

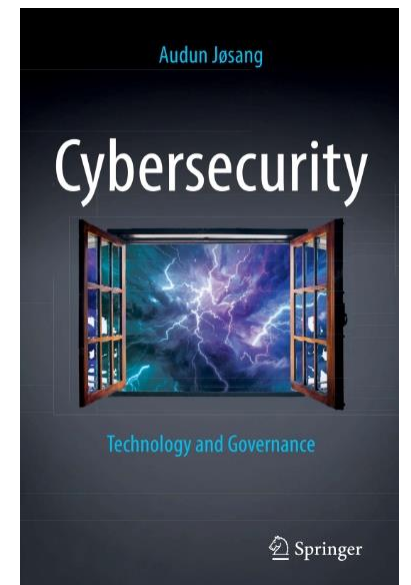
Chapter 14:

Cybersecurity readiness, security testing and audit

Cybersecurity: Technology and Governance

Audun Jøsang,

1st Edition, Springer Nature, 2024.



Overview: Cyber Readiness

Critical functions
Readiness
Incident response



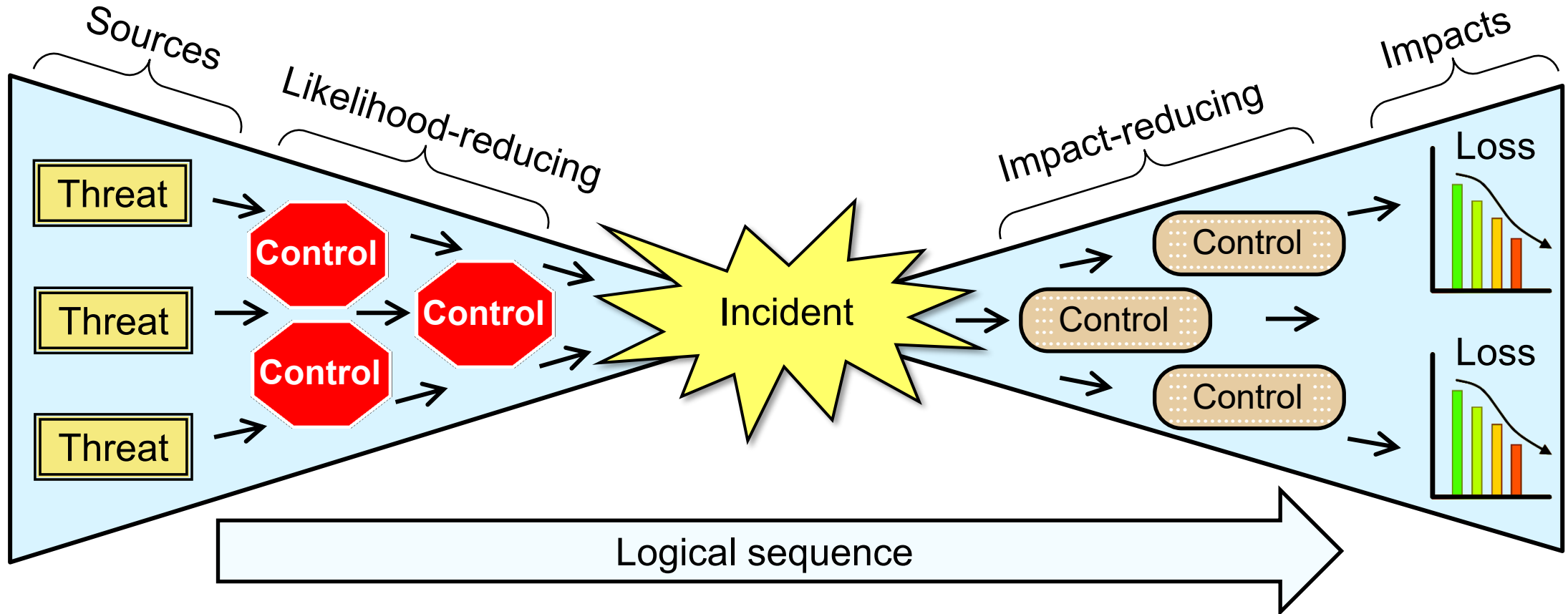
Preparedness

- Preparedness means being prepared to activate consequence-reducing measures in the event of harmful incidents.
- Risk assessment forms the basis for choosing consequence-reducing measures and resources (internal and external) to be able to handle relevant incidents.
- In the event of requirements in legislation, standards or regulations that require specific emergency preparedness measures, these must of course be taken into account.
- Carry out exercises that give a realistic picture of the company's actual ability to handle relevant incidents.
- Words of wisdom:
 - It's not enough to practice until they get it right, you must practice until can't do it wrong.
 - You don't suddenly become an expert when a serious incident occurs, your performance in handling the incident doesn't go higher than the level you have practiced.

National crisis management

- A national crisis management plan typically consists of:
 - Civil crisis response plans
 - Response plans for the defence sector
- NATO's Crisis Response System.
 - A key element of this system is the NATO Crisis Management Process.
- The national emergency preparedness system provides the basis for underlying contingency plans for serious crises in peacetime, security policy crises and armed conflicts.
 - A national health preparedness plan is an example of an underlying plan.

Risk visualization with the bowtie diagram



