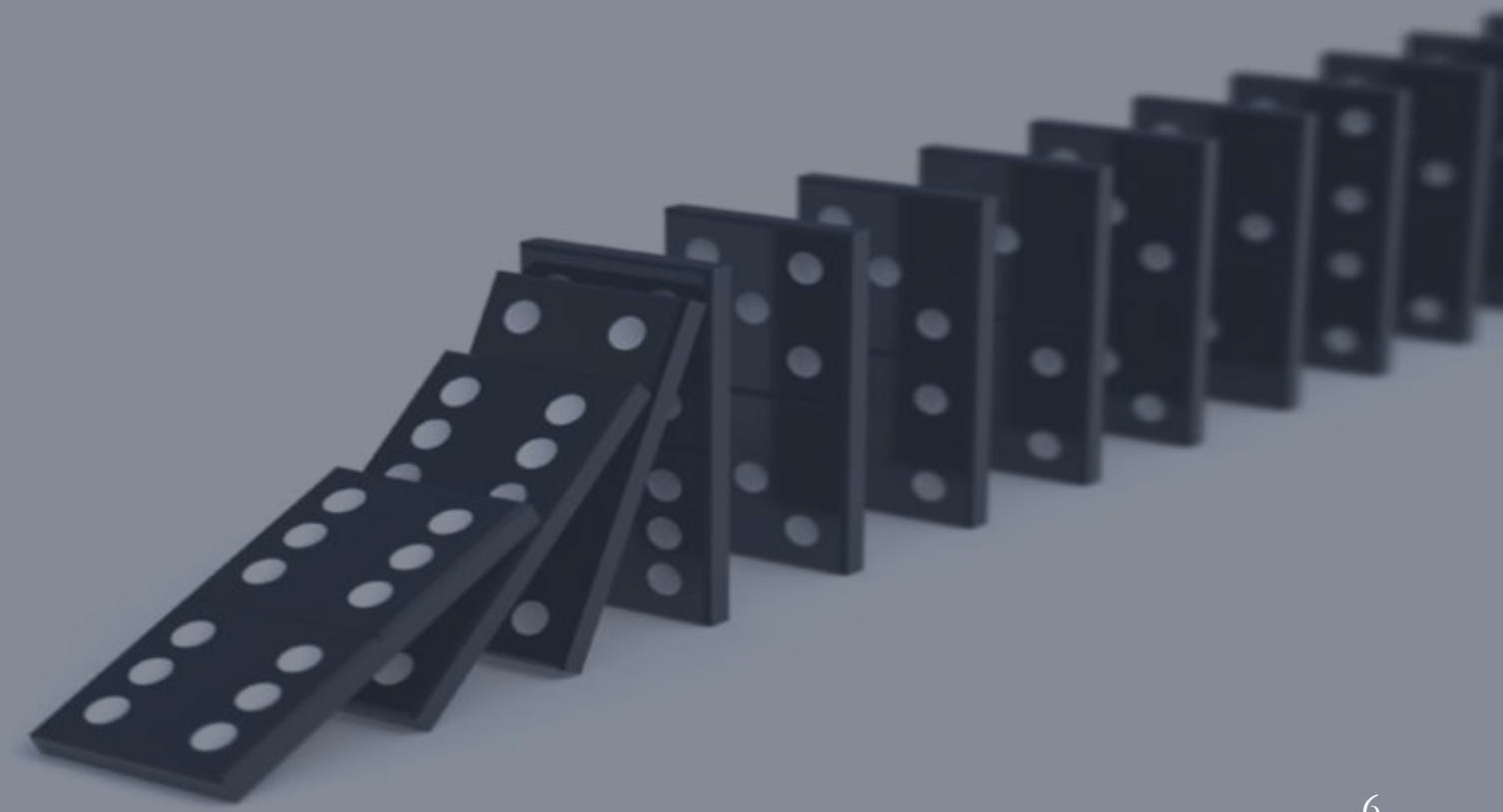
02

What is a Crisis?

It takes 20 years to build a reputation and 5 minutes to ruin it.

If you think about that, you'll do things differently.

