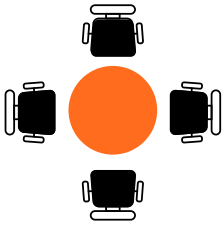
CR4B Cybersecurity Simulation Exercise: Step-by-Step Guide

Seven Steps to Cyber Readiness

1. Prior to the exercise, participants give consent and complete pre-exercise questions.
2. Introduction of exercise format and methodology to participants before the scenarios are presented (30 mins).
3. For each scenario, the participant group is presented with a summary of the incident designed to evoke a response.
4. After reading each scenario summary, the participants answer scenario questions using a response sheet.
5. A group debrief and discussion takes place in closing each scenario-specific round.
6. A final group discussion takes place after the last scenario for further overall insights (45 mins).
7. Following the exercise, findings are provided to participants in an after-report.

Repeat Steps 3 to 5 for each of the four scenarios, with each scenario round lasting 30 minutes.



Introduction

The CR4B Cybersecurity Simulation Exercise was developed as part of the Cyber Readiness for Boards Project, which investigates how corporate boards assess cyber risk and make decisions about cybersecurity investments. More specifically, this exercise investigates risk perception and how executive decision-makers make decisions when faced with an escalating cyber incident.

Participants

In referencing executive decision-makers, we acknowledge that this can involve a large group of individuals, as a 'board', and potentially external, 'non-executive' directors. We define 'executives' as those who must make decisions which drive the direction and strategy of an organisation. However, *"all organisations are different and each board needs to set its own direction and tone for cyber security."*[1]

How the Exercise Works

The CR4B Cybersecurity Simulation Exercise can be held remote or in person, and typically runs about half a day. In order to draw meaningful conclusions about cybersecurity within an organisation, all participants must be from the same organisation. The number of exercise participants may vary, but can include from 10-25 participants.

During the exercise, participants are exposed to four systematically constructed scenarios which describe events applicable to their level of decision-making. Each scenario round, including a post-scenario discussion, was 30 minutes long in duration, to allow participants to read the scenario, ask for clarifications, complete the response form, and to allow for occasional breaks. The scenarios are written to capture the cyber threat environment of the organisation and that of the sector in which it sits. These are written as a narrative around an organisation referred to as "Company A."

Methodology

The scenarios are designed to encapsulate a complete description of the process of risk taking, which together with participant responses provide the full view of risk consideration at the executive level, as highlighted by Shapira[2]: Definition of risk, attitudes toward risk, and dealing with risk. We address the definition of risk in our scenario design, toward eliciting anticipated responses and choices. A survey captures these elements, and a debrief after the survey offers participants the opportunity to *explain* their reasoning.

Scenario design for executive cyber-risks

We designed a series of scenarios which escalate in complexity and ambiguity, all relating to a cyber incident for a hypothetical "Company A." Incidents are presented across multiple rounds in the exercise to reflect escalating risk levels (low, medium, high). The content of the scenarios is informed by the authors' knowledge of IT systems and processes which real organisations are likely to have in place, and threats which can affect those elements of organisation infrastructure. Known security incidents in recent history informed the design in terms of signalling what may be possible.

One challenge to designing engaging scenarios is maintaining ecological validity[3]. Although participants will know the scenario is not real, efforts are made to ensure that the scenario is close enough to reality, that participants can consider the scenario as if they were in a real-life situation that the exercise emulates.

We manage the elements of scenario escalations across specific dimensions according to the risk level associated with the scenario. Scenario content loosely follows a structure of incident, response activity, and executive–level imperatives. The scenarios capture escalation of attack severity through a series of distinct cyber incidents. The benefit of playing through each scenario is exposure to incidents with varying degrees of impact. In terms of impact from cyber risk, this represents an escalation from low to medium to high. The severity of the cyber risk is primarily represented as the severity of an attack and criticality of the affected system, but can escalate by including a more complex mix of affected people and systems. As the scenario escalates, the level of technical complexity and uncertainty then also grows. To note, the latter is not the omission of detail, but the inclusion of factors in a scenario which a security executive is not expected to have immediate knowledge of.

