Roc

Complex Incident Management

SOLUTION SHEET

Specialist-led cyber support to contain threats, restore operations and safeguard your organisation's future.

A major cyber attack can cripple business operations. It can damage your brand credibility and result in severe financial and regulatory consequences. In these high-stakes situations, rapid, decisive action is required to contain the threat and restore normal operations.

Roc's Complex Cyber Incident Management service, delivered in partnership with leading cybercrime specialists, Mishcon de Reya, provides the expertise and support necessary to navigate the aftermath of a major breach. This minimises disruption and safeguards your organisation's future.

We offer a comprehensive response beyond technical recovery, bringing together cybersecurity specialists, crisis communicators, legal advisors, and compliance experts. Roc delivers the strategic and technical guidance needed to regain control with confidence, whether it's mitigating further risk, managing reputational impact, or ensuring regulatory alignment.

Ideal for you if...

- You experience a serious cyber attack and need urgent technical and strategic support
- You require specialist expertise beyond your in-house security team's capabilities
- You need guidance on regulatory compliance, legal obligations and stakeholder management
- You require forensic investigation and secure data handling for incident response
- You want to enhance coordination with external agencies, including law enforcement

Why Roc?

24/7/365 INHOUSE MSOC	100% UK COVERAGE	70+ HIGHLY TRAINED ENGINEERS	CYBER ESSENTIALS PLUS ACCREDITED
100% ENGINEERS SC OR DV CLEARED	ISO9001 ACCREDITED	14001 ACCREDITED	27001 ACCREDITED

Service benefits

- Downtime reduction for your organisation
- Minimise disruption
- Manage and protect your brand reputation
- Ensure regulatory compliance and avoid penalties

Find out more about how Roc can help secure your business.
Contact us today or visit our website at **roctechnologies.com**

Service overview

Specialist incident response and containment

When you experience a major cyber incident, immediate action is critical to limit damage and restore operations. Our on-site technical specialists, including BCSC Level 2 responders, work directly with your in-house teams to identify the source of the breach, neutralise threats, implement containment strategies and work to recover your data. We help minimise operational disruption and financial impact by rapidly securing compromised systems and preventing further escalation.

End-to-end crisis and stakeholder management

Effectively managing the wider implications of a cyber attack goes beyond the technical response. Roc provides expert guidance on crisis communications, legal and regulatory compliance, and corporate reputation management. We engage with key stakeholders—including customers, regulators, and the media—ensuring your response is aligned with best practices. We coordinate with external agencies such as law enforcement and industry bodies to support investigations and manage ongoing risk.

Regulatory compliance and legal support

A cyber breach can trigger significant regulatory and legal implications, requiring a strategic approach to compliance. Our specialists ensure adherence to industry regulations such as GDPR, NIS2, and sector-specific frameworks. This ensures your organisation meets mandatory reporting requirements while mitigating financial and reputational penalties. W guide your business through the complexities of post-incident governance by working closely with legal advisors and compliance teams.

Forensic investigation and data handling

Understanding the full scope of a breach is vital for recovery and future prevention. Roc conducts forensic investigations to PACE (Police and Criminal Evidence Act) standards, ensuring digital evidence is gathered and handled correctly. We trace and analyse compromised data, providing insight into how the attack occurred, what information was affected, and whether stolen assets can be recovered. This intelligence not only supports remediation but also strengthens your organisation's ability to prevent future incidents.

Complex Incident Management

Roc will help you manage and control the broader impact on your business, mitigating further risk, protecting your reputation and avoiding financial penalties. Our capabilities include:

Incident Management
Onsite technical specialists up to and including NCSC Level 2 responders working with your team to detect and remediate the threat, and recover your systems and data.

Threat analysis and removal
Establishing a definitive answer as to what caused the breach, and removing all infection or malicious presence from your digital estate, with remediation to prevent further attacks.

Impact assessment
A full and thorough tracking of activity, residency and data loss.

Law enforcement liaison
Reporting of criminal activity, ongoing updates and data handling to PACE requirements.

Specialist corporate support:

- Asset tracing and recovery – helping you recover stolen data
- Cryptocurrency investigations – tracing and recovering stolen or ransomed crypto funds
- Threat intelligence – researching specific threats
- Digital evidence gathering and reporting – compilation of dossiers to support prosecution, offering forensic investigation to PACE standards
- Internal investigation support – providing discrete support for sensitive or internal user data leaks
- Legislation and regulation support – representation and liaison with legal bodies
- Reputation management – take-down handling and malicious content tracking, recovery from data breaches, addressing cyber squatting and misinformation

Find out more about how Roc can help secure your business.
Contact us today or visit our website at **roctechnologies.com**