Building resilience through cyber crisis management

High level guide for senior management

pwc

We live in a world of constant disruptions, keeping our leaders awake at night.

PwC 2022 Global CEO Survey **1**

49% of CEOs are very concerned about **cyber risks**, making them the top threat to growth

PwC 2022 Global Digital Trust Insights Survey **2**

60% of executives expect a **surge in reportable cyber incidents** in 2022 compared to 2021

PwC 2021 Global Crisis Survey **3**

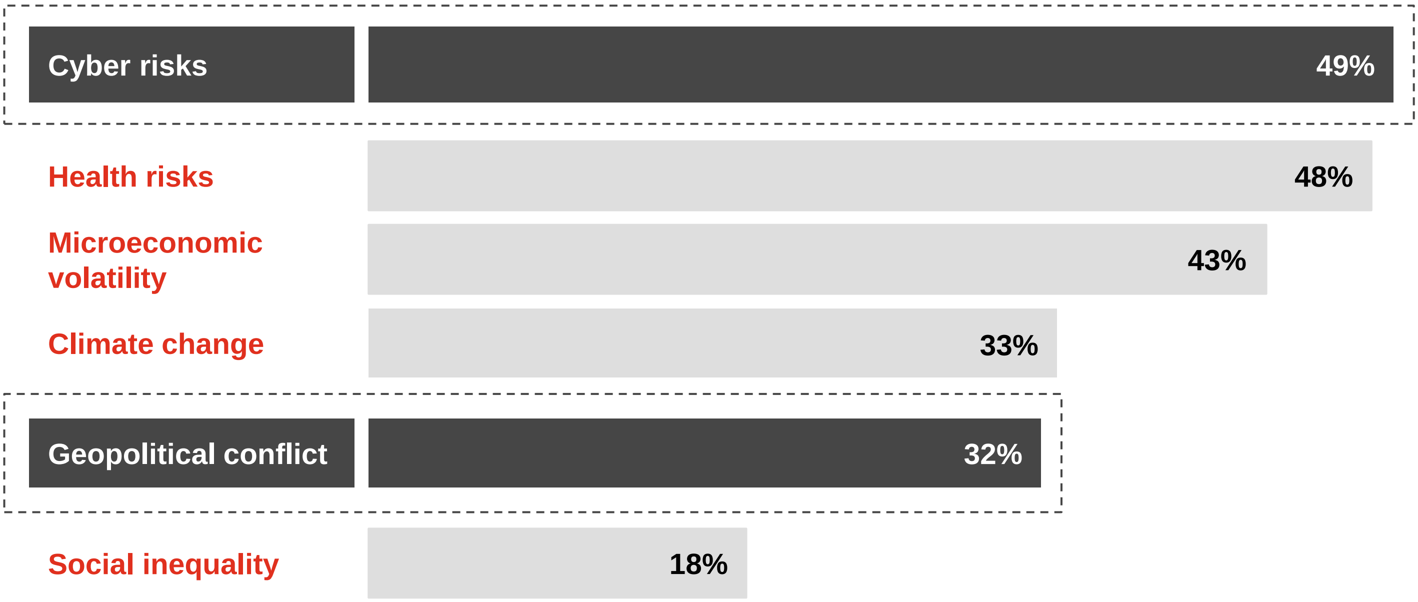
7/10 organisations stated that they are planning to **invest more** in building **resilience** and **breaking down silos** in their core resilience functions

Cybersecurity and geopolitical conflicts.

Separately, they are among the top worries of CEOs, according to PwC's CEO Survey. Together, the combined risks pose an even bigger challenge that demands immediate action.

CEOs and boards should be asking: Are we ready to mitigate escalating cyber risks related to geopolitical tensions that might flare up in 2022 and beyond?