- A bowtie diagram shows the relationship between causes and impacts related to a specific type of incident, as well as controls that are (are not) implemented. Impact severity is not shown
- Bowtie diagrams are typically used for risk assessment in civil protection.
- Bowtie analysis means creating one or more loop diagrams.

Principles of crisis management

- **The principle of responsibility.** *The entity responsible for an area in normal conditions is also responsible for the prevention, readiness, and implementation of the necessary actions in case of emergencies or disasters.*
- **The principle of similarity.** *The organization of people and resources used during emergencies should be as similar as possible to that which operates in normal conditions.*
- **The principle of proximity.** *Incidents should be handled at the lowest possible level in the organization.*
- **The principle of collaboration.** *Authorities, private enterprises and/or government agencies have an independent responsibility to establish collaboration with relevant entities and agencies in the field of prevention, readiness, and crisis management.*

Incident response

- Incident response encompasses the technical aspects of handling a cyber incident.
- Incident management also includes, for example, contact with the media/authorities and legal aspects.

PREPARATION

- Policy
- Plan
- Team
- Equipment and Tools
- Exercises

TRIAGE

- Detection
- Analysis
- Documentation
- Prioritization
- Notification

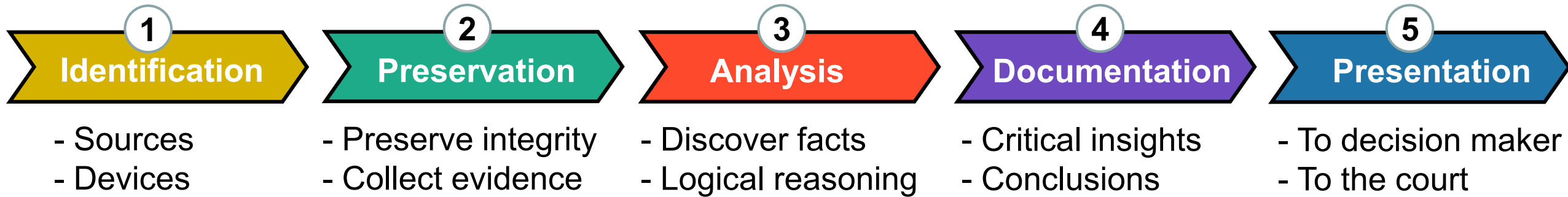
RESPONSE

- Mitigation
- Containment
- Eradication
- Recovery

POST-INCIDENT

- Lessons Learned
- Closing
- Using Incident Data

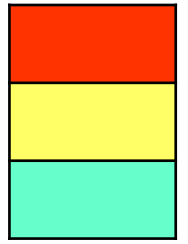
Process for digital forensics



- Network forensics.
- Wireless forensics.
- Disk forensics.
- Database forensics.

