Cyber **security**

CYBER INCIDENT RESPONSE

READY FOR THE INEVITABLE?



THREAT READY

LRQA CIRT
CYBER INCIDENT RESPONSE TEAM

CREST INCIDENT MANAGEMENT
Incident Response

Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Response: Standard Level

LRQA
Your Risk Management Advantage

CONTENTS

LRQA’s cyber incident response services	3
Benefits	4
Features	5
Service options and what is included	6
Cyber incident response consultancy	7

LRQA'S CYBER INCIDENT RESPONSE SERVICES

LRQA provides a managed incident response (IR) retainer tailored to suit the needs and threats your organisation could be facing.

Using leading industry technology and certified experts, the LRQA Cyber Incident Response Team (NCIRT) manages, contains, remediates, and reports on cyber incidents. Importantly, a managed IR retainer gives you assurance when you most need it.

As cyber-threats evolve at pace around the world, the likes of ransomware, malware, and insider threats pose a serious risk to organisations. Especially when they go undetected for a while.

The cost of an average data breach is £3.2 million, with average resolution time at 280 days. Effective incident management and response reduces the impact of a cyber breach by ensuring optimal decisions and actions are taken, based on professional analysis of available security event, forensic, and threat intelligence data.

Once a breach is identified, time is of the essence and having experts on hand to control the damage is vital to getting your systems back on the road to recovery.



LRQA CIRT
CYBER INCIDENT RESPONSE TEAM

BENEFITS

CYBER INCIDENTS ARE ONLY A MATTER OF TIME.

LRQA's experienced Cyber Incident Response Team (NCIRT) is committed to helping you at every stage of the incident response lifecycle. From preparation, eradication, and remediation, through to lessons learnt.

As part of our managed incident response service, we provide a full range of tactical and strategic solutions tailored to your environment and organisational needs ensuring a robust security posture when you need it the most.

- Certified expert team on hand 24/7 as part of your team to support your business response to a cyber attack
- Expert advice and guidance covering technical remediation, incident management, risk & business continuity planning during an event
- Dramatically reduce the time, and therefore the costs, of resolving incidents maintain productivity whilst specialist staff resolve incidents
- Expeditious containment of the incidents will prevent the spread, and thus cost, of a cyber incident
- Early resolution of incidents prevents further losses of data from a compromised system
- Your organisation could qualify for a lower cyber insurance premium by having aligned experts in place
- Conform to industry best practice and emerging legal requirements

PREPARATION

DETECTION & ANALYSIS

CONTAINMENT, ERADICATION & RECOVERY

POST-INCIDENT ACTIVITY

LRQA CIRT
CYBER INCIDENT RESPONSE TEAM

CYBER RESPONSE ENGAGEMENT MANAGER

CYBER RESPONSE INCIDENT MANAGER

- Certified incident response analysts & consultants
- Cyber response engagement manager
- Cyber response incident manager
- 24/7 response SLA
- Cyber risk assessment & guidance
- Assisted onboarding & preparation
- Incident response business continuity preparation
- Host, network, malware analysis & reverse engineering

FEATURES

We provide a full range of tactical and strategic solutions tailored to your business needs and network environment, ensuring a robust security posture when you need it, enabling you to get back to normal operations quickly, with confidence.

GLOBAL EXPERTISE

LRQA has been at the forefront of cybersecurity since 2003. Our NCIRT team has the know-how and expertise to quickly identify, investigate and remediate the breach.

RAPID RESPONSE

Our NCIRT team understand that a rapid response is critical to containing and limiting the impact of a cyber incident. Our experts can start work within hours backed by guaranteed response SLAs and rapidly analyse for signs of compromise or breach.

HANDS-ON REMEDIATION

NCIRT can provide guided and assisted hands-on technical remediation support to help guide your teams to implement recommendations to contain and eradicate then reduce the risk of future compromise.

COMMAND & CONTROL

We assign you dedicated cyber incident and engagement managers with years of industry expertise in managing crisis situations to aid in the command, control & communications over all cyber incident response activity.

TECHNOLOGY & THREAT INTELLIGENCE

Leading industry technologies and sophisticated threat intelligence is available to our SOC to ensure they always remain ahead of the latest cyber threats.

REPORTING

Cyber response and incident level reporting covering impact, recovery, technical analysis & investigation and executive-level summary encompassing all facets of a cyber incident management.

RESEARCH & REVERSE ENGINEERING

We can provide host, network and malware analysis and reverse engineering through our dedicated Research & Innovation centre.

SERVICE FLEXIBILITY

Our services provide flexibility for you and any unused IR hours can be used on alternative IR professional services to ensure you maximise value from your service.

SERVICE OPTIONS AND WHAT IS INCLUDED

SERVICE OPTIONS

LRQA's CIRT works with you regardless of your budget, environment, or organisation size.