⚠ Elevated risks for business when cyber risks and geopolitical conflicts combine



Questions: How concerned are you about the following global threats negatively impacting your company over the next 12 months? (showing only "very concerned" and "extremely concerned" responses)

Source: PwC, 25th Annual Global CEO Survey, January 2022

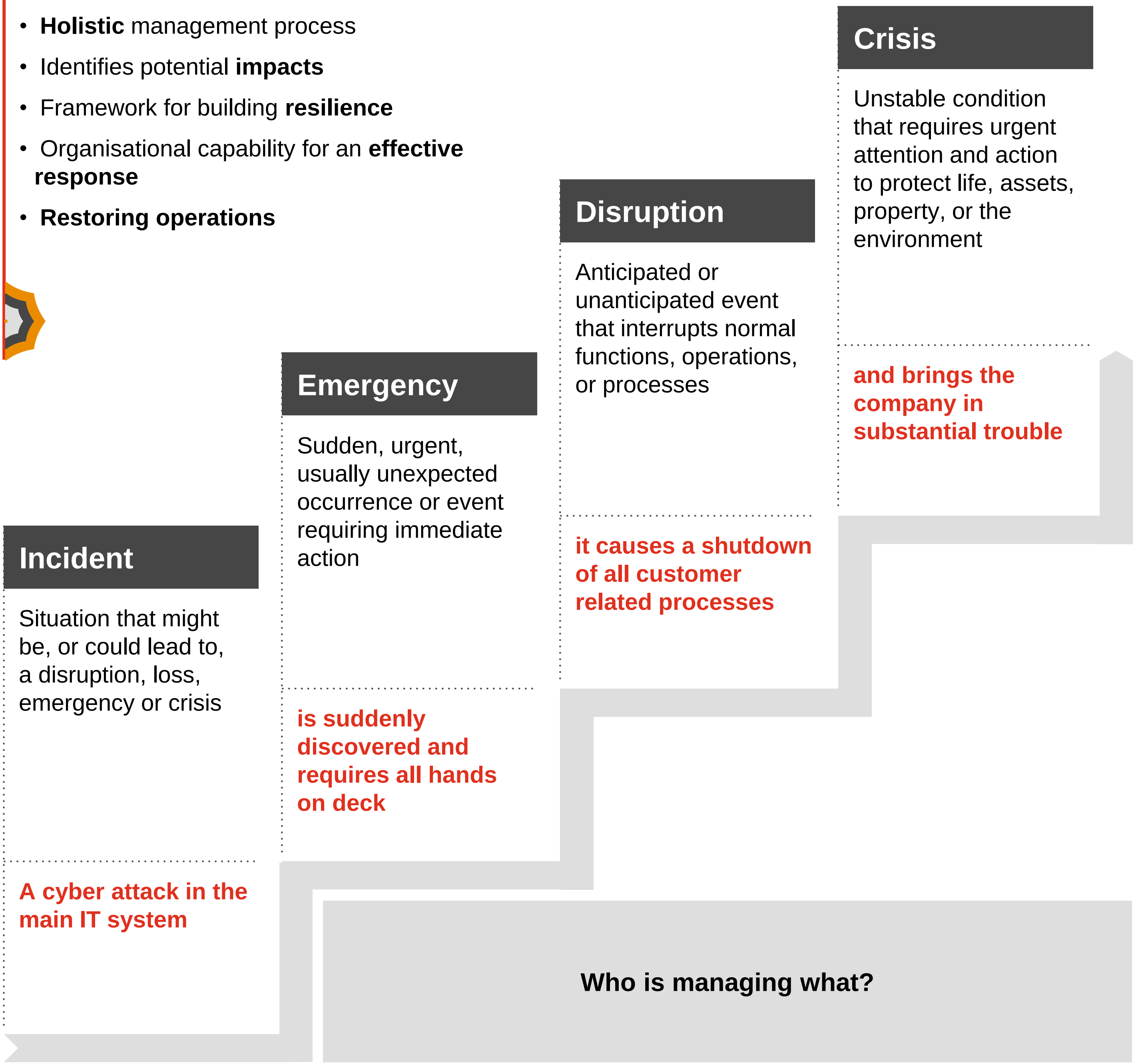
Unpack incident response and crisis management

What is a crisis?*

- Abnormal, unstable situation / abrupt and significant change
- Threatens the organisation
- Requires urgent attention and action

What is crisis management?