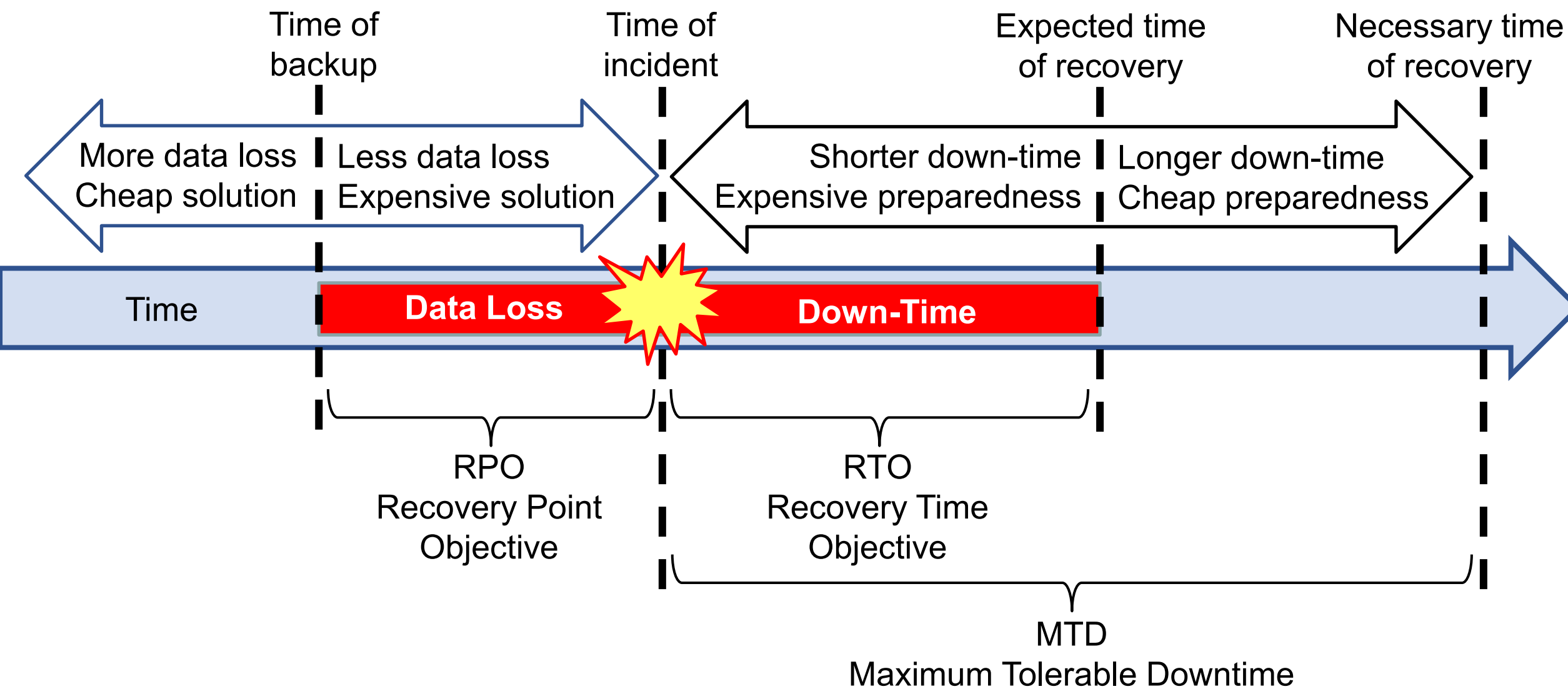
- Email and message forensics.
 - Malware forensics.
 - Memory forensics.
-