Warren Buffett



A crisis is…

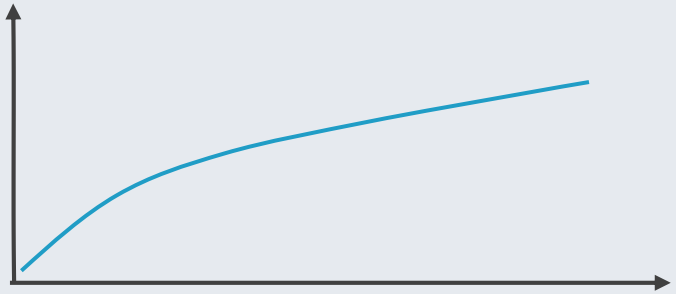
A crisis is an unforeseen event or issue that has escalated into a situation that threatens the strategic values in an organization…

…with the potential to inflict severe damage.

Types of crisis

The three types of crisis

1 The chronic crisis



FIFA corruption crisis

2 The sudden crisis

Nestlé Maggi Noodles lead scare

3 The evolving crisis

Volkswagen "Dieselgate" emissions testing

The new normal

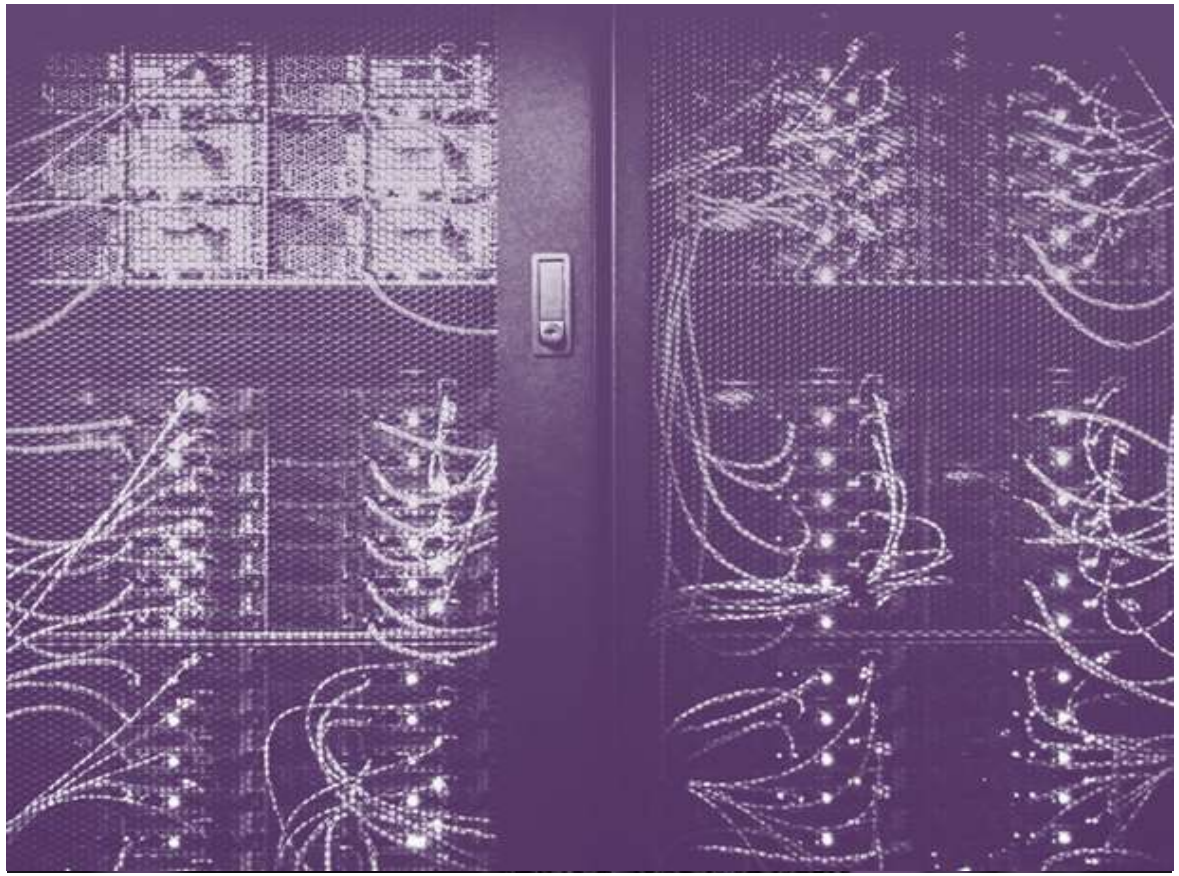
Speed	Mars chocolate recall	Within **24 hours** the news reached more than **34.4 million unique users** online.
Reach	Volkswagen “diesel-gate”	Tweeted about by influencers in **multiple languages** including **Indonesian**, **Hindi**, **Persian** & **Tamil**
Citizen journalism	Anyone can make news using a smartphone	**81% increase** in corporate crises hitting traditional media headlines compared to the 2000s

Even before social media, it was said…

A lie gets halfway around the world before the truth has a chance to get its pants on.