We ensure you get the right care and readiness you need ranging from a basic IR consultation triage service to the premium level services with guaranteed SLAs and flexible consumption models.

Service Level	24/7 Hotline	Guaranteed SLA	Pre Paid Hours	Transfer Unused Hours	Cyber Incident & Engagement Manager
Bronze	✓	4 Hours	✓	✓	✓
Silver	✓	4 Hours	✓✓	✓	✓
Gold	✓	4 Hours	✓✓✓	✓	✓

WHAT IS INCLUDED

- LRQA's guided and assisted onboarding process for essential and premium services:
  - IR policy and procedure review
  - IR tabletop planning and readiness exercise
- 24-hour IR hotline
- NCIRT guaranteed response - four hour SLA (IR consultant contact)
- Aligned cyber response incident manager
- Aligned cyber response engagement manager
- Access to our expert technical team, NCIRT
- Bank of retained hours aligned and ready for an event

LRQA CIRT
CYBER INCIDENT RESPONSE TEAM

LRQA

CYBER INCIDENT RESPONSE CONSULTANCY

LRQA's Incident Response service offerings can evaluate and significantly enhance an organisation's ability to respond to a cyber attack.

INCIDENT RESPONSE PLAN AND POLICY WRITING

LRQA will work with your organisation to create an incident response policy and plan that is tailored to your organisational needs and aligned to industry best practice. The plan will outline the tools and procedures that your security team will use to identify, eliminate, and recover from cybersecurity threats. By having a well-planned and documented policy and response plan you can ensure an expedient response when it is needed most.

TABLETOP EXERCISES – CYBER RESPONSE

Regular practice of your organisation's response to a cyber incident means teams are likely to respond more effectively when under the pressure of a real cyber incident. This engagement has been designed to test your organisation's incident response plan through carefully crafted bespoke scenarios based on the biggest threats to your organisation. During the course of the engagement, multiple scenario injects are used to test your team's thought process and decision-making skills. At the end of the engagement, a report is provided that identifies any areas that may require improvement or present risk.

RANSOMWARE RESILIENCE ASSESSMENT

The threat from ransomware has increased significantly over the past years with different techniques being adopted by threat actors and ransomware as a service operators. LRQA has designed this service to assess an organisation's current preparation, security technologies and backup strategy to ensure that it can recover from a ransomware attack. This also assesses an organisation's security posture to prevent and detect attackers who are intent on widely distributing ransomware across the organisation's endpoints.

INCIDENT RESPONSE MATURITY ASSESSMENT

Provides valuable insight into your incident response capability covering, people, processes and technology. Part of the assessment includes the benchmarking of your current capability against a robust incident response capability framework. Analysis of the results will provide a set of recommendations that can be used as a roadmap toward improvement. The assessment will also include a review of your existing logging capabilities and make recommendations on how to enhance them in order to maximise the capability of any SIEM or SOC solutions that you have in place.

CYBERSECURITY FIRST RESPONDER TRAINING

This one-day training course is designed to prepare your cybersecurity team to act effectively and efficiently against a cyber attack. Ensuring that your team have the correct knowledge to be able to react to a cyber incident and can help minimise and ensure an expedient response.

PLAYBOOK REVIEW

Response to cyber incidents requires a well-planned and repeatable process. Through the use of playbooks, we make sure that your security team know what to do in a particular event. This engagement has been designed to support maturing security teams by reviewing in-use playbooks and providing guidance on best practice as well as how to optimise processes to reduce incident volumes.

THREAT HUNTING

This is a proactive service and compliments a penetration test to provide the organisation with the confidence that they have not been compromised. A penetration test is used to identify weaknesses in the organisation's infrastructure. A threat hunt can use the findings of this report to complete targeted 'hunting' to see if any of these weaknesses have been exploited and if an attacker is hiding in the infrastructure.

COMPROMISE ASSESSMENT

This is a reactive engagement when an organisation suspects that its infrastructure could have been compromised. This service can be called upon to provide confidence that a zero-day or critical vulnerability has not been exploited. This assessment has been designed to discover unknown security breaches, malware, and signs of unauthorised access.

ABOUT LRQA

LRQA is a leading global risk management partner.

Through our connected risk management solutions, we help you navigate an evolving global landscape to keep you one step ahead.

From certification and cybersecurity, to safety, sustainability and supply chain resilience, we work with you to identify risks across your business. We then create smart, scalable solutions, tailored to help you prepare, prevent and protect against risk.

Through relentless client focus, backed by decades of sector-specific expertise, data-driven insight and on-the-ground specialists across assurance, certification, inspection, advisory and training, we support over 61,000 organisations in more than 150 countries.

LRQA – Your risk management advantage.

GET IN TOUCH

Visit **LRQA.com** for more information or email **enquiries.uk@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

LRQA
Your Risk Management Advantage