BIA – Business Impact Analysis



- A Business Impact Analysis (BIA) is performed as part of contingency planning to identify critical functions that, in the event of an outage, will cause the greatest financial or operational loss.
- Specification of Recovery Time Objective (RTO) which is the objective for the speed of recovery from interruption (i.e., the maximum acceptable period of time for interruption) for each critical function.
- Specification of Recovery Point Objective (RPO), which is the highest acceptable age of backups that need to be restored. If an organization has a short RPO of a few hours or minutes, backups need to be done correspondingly frequently.
- A distinction is made between (limited) crisis events and catastrophic events for the specification of RTO and RPO. In the case of disaster events, longer RTO and RPO are acceptable because recovery is expected to be more difficult.

RPO and RTO



Example RTO and RPO

- The table provides examples of RTO (recovery time target) and RPO (recovery point target) that can be specified for various critical functions.
- Distinction between crisis and disaster events for the specification of RTO and RPO.

Criticality of function	Colour		RTO and RPO in case of crisis events	RTO and RPO in the event of a disaster
High		Red	RTO Within 2 hours with full functionality and capacity. RPO: 2 hours.	RTO Reduced operation within 1 day, 100% operation within 7 days. RPO: 2 hours 2 times.
Medium		Yellow	RTO Up to 8 hours with full functionality and capacity. RPO: 24 hours.	RTO Within 7 days with full functionality and capacity. RPO: 24 hours.
Low		Green	RTO Up to 1 week of full functionality. RPO: 1 week.	RTO Within 3 weeks of reduced operation within 4 weeks of full functionality and capacity. RPO: 1 week.

Exercises for cyber incident response

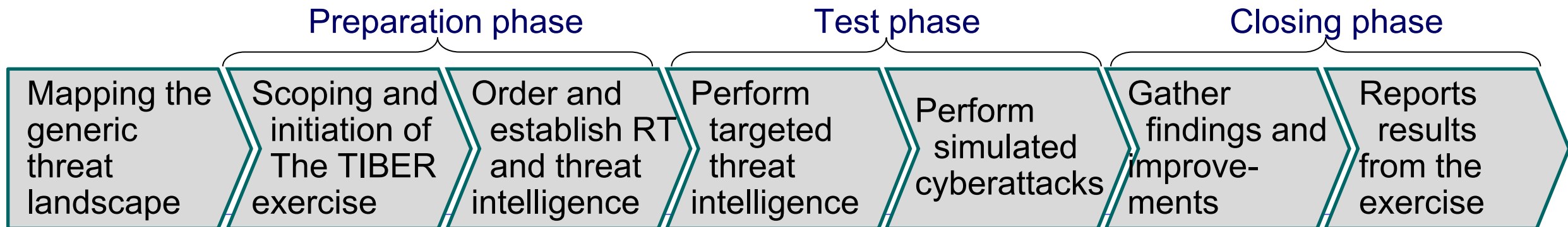
- Forms of exercise:
 - Tabletop: The response team sits together to go through the handling of specific attack scenarios
 - Hybrid: Paper exercise combined with elements of simulated attacks
 - TIBER (Threat Intelligence-based Ethical Red Teaming) simulated realistic attacks against
- Exercise directive shall specify:
 - Purpose: 1) practice something the company is prepared for, 2) test the ability to handle incidents that the company is not prepared for
 - Focus level: 1) individual functions, 2) the entire business, 3) an entire sector, 4) national exercise
 - Exercise elements, i.e. types of attacks and how they should be carried out
- Plan the exercise and produce documentation for the exercise
- Evaluation and follow-up after exercises
 - How experience from the exercise will be incorporated into incident management plans

Cyber Exercise Teams

- Blue Team (BT):
 - Defending against cyber attacks during cyber exercises, and that carries out incident response in the event of cyber incidents. During regular operations (outside of test situations), the same group is typically organized as the SOC (Security Operations Centre) and CERT/CSIRT (Computer Emergency Response Team or Computer Security Incident Response Team).
- Pen tester (penetration tester):
 - Ethical hackers who try to break into a computer system with the intention of uncovering vulnerabilities. The BT has been informed that the pen testing is taking place.
- Red Team (RT):
 - Goes beyond pen testing by exploiting vulnerabilities, adding physical pen testing, social engineering, and an element of deception and surprise. The BT is not informed about the simulated attacks, and will therefore treat it as a real attack.
- White Team (WT)
 - Small group of people who are informed that an RT is carrying out simulated attacks.
- Purple Team
 - Combination of BT and RT.