- **Holistic** management process
- Identifies potential **impacts**
- Framework for building **resilience**
- Organisational capability for an **effective response**
- **Restoring operations**



Incident

Situation that might be, or could lead to, a disruption, loss, emergency or crisis

A cyber attack in the main IT system

Emergency

Sudden, urgent, usually unexpected occurrence or event requiring immediate action

is suddenly discovered and requires all hands on deck

Disruption

Anticipated or unanticipated event that interrupts normal functions, operations, or processes

it causes a shutdown of all customer related processes

Crisis

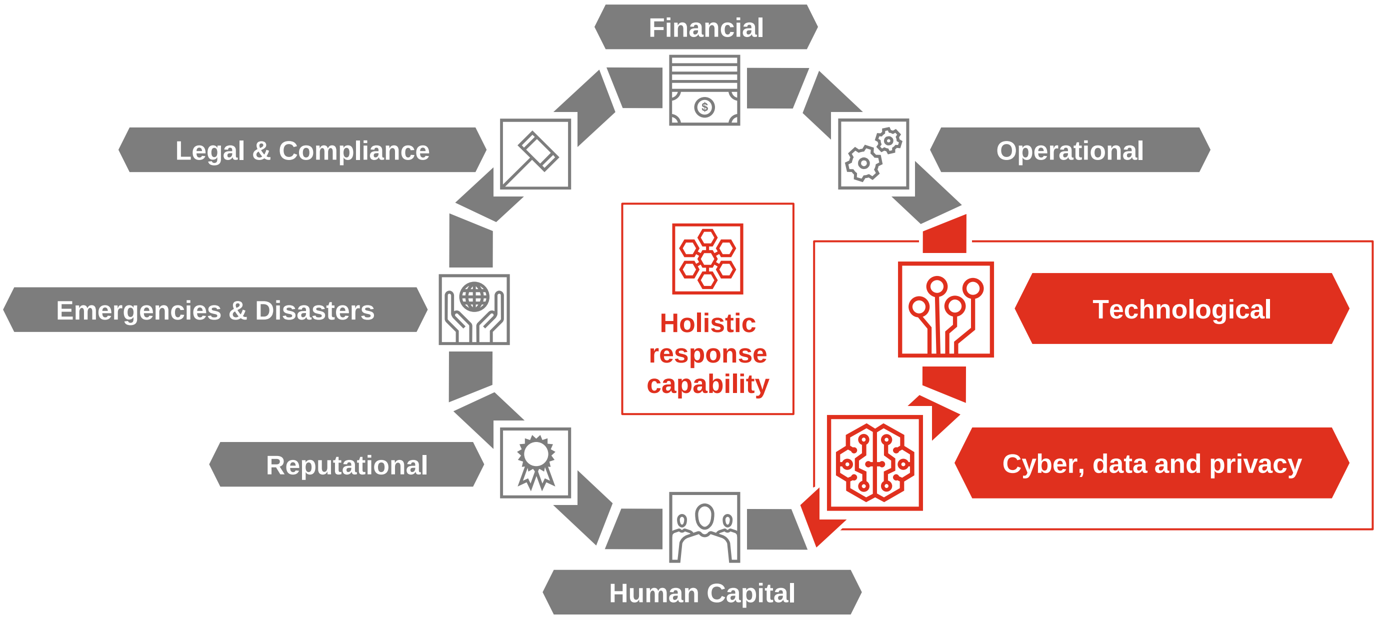
Unstable condition that requires urgent attention and action to protect life, assets, property, or the environment

and brings the company in substantial trouble

Who is managing what?

***Terminology from ISO 22300**

A holistic response capability will help recovering quickly and emerge stronger from a crisis.