Winston Churchill

03



What is Cybercrime?

The Middle East is one of the world's most cyber-attacked regions

The Middle East has the highest average number of breached records with nearly 40,000 breached records per incident.

49% of vulnerabilities arise from management issues of permissions and access control.

50% of all cyber attacks in the Middle East target the oil & gas sector.

It takes companies in the Middle East 381 days on average to identify and contain a breach.

The UAE is one of the region's most-targeted countries. Iranian Government sponsored attacks were reported in 2019 and may increase in 2020 given rising tensions

31% of companies in the UAE and Saudi Arabia don't have a response plan in place to respond to a cyber incident.

The UAE is listed as 6th most targeted country by banking malware attacks. Malware attacks in UAE increased by 12 per cent in the first three months of 2019.

75% of documented intrusion sets appear to be motivated primarily by cyberespionage actions.

Source: IBM & Ponemon Institute 2019; Dark Matter 2019

Did you know?

The average global cost of a cybercrime in 2019 was recorded at $3.92 million, a 1.5 percent increase to the previous year.

The Middle East recorded the second highest average cost of data breaches at $5.97 million.

Consumer cybercrime profiles and behaviour

20% of cybercrime victims use the same password across all online accounts

Cybercrime victims in the UAE spent an average of 47.8hrs dealing with the aftermath of a breach

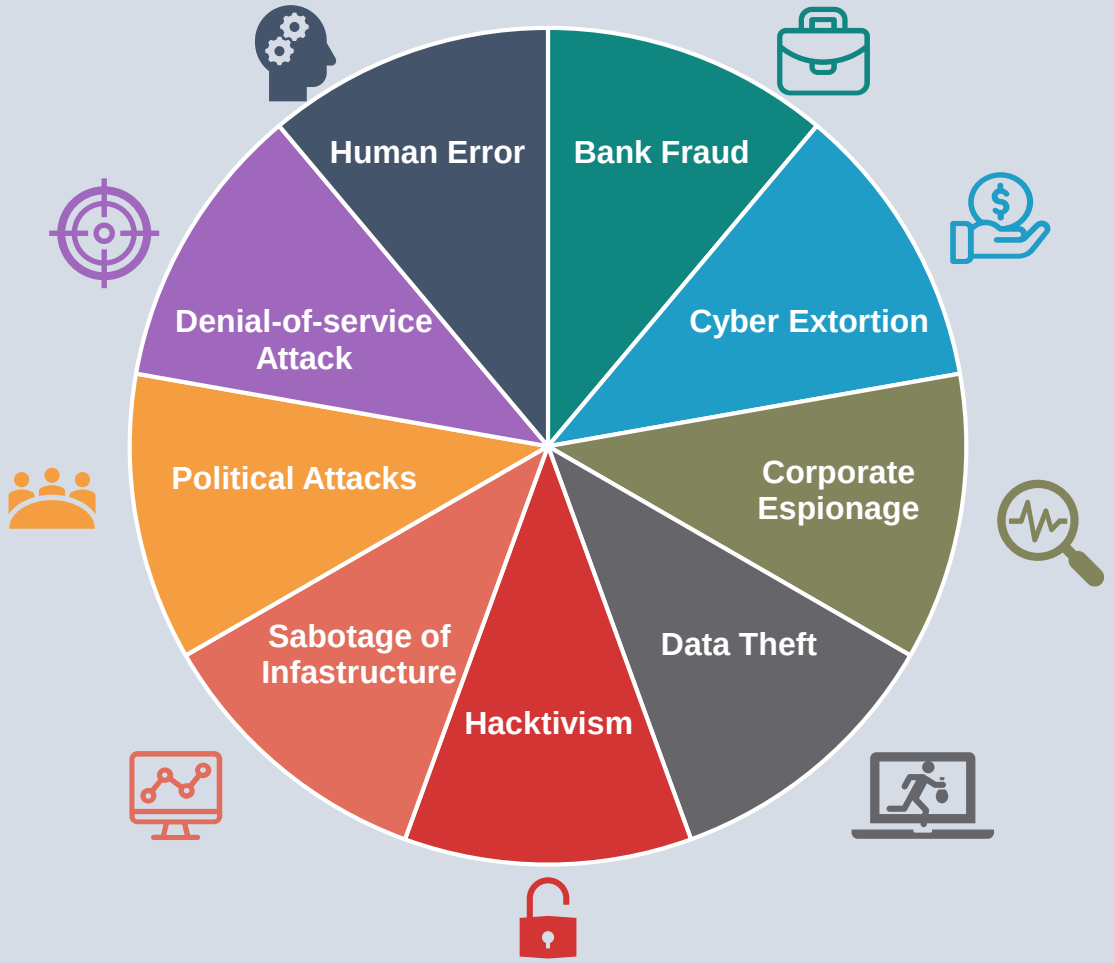
Consumers who own the newest technologies and most devices are most likely to be victims

