Test your organisation’s capacities and develop your CyberResilience through Crisis Management

- Customisable scenarios tailored to your business
- Cyber-attacks based on real-life cases
- A simulated crisis involving all of your services
- Animation by our cyber experts
- Feedback and complete report on lessons learned

The objectives and benefits of Crisis Management training

- Cyber crisis management does not only involve technical functions, but the entire organisation
- Training and education are necessary to prepare for effective crisis management
- Conducting cyber crisis management exercises requires expertise
- Airbus CyberSecurity is an experienced partner capable of supporting you in this process

Airbus CyberSecurity

- A leading European provider protecting EU institutions
- An end-1-end integrator for IT and OT industrial cyber security
- A trusted partner for Airbus, Governments and Critical Industries
- Unique experience with platform security and embedded systems
Is your organisation prepared for a cyber security crisis?

MEDIA PRESSURE
- Understand the relationship with media during a cyber security crisis
- Adopt a strategy to respond to print, digital and broadcast media
- Test your crisis communication plan through interviews with crisis managers and TV spokespeople

OUR COMPREHENSIVE EXERCISE CATALOGUE
- Large number of proposed exercises
- Diverse range of environments adapted to your specific needs and objectives
- Place your organisation team members in a realistic crisis situation within a crisis unit
- Possibility for your teams to test and experiment with reflex sheets, maps, directories and plans on concrete cases that could affect your organisation

ATTACKS BASED ON REAL CASES
- Information system sabotage
- Data leak: disclosure of confidential information
- Theft of strategic data by a competitor
- Shutdown of factories and machines following a cyber-attack
- Fake news and damage to the company’s reputation
- Malware blocking computers
- Ransomwares holding the organisation hostage

BUZZ ON SOCIAL NETWORKS
- Identify the causes of reputational crisis resulting from rumours
- Analyse the consequences of malicious propaganda
- Plan and coordinate your actions to handle the crisis

MEDIA PRESSURE
- Understand the relationship with media during a cyber security crisis
- Adopt a strategy to respond to print, digital and broadcast media
- Test your crisis communication plan through interviews with crisis managers and TV spokespeople

OUR COMPREHENSIVE EXERCISE CATALOGUE
- Large number of proposed exercises
- Diverse range of environments adapted to your specific needs and objectives
- Place your organisation team members in a realistic crisis situation within a crisis unit
- Possibility for your teams to test and experiment with reflex sheets, maps, directories and plans on concrete cases that could affect your organisation

ATTACKS BASED ON REAL CASES
- Information system sabotage
- Data leak: disclosure of confidential information
- Theft of strategic data by a competitor
- Shutdown of factories and machines following a cyber-attack
- Fake news and damage to the company’s reputation
- Malware blocking computers
- Ransomwares holding the organisation hostage

BUZZ ON SOCIAL NETWORKS
- Identify the causes of reputational crisis resulting from rumours
- Analyse the consequences of malicious propaganda
- Plan and coordinate your actions to handle the crisis

OPERATIONAL SUPPORT FROM OUR SPECIALISTS TAILORED TO YOUR SECTOR
- SOC: Security Operations Centre
- CSIRT: Computer Security Incident Response Team
- CTI: Cyber Threat Intelligence
- ICS: Industrial Control Systems
- Partner companies (training, simulation tools)

SCENARIOS TAILORED TO SUIT YOUR ORGANISATION
- Consideration of your specific needs
- Proposal of standard or customised scenarios, architectures and injects that can be adapted to your objectives/parameters
- Organisation of exercises in our or your own premises in the Paris region, in other regions, on one or more sites

AN IMPACT THAT INVOLVES ALL OF YOUR SERVICES
- Making critical decisions while under pressure from management
- Challenging choice between several solutions by the IT department
- Budget and massive expense management by the Finance Department
- Key messages to be transmitted urgently through Communication
- Prioritisation of presence by Human Resources
- Interactions between numerous departments: Technical Management, Commercial Management, Operational Management, etc.

A REALISTIC SIMULATION WITH OUR CYBERRANGE
- A simulation environment for highly sophisticated and realistic cyber security exercises
- The best way to respect procedures and adapt your IT tools through simulated cyber-attacks in real conditions
- A mobile solution that can be easily and quickly deployed on either your or our premises

AN IMPACT THAT INVOLVES ALL OF YOUR SERVICES
- Making critical decisions while under pressure from management
- Challenging choice between several solutions by the IT department
- Budget and massive expense management by the Finance Department
- Key messages to be transmitted urgently through Communication
- Prioritisation of presence by Human Resources
- Interactions between numerous departments: Technical Management, Commercial Management, Operational Management, etc.
4 different packages tailored to your needs

**Theoretical training:** a course on the fundamentals and specifics of cyber crisis management to equip your organisation with the tools and best practises for effective crisis communication

**Practical training:** a practical case study that highlights the importance of effective crisis management for your organisation’s employees

**Discovery exercise:** a crisis tabletop simulation including the testing of real-time decision-making processes and systems within your company, including your CISO, Finance, HR and Communication teams

**Global exercise:** adding a real cyber-attack to a simulated information system with our CyberRange, training your decisional and operational teams (including your system administrators and SOC staff)

**Feedback and lessons learned**

**At the end of the exercise**
- ¼ of the exercise time
- Discussions and exchanges between the facilitation team and all participants

**A month after the exercise**
- Full report with possible improvements
- Evaluation grids included with a methodology
- Optional presentation to management and/or specific teams