Financial

Operational

Technological

Cyber, data and privacy

Human Capital

Reputational

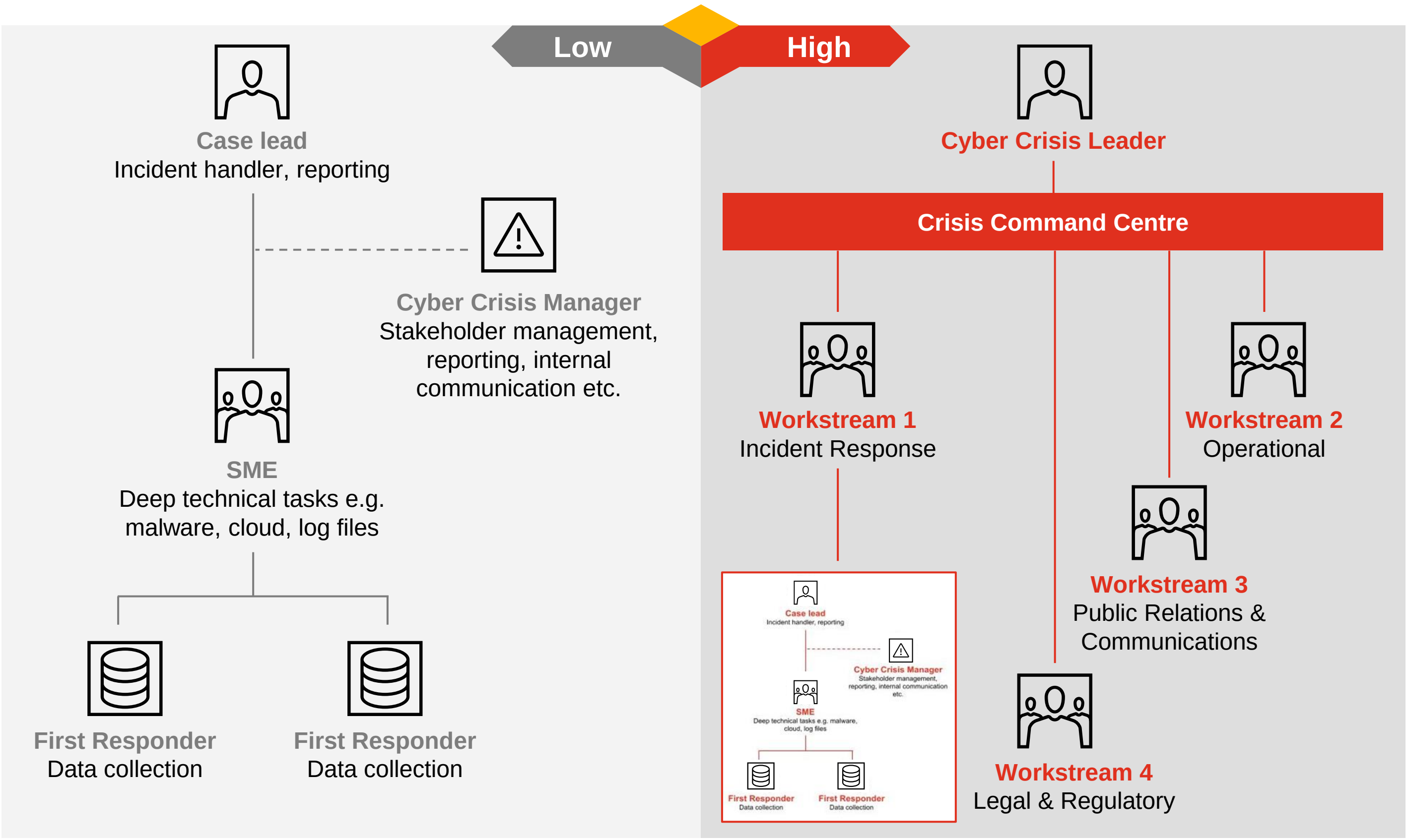
Emergencies & Disasters

Legal & Compliance

Holistic response capability

- Crises and incidents can be triggered by multiple factors. Technological, cyber, data and privacy triggers are rarely isolated but have a significant business impact on other business areas.
- Cyber crisis response teams need to be tailored to the crisis – from a lean approach to multidisciplinary support across business functions.