Consumers trust those that manage their data to protect it and do not accept cybercrime is inevitable

Source: Norton Cyber Insights Report 2017

Sabotage and espionage are key threats for MENA companies

While attacks on retailers, technology firms and banks often dominate the headlines, there are many forms of cybercrime impacting all sectors from finance to infrastructure, healthcare to the public sector.

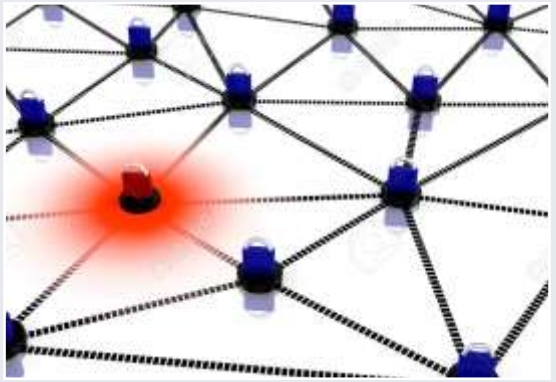


Human error and software glitches account for highest risks for companies in MENA

System glitches and human error account for 49% of cyber breaches

91 % of companies in the MENA region use outdated software, 83 % unsupported software

91% of companies' employees use weak or default passwords



87 % of companies in the MENA region use insecure network protocols

Source: Dark Matter Cyber Security Report 2019

Local Examples

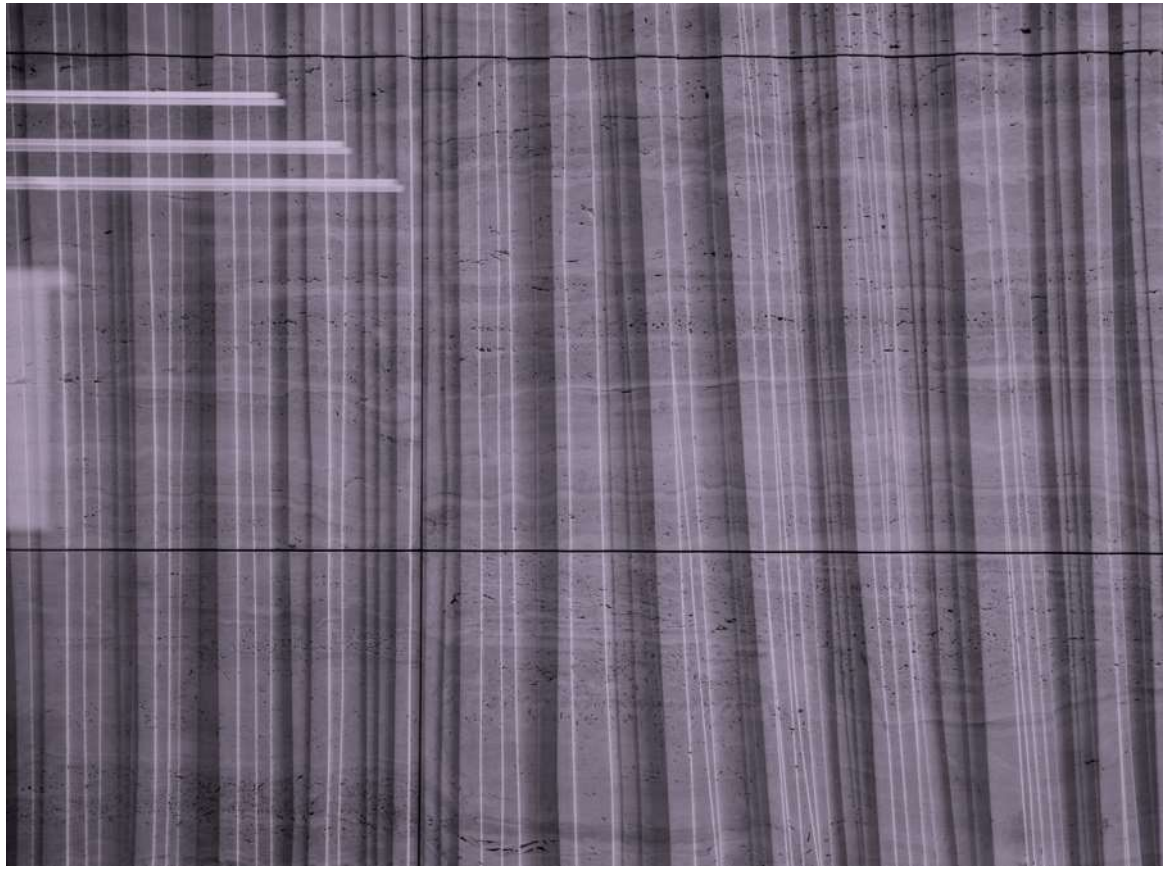
Organizations that have been hit by cyberattacks in the GCC