Scenario dimensions

Scenarios are designed across clear dimensions, along which a participant may draw on judgement calls, as an executive involved in a management decision-making process and weighing up factors.

The dimensions which are used to construct the 'recipe' for each of the scenarios include:

- **Risk externalities**
- **Stakeholder management**
- **Anticipated risks**
- **Areas of uncertainty**
- **Technical areas of complexity**
- **Attack classification.**

For each scenario, the authors anticipate a response from "low" to "high". In this sense, the exercise is as much about evaluating the scenario design approach as it is evaluating risk perceptions of participants.

Anticipated risks

We assess the scenarios for business risks as per the Cambridge Taxonomy of Business Risks[5] which outlines business risks that can be explicitly modelled as shown.

Financial risks

Economic outlook and variables, market crisis, trading environments, business and competition.

Geopolitical risks

National security, corruption & crime, government business policy, change in government, political violence, and interstate conflict.

Social risks

Socioeconomic trends, human capital, brand perception, sustainable living, health and disease.

Environmental risks

Extreme weather, geophysical, space, climate change, environmental degradation, natural resource deficiency and food security.

Governance risks

Non-compliance, litigation, strategic performance, management performance, business model deficiencies, pension management and products & services.

Technology risks

Targeted cyber-attacks, critical infrastructure collapse, direct and indirect industrial accidents and the inability to keep up with advances in technology.

Attack classification

To capture how participants perceive the severity of the scenario, we adopted the six-category scale for cyber-attack categorisation proposed by the UK's National Cyber Security Centre (NCSC)[4] By designing and discussing scenarios according to this scale, we can arrange scenarios and structure engagement along a journey of increasing incident severity.

1	2	3	4	5	6
Category 1	**Category 2**	**Category 3**	**Category 4**	**Category 5**	**Category 6**
National cyber emergency	**Highly significant incident**	**Significant incident**	**Substantial incident**	**Moderate incident**	**Localised incident**
Causes sustained disruption of essential services or affects national security, leading to severe economic or social consequences or to loss of life.	Has a serious impact on central government, essential services, a large proportion of the population, or the economy.	Has a serious impact on a large organisation or on wider / local government, or which poses a considerable risk to central government or essential services.	Has a serious impact on a medium-sized organisation, or which poses a considerable risk to a large organisation or wider / local government.	Poses considerable risk to a small or medium-sized organisation, or preliminary indications of cyber activity against a large organisation or the government.	Poses considerable risk to an individual, or preliminary indications of cyber activity against a small or medium-sized organisation.

Complexity and uncertainty

In the scenario questions (See Appendix) we ask participants to identify areas of complexity and uncertainty. As measure of the response to the design regarding stakeholders, we also ask participants to indicate the scope of responsibility for the incident on a scale from private sector to state-owned.

In sum, our characterisation of scenarios is across dimensions of risk impact, the level of stakeholder management needed, anticipated risks, and areas of uncertainty and technical complexity. The characteristics are distinctly encapsulated in the narrative of the associated scenario. These characteristics become different dimensions over which cyber risk escalation is expressed.

Lessons Learned

1 Looking beyond the board

While we started by creating an exercise for board members, we expanded our scope to include other executives involved in cybersecurity decision-making. This was done not only to address the difficulty in recruiting a board, but also to better capture the intricacies involved in addressing cyber risk in an organisation, whereby responsibility is often split. Cyber preparedness is a team effort to be undertaken by many players in an organisation, and thus we were able to focus on the interplay of communication and responsibilities between roles.