Response tailored to impact



Low

High

Case lead
Incident handler, reporting

Cyber Crisis Manager
Stakeholder management, reporting, internal communication etc.

SME
Deep technical tasks e.g. malware, cloud, log files

First Responder
Data collection

First Responder
Data collection

Cyber Crisis Leader

Crisis Command Centre

Workstream 1
Incident Response

Workstream 2
Operational

Workstream 3
Public Relations & Communications

Workstream 4
Legal & Regulatory

Business impact when cyber crisis management capability is not made a priority

Key Root Causes Include:

1

The Domino Effect

Inability to validate relationships and interdependencies among business systems and supporting technology

2

No Current State

Inability to easily maintain and evergreen these relationships due to daily changes

3

Functional and Data Silos

Lack of Enterprises Resilience data model and integrated tooling as tools and data focus functionality

4

Failure to Communicate

Inability to communicate risk posture, business/customer impacts or business performance effectively to C-Level or the Board

Key consequences include:

People

Detachment from the current situation and lack of ownership. Potential personnel burnout and even loss of key personnel.

Process

Unclarity on business and response priorities leaving the debate open during a recovery.

Technology

Single points of failure and unaligned technology and security architecture create difficulties for an efficient response.

Business

Due to the above, a frustrated business that has no clear outlook on recovery time and minimum available services leaving them vulnerable in maintaining critical businesses.

What should board and CEO be doing about heightened cyber risks now?

We recommend that boards make time to review their organisation's **cyber posture** and **threat response capability** as soon as possible. CEOs and senior management need to know where to shore up weaknesses. Boards and CEOs should arrange for **table top exercises** with their CISOs to get a taste of what the organisation is up against and how the security team defends against them. These exercises can be very effective in quickly educating boards and CEOs and giving them the **confidence** to decide and act.

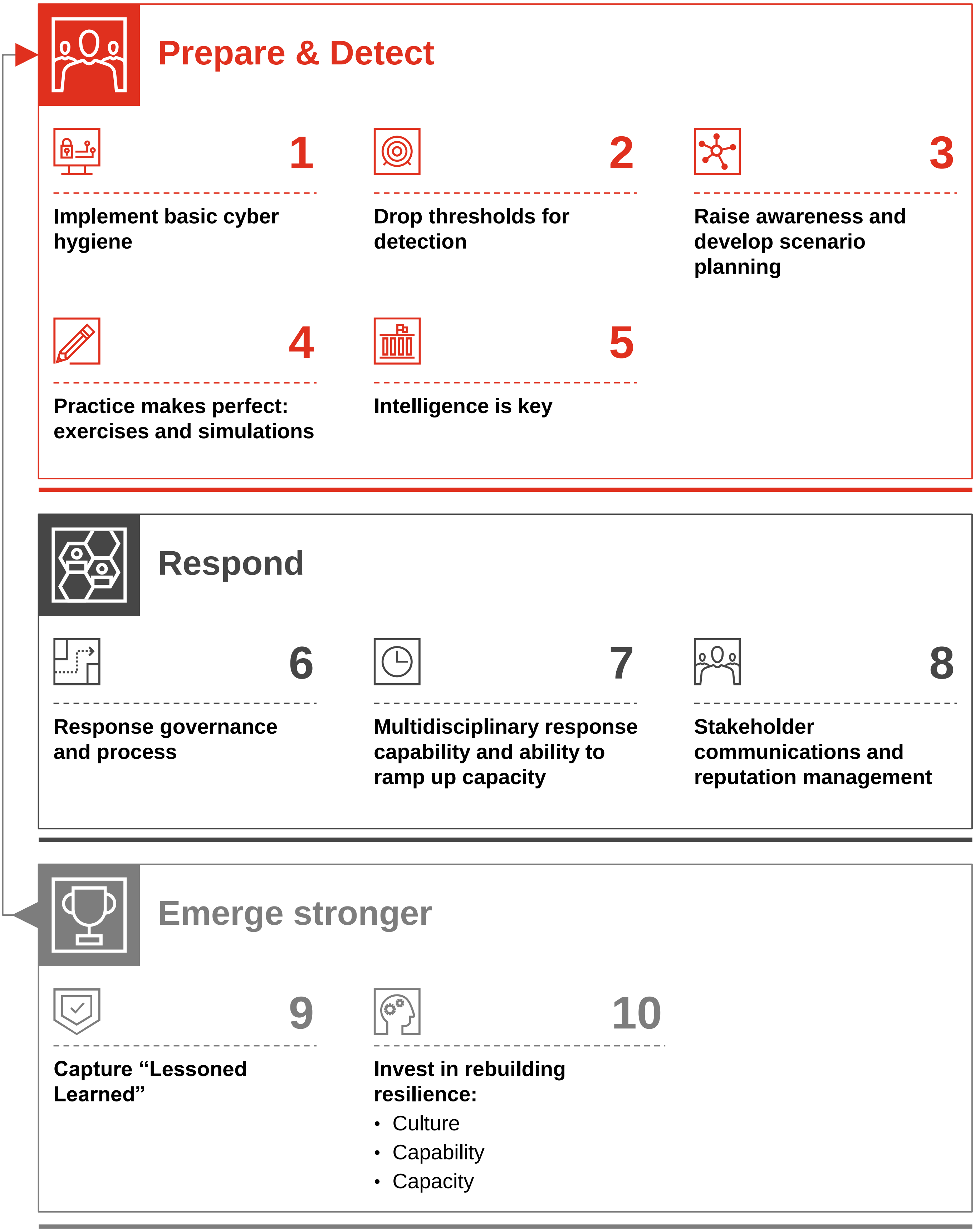
? What to ask your CISO?