Why is cyber communications different?

Cyber security communications must be seen as a practice in its own right vis-à-vis crisis communications in general.

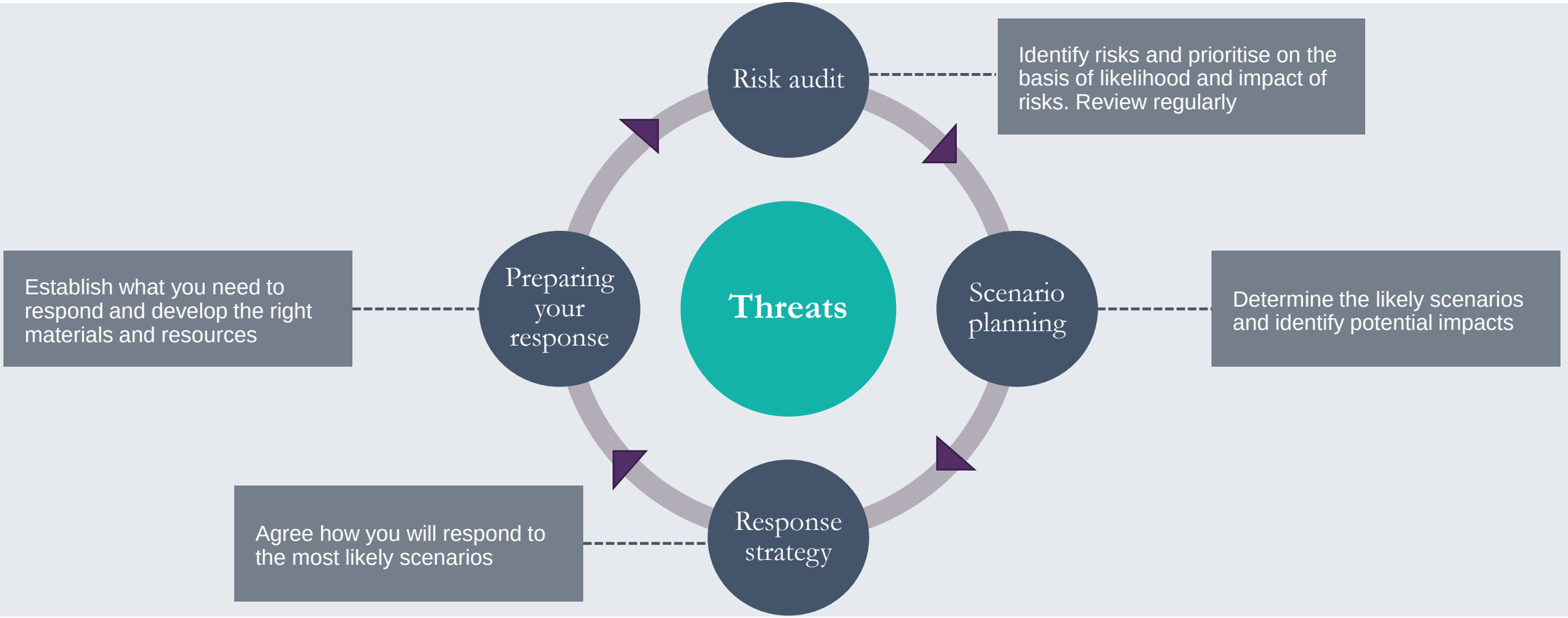
Dynamic	Cyber incidents are dynamic, evolving in nature and it often takes considerable time to determine the scale of an issue and its source; which presents communications challenges as to if/when to make a breach public.
Open-ended risk	Cyber risk is an open-ended risk. As a result communications need to be more versatile, adaptive and flexible; resilience-building will always be imperfect.
Trust & reputation	Cyber crime results in trust and reputational consequences – with client/customer expectations often disproportionate to what can be achieved. These are even harder to predict due to the impact of social media outlets used by customers.
Unknown source	Attacker(s) and their intentions are often unknown (and may remain so) which makes communications strategies difficult to pre-define and subject to change. The rise of state-sponsored attacks adds another challenging geo-political dimension.
More than IT	Cybersecurity is not just an IT issue. Sales, marketing, operations, logistics and many other functions may be involved depending on the nature of the crisis and how it develops. Cross-departmental information sharing must not be siloed.
Media attention	Media attention has dramatically increased and reputational damage has become more likely. Media can be confused by the technical details and misreport, and often encourages organizations to speculate before facts can be confirmed.

