Crisis and Resilience

Unexpected cyber incidents can hit your business hard and fast. Being ready matters. More and more, companies see the need to plan ahead for cyber crises to ensure their important business services can continue to operate. Let us help you prepare for the worst with our Crisis and Resilience Services.

These Crisis and Resilience Services give you:

Multi-level insights

You gain insights into the resilience of your organization across all domains, giving you the complete picture.

Realistic simulations

Practice your response to a realistic simulated cyber attack, based on current threat intelligence.

A global partner

You benefit from our experience of serving customers all over the world, from multinationals to government.

Why choose Crisis and Resilience Services?

Making sure your organization can keep running during a cyber crisis is challenging.

- How do you ensure your senior staff know their own role and responsibilities during a crisis?
- How resilient are your important business services against severe but plausible events?
- How would you continue to operate your critical business activities in the event of a cyber attack?
- How can you practice your response to a cyber crisis?

A well established crisis management and resilience program will make sure your organization has the necessary tools in place to anticipate and respond to evolving threats. It will also help you in complying to new EU cybersecurity regulations, such as **NIS2** and **DORA**, as well as the **FCA/PRA** regulations on Operational Resilience in the UK. We have extensive expertise in helping customers with their crisis and resilience. Let us help you.

The Crisis and Resilience Services we offer

- Crisis Management
- Operational Resilience
- Business Continuity Management
- Cyber Crisis Exercises

Crisis Management Services

Organizations often focus on the technical response, but is your organization prepared to deal with the wider organizational crisis that follows a cyber incident? We can help you design and implement Crisis Management frameworks, plans, playbooks and procedures, or help you draw lessons from a cyber incident you have experienced. This means:

- You understand how mature your crisis management framework is and what needs improving to align to international standards.
- You have an embedded crisis management framework, aligned to the international crisis standard ISO 22361.
- You have a tried and tested crisis response plan, so that you are not caught off guard in case of a major cyber crisis.

Operational Resilience Services

Operational resilience is essential for making sure your business can keep running in the face of disruptions, such as cyber attacks or technical malfunctions. An operational resilience program will make sure you have tools in place to anticipate and respond to evolving threats. One of the ways to do this is through **Cyber Impact Tolerance Testing**.

Cyber Impact Tolerance Testing

1	Our experts conduct a review of your critical applications, to identify how vulnerabilities impact the resilience of your important business services.
2	We create scenarios for your senior staff, so they can demonstrate how they would ensure the recovery of their important business services.
3	You receive a report of the findings. It also details recommendations, so that you can improve the resilience of your important business services.

Business Continuity Management

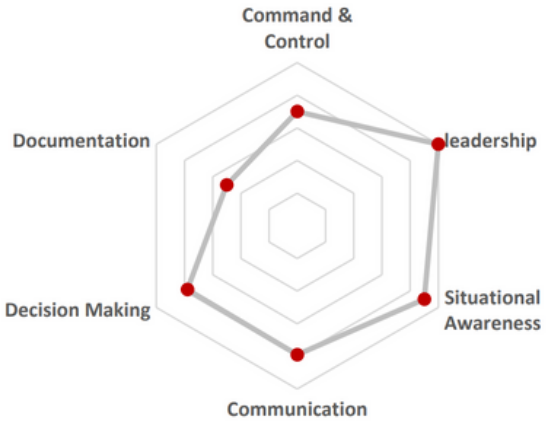
Continuity of critical services is key to protecting the viability of your organization. We can help you with this. For instance by designing a **Business Continuity Management System** (BCMS) that aligns to the international standard ISO 22301:2019.

Obtain an end-to-end view of your organization's services and the resources needed to ensure your critical activities can continue in case of disruption.

Have tried and tested plans in place detailing what recovery strategies are available to your staff, to help them continue critical business functions.

Cyber Crisis Exercises

A cyber crisis doesn't just need a technical response, but requires a coordinated response across the entire organization. How does your strategic response align with the operational technical response? What do people expect from each other? How can you escalate from identifying the attack to strategic decision making? A **Cyber Crisis Exercise** helps you practice your response at operational, tactical and strategic levels.



Gain insight into your organizational crisis response capabilities, as shown above.

Give your staff the chance to put their plans into practice, so that they can test them.

What our customers say

"The pressure felt real"

"The Cyber Crisis Exercise we did was very well put together and tailored to our situation, which added to the realism and feeling of immersion."

Choosing the right Crisis Exercise

Depending on your needs, your target group and your goals, we can help you with a range of different exercises. We also offer exercises created especially for OT systems.

Crisis Exercises

Walk-through	This simple exercise guides participants through a scenario in a controlled discussion-based format.
Tabletop	This more realistic exercise contains simulated scenario updates the crisis team responds to.
Functional	An exercise with a specific focus, such as trying out response tooling or improving communications.
LIVE - Full scale	The most realistic exercise, involving multiple response teams and performed over a longer period.
Gold-Teaming	Using the outputs of a red team or pentesting assessment, this exercise for your strategic or tactical teams is based on actual attack attempts.

SECURITY INNOVATION
A BUREAU VERITAS COMPANY

About Security Innovation/ Bureau Veritas

Security Innovation is a leader in software security, providing comprehensive assessment solutions to secure software from design to deployment, across all environments, including web, cloud, IoT, and mobile. Leveraging decades of expertise and as part of Bureau Veritas, a global leader in Testing, Inspection, and Certification, we seamlessly integrate world-class security into development processes, safeguarding the way companies build and deliver products.

Security Innovation is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80.000 employees and is active in 140 countries.

Example case | Crisis and Resilience

Which problem did the customer have?

A global lighting manufacturer wanted to understand what impact a ransomware attack would have on their manufacturing plants, and how their crisis response teams would come together to coordinate the response.

Result

We created a number of cyber crisis simulations for this client, tailored to each of their sites across the globe. These trained their response teams and revealed a number of opportunities for improvement.

BUREAU VERITAS

Interested?

Contact us today to start raising your cyber resilience.

sisales@securityinnovation.com

+1 877 839 7598

securityinnovation.com