Cyber **security**

KEY PERSONS ASSESSMENT

THREAT READY



LRQA.COM

LRQA

Your Risk Management Advantage

CONTENTS

3 What is a key persons assessment?

4 Why you need a key persons assessment

5 Key persons assessment objectives

6 The The cybersecurity threat landscape

7 How does cyber threat intelligence benefit you?

8 Why use LRQA for your key persons assessment?

WHAT IS A KEY PERSONS ASSESSMENT?

Forewarned is forearmed; the key persons assessment (KPA) provides a comprehensive review of the personal attack surface of key individuals and employees working for your organisation, as seen through the lens of a threat actor.

This approach replicates the process threat actors are known to undergo when seeking fresh targets of intimidation, blackmail and coercion to exploit and compromise an organisation.

A KPA provides a detailed review of the critical human elements of your organisation, uncovering gaps in personal cybersecurity defences, fake social and professional media profiles, and potentially sensitive online activity that threat actors may leverage to embarrass or coerce VIPs.

A KPA report empowers an organisation with an early warning of potential human-centric attack vectors, to which traditional technical assessments and tests are completely blind. No amount of advanced cybersecurity defences can prevent a motivated internal individual with capable external assistance from acting against your organisation's best interest. A KPA report provides early warning, key intelligence insights and mitigation against this attack vector.



WHY YOU NEED A KEY PERSONS ASSESSMENT

A key persons assessment (KPA) provides a highly-unique insight into how threat actors perceive both the organisation and its employees from a human-centric rather than a technical perspective.

This approach is invaluable to any organisation seeking to quantify the cybersecurity risk exposure posed to their key personnel and executives, and how online activities of key personnel can be leveraged by threat actors into an effective attack against themselves or their employees.

WHO IN MY ORGANISATION IS A TARGET?

HOW AND WHY ARE THEY LIKELY TO BE ATTACKED OR EXPLOITED?

ARE THREAT ACTORS DISCUSSING THEM ON THE DARK WEB?

WHICH ATTACKERS ARE LIKELY TO EMPLOY THESE TACTICS?

Specifically, any organisation that has received threats or targeted attacks against their key individuals or executives and seeks an understanding of how personnel are perceived by threat actors, would benefit from engaging a KPA.

LRQA threat intelligence analysts comprise combined decades of experience in both cybersecurity and military intelligence techniques, and utilise this broad base of expertise to effectively replicate the processes threat actors are known to employ. Armed with this viewpoint, an organisation can effectively seal the leaks in their public and personal media presences, and advise key executives on the positive defence of their online profile and activities.

KEY PERSONS ASSESSMENT OBJECTIVES

A key persons assessment will help your organisation to answer the following key questions, providing critical insights into your organisation.

Inform internal policy regarding social and professional media, threat actor contact procedures and disciplinary process in light of real-world examples and quantifiable data.

Immediately identify relevant real-world content, whether posted by an executive or a cyber or physical attacker, anywhere in the world.

Identify online activity associated with key persons that threat actors may weaponise against your company or executives.

Establish the probable forms a personal attack against key persons could take. Prepare both immediate countermeasures and long-term training objectives to manage this risk.

Identify fake accounts on social and professional media impersonating key brands, persons and executives, potentially indicating threat actors preparing a confidence attack.

Highlight active threat actors and malware campaigns being used in your industry and against your peers.

Detect exposed credentials of your key persons and executives which could be used to gain access to internal resources.

Detect data leakage regarding key persons through information uploaded to paste sites, forums and criminal dark web sites.

360° EXECUTIVE THREAT ASSESSMENT

KEY ASSESSMENT COMPONENTS



- OPERATIONAL SECURITY
- PUBLIC RECORDS
- TRAVEL VULNERABILITIES
- INFORMATION LEAKAGE
- FINANCIAL FOOTPRINT
- PATTERN OF LIFE
- DIGITAL PRESENCE
- RELATIONSHIP SECURITY

THE CYBERSECURITY THREAT LANDSCAPE

Many threat actors, from the simple hacktivist to sophisticated organised criminal groups, teams are increasingly targeting humans within an organisation rather than the technical footprint of the organisation itself.

As cyber defences improve and cyber awareness expands, it is the key executives and critical employees within a target that represents the most expeditious route for threat actors to gain a foothold.

Cyber extortion is one such attack route, generally utilising email or social media-based ransom demands. Threat actors locate personal or sensitive information about a key executive or manager. This can be in the form of personal information about spouses and offspring, photographs of compromising postings or online memberships. Also, in the age of public data breaches, many reports have surfaced of the targeting of individuals via this exposed data, for example the high-profile data breach of the popular adult website Ashley Madison.

Once a compromising vector is discovered, the individual is contacted and threatened with the release of this personal information to their industry contacts, family, and friends if certain tasks are not performed. These illicit 'assignments' can range from simple cryptocurrency extortion for retrieval of internal corporate data, spying on executive communications channels, or implanting hostile malware within private networks.

This variety of human-centric attack vector compels capable individuals to avoid detection and adapt to their organisation's defences, effectively creating a highly motivated and persistent threat actor agent already inside an organisation's perimeter.



HOW DOES CYBER THREAT INTELLIGENCE BENEFIT YOU?

Fraud prevention, risk analysis, and other high-level security staff are tasked with understanding the current threat landscape for their organisation. Threat intelligence provides key insights on threat groups, targets, motives, and their tactics, techniques, and procedures (TTPs).

Security operations teams are routinely overwhelmed by the volume of alerts they receive from monitoring appliances and external data feeds. Threat intelligence can be combined with the security solutions already in use, helping defenders quickly prioritise alerts and identify threats.

Security testing scenarios for ‘red team’-based assurance activities are best realised informed by real-world intelligence about your organisation. Combined with current trends in attacker TTPs and aligned to the industry-standard Mitre ATT&CK Framework, cyber threat intelligence brings a level of concrete

Vulnerability management teams are tasked with accurately prioritising the most critical exploits and weaknesses affecting technical infrastructure. Combining vulnerability data from your organisation with threat intelligence data provides valuable context, empowering defenders to differentiate imminent threats from those that pose a lesser risk.

Brand and fraud prevention teams can meet great difficulty in prompt discovery and takedown of infringing and criminal phishing domains, due to the sheer size of the internet and the wide variety of registrars and agencies across the globe. LRQA’s threat intelligence services can readily detect these fraudulent domains, and offer rapid takedowns.



WHY USE LRQA FOR YOUR KEY PERSONS ASSESSMENT?

LRQA's threat intelligence analysis represents a high bar for both quality of output and intelligence confidence.

All findings are extensively curated and reviewed by experienced analysts; no automated or 'bulk' findings are included in this analysis unless especially relevant to an intelligence objective. The results presented are of a sufficient standard to support both operational and strategic-level decision-making.

The assessment will be conducted by LRQA's team of CREST-certified cyber threat intelligence analysts. Our team are adept in identifying risks presented by online and public activities, and viewing these results in the context of modern threat actors' behaviours, techniques, and objectives.

To safeguard both individuals and the organisation, LRQA analysts follow strict protocols of redaction to ensure individual privacy is fully respected, and only details critical to the investigation are included in the results. Our priority is always to enhance and uphold the privacy and liberty of your organisation and its individuals.

We can provide threat intelligence coverage across multiple intelligence domains on an ongoing basis, ensuring critical findings are detected early and reported swiftly and clearly.

Whether your requirement is at a technical indicator (tactical), general awareness (operational) or board-level decision making (strategic) level, LRQA deliver the right outcome for your organisation.



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