04



Preparing for an incident

Risk Audit: Proactively mitigating reputation threats



Risk Audit: Understanding the issues you may face

Objectives

Determine vulnerability to crisis situations and identify potential reputational risks and scenarios that may emerge

Evaluate existing communications processes and protocols for dealing with incidents and benchmark against best practice

Review process

Review existing protocols and incident response plans to identify any gaps

Audit of all potential risks to the business

Audit of owned channels, e.g. website and social media

Outcome

Written report and risk register of potential scenarios, prioritised by likelihood and severity

Recommendations for implementing best practice into the crisis communications process

Assessment of channel readiness and internal resources, and recommendations for training

Crisis Communications Manual: Defining your crisis processes

Objectives

Ensure processes and materials are in place and clarify where and how they will be used

Ensure speed and consistency of response should an incident occur

Identify and prioritise key stakeholders to enable efficient and focused communications in a crisis situation

Review process

Review existing crisis manuals, procedures and continuity plans, and update where necessary

Refine the CMT set-up, roles and responsibilities

Confirm notification and escalation processes

Review ways of working with key stakeholders

Outcome

Create a consistent crisis communications manual, including:

Procedure for managing incidents and priority scenarios

Directory of contacts and emergency database

Key message framework and draft holding statements (internal and external)

Pre-agreed monitoring process

Crisis training: Ensuring your teams are prepared

Objectives	**Ensure your escalation processes** are embedded within your organisation	**Create** a solid global team of crisis communicators	**Ensure** your senior spokespeople can handle media interviews in the event of a crisis
Review process	**Review** existing knowledge of protocols and processes	**Survey** current crisis communication capabilities and identify areas for development	**Identify** your key crisis spokespeople and deputies
Outcome	**Bespoke, global training programme** developed for your communications teams and regularly refreshed	**Crisis simulation** exercise to test knowledge of procedures and best practice	**Crisis media training** for your key spokespeople

Crisis Simulation – The Kekst CNC Situation Room

Testing crisis processes and protocols in practice before they are put into action is key to best-practice preparedness.

The CNC Situation Room immerses participants in a tailored crisis situation using our proprietary digital software and hardware. The client's team is confronted with a wave of developments across online and offline channels, designed to mirror a real-life, real-time crisis. Participants have to respond to a multitude of inputs and use their judgment and comms skills in action with role-play and team-work skills tested.

Your team at the heart of action
Your team will be given dedicated laptops and phones with a bespoke user interface. The online tool also allows your team members in other locations to join the simulation.