- How exposed are our systems, people and assets in countries that are targets of attacks? How closely are we monitoring the connections into and out of those countries in our corporate systems?
- What's the plan if we decide that we need to disconnect our systems? How quickly can we do it without harming our operations and our people?
- Do we have an incident response (IR) and crisis response (CR) playbook? Have we done exercises to test it? When was the last time we tested our IR and CR plan? Have we discussed actions if hostilities begin? What are those actions?
- How sophisticated are our threat detection capabilities? Are we able to detect intrusions in real time? How well do we monitor the cross-over from our IT systems to the tech that runs our operations?
- Do we have strong relationships with national and/or local government agencies focused on cybersecurity?
- How well do our employees help protect the organization against theft of account names and passwords via phishing and social engineering? When did we last scan our systems to detect unauthorized
- How good are our foundational cybersecurity capabilities? What is the state of our organization's cyber hygiene?

In light of the geopolitical events, additional steps the board and CEO should be taking:

CEOs and boards will have to consider more consequential questions. Should we disconnect and isolate the systems that are in the war zone? Can we continue to tolerate the risks or accept a reduction in functionality or capability in certain territories? Should we accelerate key mitigating measures that will require a re-prioritisation of resources?

Cyber attack is a business problem. A 10-step roadmap to resilience.



Prepare & Detect

1 Implement basic cyber hygiene

2 Drop thresholds for detection

3 Raise awareness and develop scenario planning

4 Practice makes perfect: exercises and simulations

5 Intelligence is key

Respond

6 Response governance and process

7 Multidisciplinary response capability and ability to ramp up capacity

8 Stakeholder communications and reputation management

Emerge stronger

9 Capture “Lessoned Learned”

10 Invest in rebuilding resilience:

- Culture
- Capability
- Capacity

Gartner predicts by 2025, 70% of CEOs will mandate culture of organisational resilience to survive*

*Source: Gartner Research 2021”Predicts 2021: Organizational Resilience”

Jane He
Crisis & Resilience
Director
+49 15122898663
qian.x.he@pwc.com

Jens Greiner
Crisis & Resilience
Director
+49 1753532089
jens.greiner@pwc.com

Lorenz Kuhlee
Incident Response
Director
+49 15150049769
lorenz.kuhlee@pwc.com

www.pwc.de/krisenmanagement