TIBER (Threat Intelligence-based Ethical Red Teaming)

- Background:
 - Need to conduct realistic RT exercises to be prepared for real cyber attacks
 - Risky to do realistic RT exercises with systems that are in production
 - Need for a framework to carry out RT exercises in a safe way
 - The EU finance sector was concerned about cyber attacks, initiated the TIBER-EU framework
- TIBER-EU:
 - EU framework for RT exercises, primarily in the financial sector, but also other sectors
 - Requires RT to be remote and independent of the business, to make exercise realistic
 - Simulated attacks are based on CTI, for the most realistic exercises possible
 - Must take into account legal aspects of TIBER exercises, due to their intrusive nature



Importance of correct classification

- Correct classification and prioritisation of incidents is important for resources to be able to allocate sensibly and for the incident to be resolved as quickly as possible.
- If it takes a long time from an incident to being notified, prioritized, and handled, the scope of damage, resource usage, and recovery time can increase significantly.
- Misclassification of an incident can lead to a business spending a lot of time and resources on non-material incidents while serious incidents go under the radar.
- An incident that could initially have been solved easily can escalate and spread if reactive measures are not taken quickly enough.
- In the case of complex malware, few people will be able to see the actual extent of the damage until after the incident. In such cases, many enterprises will need to obtain expertise outside their own activities.

Importance of competence and experience for decision-making

- When a security incident occurs, there will typically be a discussion about whether services should be shut down, whether measures should be taken or whether it is best to sit still and just observe to understand what is happening.
- This is a very difficult assessment that requires that those who assess the incident are competent and have experience.
- The extent of the damage can be very different for the different choices.
 - Shutting down a service can have consequences for the company's deliveries, and a premature shutdown can make it difficult to clean up and get started again.
 - Not shutting down services can lead to these being compromised.
 - Introducing measures without knowing if the attacker has been completely eradicated can cause the attacker to go into hiding while still having a backdoor to the web.
- Companies must strive to ensure that all relevant resources are seated around the table when such decisions are to be made.

Global threats require a unified response

- Cyber security has evolved from being about technical aspects that each company handles itself, to becoming a strategic challenge that is addressed sector-wise, nationally and globally.
- The supply chain attack against IT provider SolarWinds is a well-known example that led to widespread consequences for businesses around the world. Such global events show that cyber operations have a large scale and a global impact.
- Attack against one is the defense for all the others. This principle means that cooperation between like-minded countries makes it possible to respond to cyber incidents far more effectively. Global threats require a unified response.



Learn from the incident, and not point to scapegoats

1. **Good understanding of the incident.** To explain an incident, those who report and communicate themselves must have a good understanding of the incident.
2. **Focus on the "what".** Focus on what went wrong, not who did something wrong. Individuals are never the root cause, except perhaps for intentional events.
3. **Fokus on "how".** How the same type of incident can be avoided in the future.
4. **Open door.** Employees must always feel welcome to talk about incidents and observations, and to report their own or others' deviations without fear of criticism.
5. **Exclude the assessment of individuals.** Although individuals have shown a persistently poor safety culture, this should not be mentioned in the incident report. Correcting such attitudes is perhaps more appropriate in HR.
6. **Focus on learning.** The most important thing is to learn how to avoid similar incidents in the future, and to be better able to handle incidents if they do happen.

<https://www.threatstack.com/blog/how-to-conduct-a-blameless-security-post-mortem>

End of presentation