Crisis specialists form the back office
CNC plays the role of a range of internal and external stakeholders, from aggressive journalists to disgruntled senior management, adapting the scenario dependent on how the crisis participants respond.

Online articles, social media, videos

Real-time interaction

Live interviews

05

Communicating during a cyberattack

Responding to a cyber breach

The days after a disaster can be a make-or-break time for a company's reputation. What senior executives say and do can worsen the reputational damage caused by the crisis…or mitigate it.

The Economist

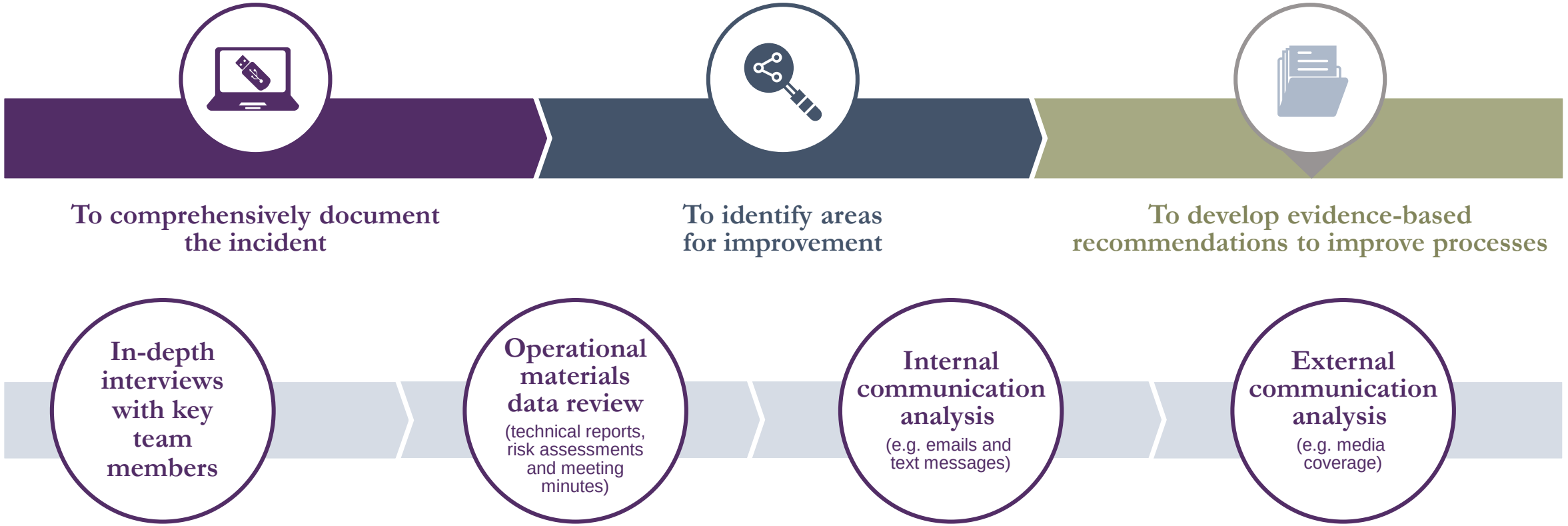
Considerations in reacting to a cyber incident

06

Recovery post incident

After-Action Review kick starts crisis recovery

After-action reviews (AAR) are used to kick start the recovery process following a crisis. The aim of an AAR is primarily to record, learn and recommend.



Reputation Rebuild: Moving on

External communications

- Moving the narrative away from the issue
- News stories
- Digital and owned channels
- SEO

Employer Brand

- Telling the story internally
- Rebuilding confidence
- Retaining talent
- Recruitment

Investor Relations

- Share price and sentiment Analyst relations
- Investor materials and briefings

07

Key Considerations

Questions to consider

Does my leadership team or Board have appreciation for the risks posed by a cyber security incident and are they willing to invest in planning and response testing?

Are my crisis communications protocols “cyber proof” and how do we communicate if our normal channels are impaired or not accessible?

