>_Code blue
by Dussmann

Who we are

Code Blue by Dussmann's service portfolio includes services to protect organizations before, during and after cyber crises. The team consists of experts specializing in cyber risk management, reputation management, data protection, ransomware negotiation, Incident Response (IR) and business continuity.

Code Blue by Dussmann is a joint venture between the global services company Dussmann, headquartered in Berlin, and Tel Aviv-based Code Blue Ltd. The experts at **Code Blue Ltd.** Israel have successfully managed numerous complex cyber crises and significantly minimized the impact for their international clients.

The service company **Dussmann** is a solution partner in the areas of integrated facility management, food services and technical plant engineering. It is the largest division of the family-owned **Dussmann Group**, which provides services for people with 66,000 employees in 21 countries.

10 reasons for Code Blue by Dussmann

1. Ready to go worldwide - Europe, South America, Asia and Middle East.
2. All-in-one solution - comprehensive on-call and crisis crisis management services from a single source.
3. Alite cyber crisis team - operated by graduates of the Special Forces graduates certified by the U.S. HLS.
4. Cyber crisis prediction - groundbreaking prediction for crisis crisis response and recovery.
5. Holistic risk assessment - examining corporate governance, cyber insurance and financial resilience.
6. Reputation management experts - experienced specialists in communication, negotiation and deception.
7. Cutting-edge technology - technical platforms for preparedness management.
8. Intelligence-driven reputation - technical tools for advanced intelligence and reputation management.
9. Innovative BCP operations - pioneering work for the world's unique BCP cyber operations.
10. Customized defense portfolio

>_ No more crisis!

In a digital world, cyber security is non-negotiable

>_Code blue
by Dussmann

Cyber crisis management is a matter for the board

Across the company, cyber attacks are one of the few crisis situations that can pose an existential threat. The solution to cyber incidents must not be the sole responsibility of the IT department, but requires strategic action at crisis team level. Thanks to our extensive experience in actual IT-emergency and crisis situations, we have the know-how to establish effective crisis management. We are able to support you in an emergency and ensure effective communication and business continuity in crisis situations.

Crisis management team as a service

We know that effective cyber crisis management should ideally be the responsibility of a central crisis team that is also responsible for other crisis situations. This requires some specific adaptations.

We offer the following consulting services:

- Provision of a complete Crisis Management Team (CMT) and Incident Response Team for cyber emergency using unique methodology to reduce crisis length and damages. A central crisis team that establishes the necessary interfaces and coordinates all experts from PR and reputation management, incident response (IR), data protection, forensics and action leaders specifically required for crisis management.
- Preparing the organization to handle cyber crisis on all levels.
- Assessment of the cyber business continuity risks to which you are or could be exposed in the future, as well as options for risk minimization and annual workplans.
- Preparation of cyber emergency and business continuity protocols, in accordance with the ISO 22301 standard and the extensive knowledge of the company in handling cyber crisis.
- Advice on the understanding of roles and working methods of the crisis team in various cyber attack scenarios.

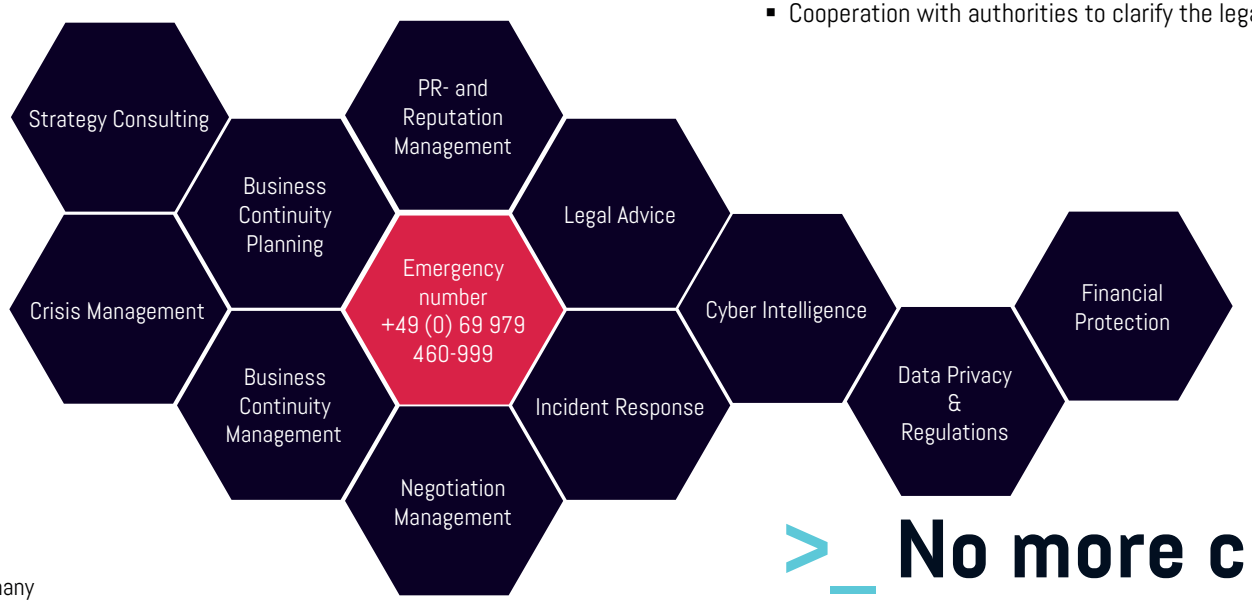
Cyber crisis management simulations

In close collaboration with you, we develop a scenario for a cyber crisis management simulation. This can include a DDoS attack, an attack with ransomware or the theft of data with subsequent blackmail.

During the simulation, we integrate various scenario developments, moderate the crisis management simulation and monitor your response to the mock crisis in collaboration with our crisis experts and IT experts. In doing so, we focus on:

- Your approach to crisis management and dealing with various participants and stakeholders.
- The way in which the crisis is communicated.
- Maintaining operational continuity.
- Compliance with data protection regulations.
- The measures taken by the IT department.

Following the simulation, you will receive a detailed report in which we analyze what went well and where there is room for improvement.



Rapid response in the event of an incident

Our team of experienced experts offers you comprehensive support as your external crisis team and forms the crisis team in cases of cyber attacks such as cyber extortion through ransomware, data theft and DDoS attacks.

- Immediate advice by telephone and formation of a crisis team within four hours at your premises or remotely.
- Expert support and advice from the crisis team.
- Support with crisis communication so that you remain in control and get ahead of the situation.
- Recovery of operational continuity to minimize the damage.
- Access to legal experts from our network on all relevant legal issues.
- Use of state-of-the-art cyber threat intelligence information for better decision-making.
- Targeted research on the darknet to assess the situation.
- Negotiation with cyber extortionists.
- Support in the procurement of crypto payment means such as Bitcoin or Ether and the payment process in cooperation with our partners.
- Cooperation with authorities to clarify the legal situation.

>_ No more crisis!

www.codebluecyber.com
Code blue GmbH | Stützeläckerweg 14 | 60489 Frankfurt am Main / Germany