2 Calibrating the expert

Our executive participants are decision-makers, many with invaluable experience working with cyber risk in a professional setting. Thus, they are the experts in the room. While many exercises aim to offer recommendations to or rate their participants, we acknowledge that succeeding or not as an executive decision-maker is best judged by the organisation they are employed by. Each organisation has a unique risk appetite and risk culture, which means there is no across-the-board answer. Thus, this exercise aims not to offer recommendations back to decision-makers but rather to gauge their individual response tendencies against themselves-as a group. Thus, we aim to calibrate the expert under the belief that when decision-makers who work together share the same risk perception, they can improve cyber readiness.

3 Risks extend beyond cyber

Cyber risk is just one business risk associated with a cyber incident. Due to their complex nature, cyber incidents may pose a wide array of business risks for organisations. Adopting a wider scope of business risks, this exercise adopts the Cambridge Risk Taxonomy[4], which indeed is not rooted in cybersecurity (though it does include cyber risk under technology risks). In this way, we can explore more fully how executive decision-makers perceive risks associated with cyber incidents, and also how they might prioritize various business risks.

References

1 R. Horne, "Governing cyber security risk: It's time to take it seriously: Seven principles for Boards and Investors," 2017. [Online]. Available: https://www.pwc.co.uk/cyber-security/assets/ governing-cyber-security-risk.pdf

2 Z. Shapira, Risk taking: A managerial perspective. Russell Sage Foundation, 1995

3 S. Schechter, "Common pitfalls in writing about security and privacy human subjects experiments, and how to avoid them," Microsoft, January, 2013

4 National Cyber Security Centre, "New cyber attack categorisation system to improve uk response to incidents," 2018. [Online]. Available: https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response incidents

5 Cambridge Centre for Risk Studies, University of Cambridge, "Cambridge centre for risk studies, 2019; global risk index 2020 executive summary," 2019

Acknowledgements

Research Team

Prof Siraj Shaikh, Coventry University (siraj.shaikh@coventry.ac.uk)

Dr Kristen Kuhn, Coventry University (kristen.kuhn@coventry.ac.uk)

Dr Simon Parkin, TU Delft (s.e.parkin@tudelft.nl)

This research was supported by the UK National Cyber Security Centre (NCSC) and Lloyds Register Foundation (LRF) under the "Cyber Readiness for Boards (CR4B)" project.

For further information, please see our publication: "Scenario-Driven Assessment of Cyber Risk Perception at the Security Executive Level."

Appendix – Participant Forms

Pre-exercise questions

1. What is your current role (job title)? [free-text]
2. How many years of work experience do you have? [number]
3. In your current role, who do you report to (given their role/job title)? [free-text]
4. Please give a brief summary of what IT-related decision making you carry out in your role. [free-text]
5. What do you perceive as top cybersecurity risks to organisations? You may choose from any one or more of the following risks: [Financial, Geopolitical, Technology, Environmental, Social, and Governance]. If more than one, could you rank them in the order of priority, with the highest risk at the top (1) down to lower risk at the bottom (6). [Six rows, each with risk labels as above].

Scenario questions (repeated for each scenario)

1. Which of the following categories does the incident fall into? Please select only one. [Cyber Attack categorisation with "category definition" only]
2. Please explain why you made your specific choice for Question 1. [free-text]
3. Which of the following risk types does this incident raise? You may choose from any one or more of the following listed in the `Risks' column below. [Financial, Geopolitical, Technology, Environmental, Social, and Governance]. You may choose from any one or more of the following listed in the `Risks' column below. If more than one, please rank them in the order of priority, with the highest risk at the top (1) down to lower risk at the bottom (6). [Six rows, each with risk labels as above]
4. For the purposes of risk mitigation, what is the split of responsibility between the state and the private sector (the organisation in the scenario)? Use the scale below to assign this split between the state and the private sector. Choose '3' if you consider the responsibility to be equally shared between the state and private sector. [5-point scale]
5. From the description of the scenario, what aspects are most uncertain to you, and why? [free-text]
6. From the description of the scenario, what technological areas are most complex to you, and why? [free-text]