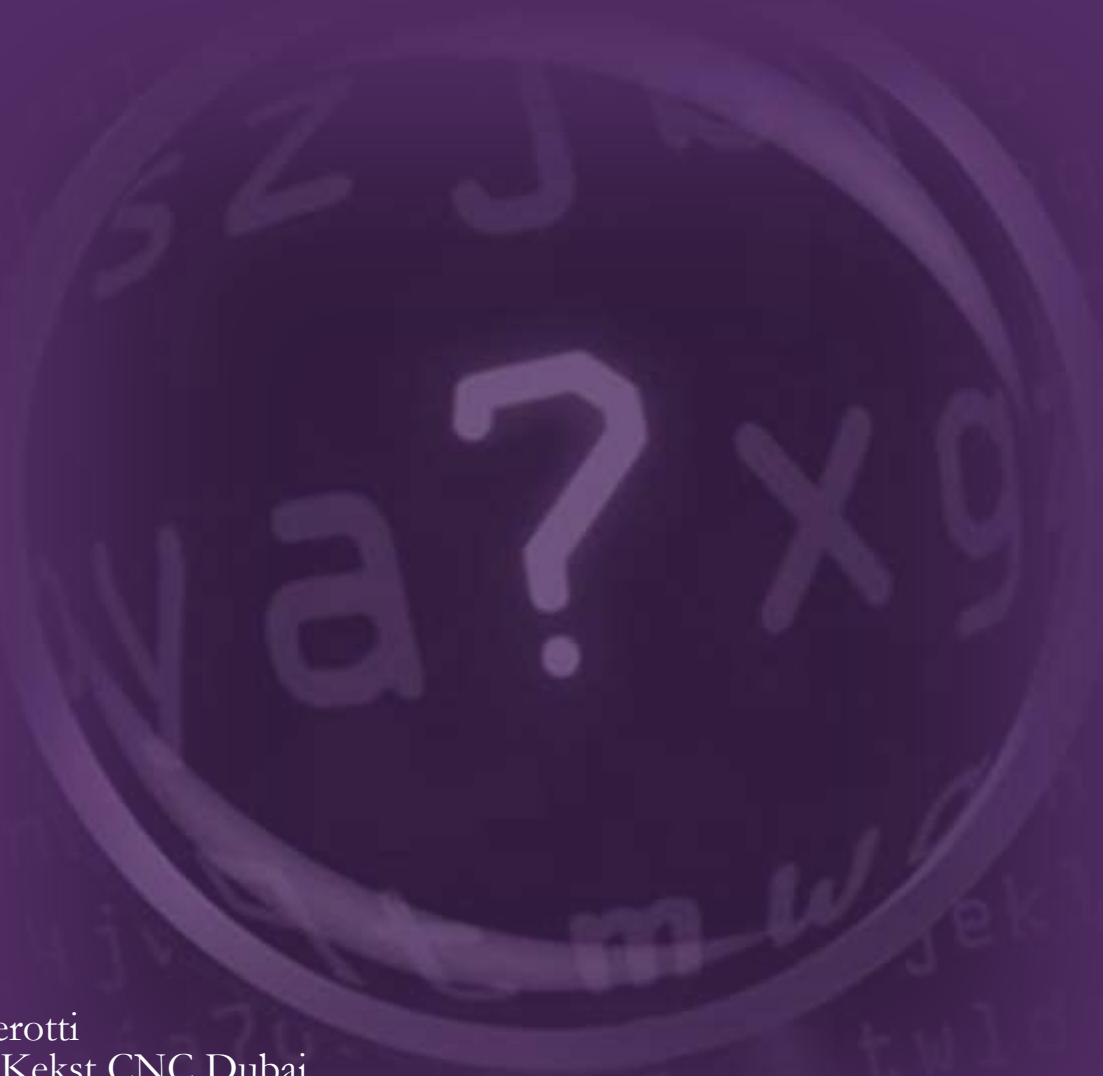
Do we have training and awareness programs in place designed to educate employees and reduce negligence?

Are there clear protocols for responding to a breach involving communications from the beginning, not as an afterthought. Does this include customers, supplier, regulator and employee communications, not just the media. How about social media? Who is responsible for what?

Do I know who the Incident Response team is for a cyber breach? Is it the same for business recovery, or does it involve different functions? When did we last test our responses?

KEKST CNC

Thank you!



Questions?

Ben Curson
Partner, Kekst CNC London
ben.curson@kekstcnc.com
T +44 203 755 1606
M +44 (0)7983 921 720

Valentina von Lutterotti
Senior Consultant, Kekst CNC Dubai
valentina.lutterotti@kekstcnc.com
T +971 4 367 6153
M +971 55 1230208