WHO WE ARE

Formed in 1996, Netcetera is one of Europe's leading Web Hosting service providers, with customers in over 75 countries worldwide.

In partnership with Riela Cyber, the Security Operations Centre (SOC) also based in Ballasalla, Isle of Man, we will provide you with bespoke cyber security solutions which have scalability at their heart.

With a unique blend of best in class cyber security software managed by our team of cyber security experts, we are proud to help businesses safeguard their operations.

OUR APPROACH

Comprehensive cyber security is more than protecting data and detecting breaches of the perimeter.

The people and processes that operate your technology are critical to your business and can pose as much of a threat as a system vulnerability.

Our approach is aligned with the NIST cyber security framework, designed to help businesses manage their cyber security and reduce their cyber risk. Our partnership enables us to achieve this by leveraging the strength of both MSP and MSSP solutions.

MSP vs. MSSP

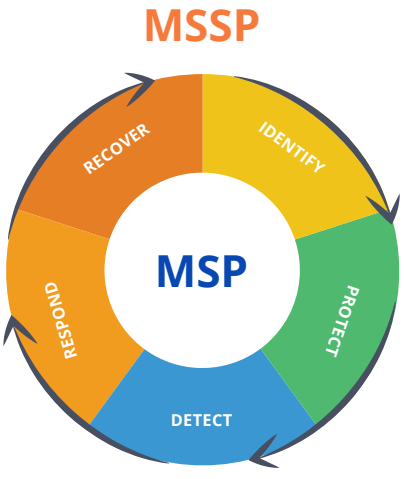
IT Support Managed Service Providers (MSP) are focused on the health of the technology and digital assets that support your business operations. Their priority is to provide high system availability and respond to support requests.

Managed Security Service Providers (MSSP) are focused on the security of technology and digital assets. Their priority is to detect and respond to cyber security threats. This proactive risk-based approach ensures that existing security risks are identified before the effective protection measures are applied.

A POWERFUL COMBINATION

Technology that powers your business should not pose a risk to your business operations, reputation or revenue. Combining the services of MSP's and MSSP's can deliver exceptional resilience and provide your clients and suppliers with the confidence that their data is protected.

Improving a companies cyber security posture requires a layered approach. Not only to create a protective layer around the technology but also to address the five functions of the NIST cyber security framework.



SECURITY SERVICES

Our comprehensive and tailored security solutions can protect the technology at the core of your business. Depending on the capabilities and scope of your IT Support MSP, we can blend security controls and defences into every system, process and employee to build effective safeguards.

KEY:	Protect	Respond	A typical MSP	✓
Identify	Detect	Recover	Riela Cyber & Netcetera - MSSP	✓

ENDPOINT MANAGEMENT

Typically, MSP's have to test Windows and other updates prior to security patching - wasting time and money. Our enhanced endpoint management will keep your devices fully patched automatically, drastically reducing vulnerabilities and attack vectors.

Our SOC integrated system monitors performance and raises notifications of workstation & server issues often before the users have noticed a problem.

Full security suite	✓	✓
Root cause analysis	✓	✓
Corrective action	✓	✓
Remote support desk and helpdesk SLA	✓	✓
Automated updates		✓
Performance monitoring		✓
Computer resource monitoring		✓
Security Operations Centre (SOC) integration		✓
Automated resolutions for repeating problems		✓

Remote support is simple, and repeating issues are given automated resolutions.

PRIVATE EMAIL HOSTING

Riela Cyber ensures at least 5-layers of email protection from different vendors to maximise defences.

All high-level protocols are correctly configured while our monitoring tools correlate this with other activity to help identify Advanced Persistent Threats.

Private secure email hosting	✓	✓
Managed mailbox migration	✓	✓
Domain name management	✓	✓
Mobile device access management	✓	✓
Mail flow security monitoring		✓
Mail flow security reporting		✓
5-layers of multi-vendor defenses		✓

Check your the security of your outbound email connection. Send a blank email to: dmarc@emailsecurity.im

NETWORK TRANSPARENCY

If there was a breach, would you know? What impact could a breach have on your systems? Your clients?

Riela Cyber monitors all traffic and assets on your network, leaving no weak links, quickly identifying suspicious activity and all known vulnerabilities.

Remote network management	✓	✓
Remote mitigation service	✓	✓
Hardware performance monitoring		✓
Vulnerability scanning - external		✓
Vulnerability scanning - internal		✓
Security event logging		✓
Security Operations Centre (SOC) integration		✓

Fully integrated into our SOC, Riela gives advanced warning of hardware problems and failures, reducing system downtime significantly.

NETWORK DEFENCE

Hackers are experts at avoiding detection and often stay under the radar.

Our state of the art Security Information and Event Management (SIEM) tools enhance network defences by taking a deep dive into network traffic and events.

Secure network design and deployment*	✓
Detection and prevention of network intrusion	✓
Advanced event logging and threat analytics	✓
Advanced network traffic behaviour analytics	✓
Managed malware protection	✓
AI real time network monitor	✓
Security Operations Centre (SOC) integration	✓

Correlating this with Behavioural Analysis and Artificial Intelligence immediately highlights unusual activity and quickly identifies Advanced Persistent Threats.

EXTERNAL THREAT MANAGEMENT

If a bad actor wants to attack, how can we make it harder for them?

We hunt for all the information a bad actor could discover, then build defences against them.

- Threat hunting ✓
- Intelligence ✓
- Extensive dark web monitoring ✓

INTERNAL THREAT MANAGMENT

If an intruder or company insider were leaking data, would you know?

- Insider threat detection ✓
- Advanced data loss prevention* ✓

Our SOC monitors data leaving your business and spots potential abnormal behaviour and traffic patterns that could indicate an intruder or disgruntled staff member before it has a chance to have a detrimental impact.

A recent IBM report found that it took an average of 280 days for organisations to identify and contain a data breach.

THREAT OFFENSIVE

Monitoring is one thing, but we need to stop attackers in their tracks before there is a chance of damage.

- AI real time network autonomous response ✓
- Offensive threat hunting ✓
- Offensive intelligence ✓

Our AI autonomous response tool will effectively contain in-progress attacks in the shortest period of time.

Acting in seconds, it is critical in stopping the onset of ransomware and other fast-moving threats from inside your digital environment.

In order to stop bad actors in their tracks, we will profile your attacker, gain leverage against them, and find ways to neutralise the threat.

RISK ASSESSMENTS

The range of Cyber Assessments we offer with Riela Cyber enables transparency, visibility and insight into your online estate. Before creating a bespoke plan, it is important to have a snapshot of your current security posture, enabling us to provide you with the services you need, and nothing more.

WHAT WE OFFER

Cyber Essentials is a government-backed and nationally recognised certification built to recognise your secure services.

- Cyber Essentials (Assessors) ✓
- IASME Governance (Assessors) ✓
- Penetration Tests ✓
- Bespoke Assessments ✓

Working with the National Cyber Security Centre (NCSC), the certification helps businesses by assessing performance against five vital security controls. To take it a step further, the IASME Governance certification has the benefit of including GDPR requirements, the five essential security controls of Cyber Essentials, plus more.

The certification offers businesses specific advantages to assure optimal cyber security compliance, acting as a direct alternative to ISO 20071.

Penetration Testing provides maximum insight into your existing security measures and controls. The Riela Cyber penetration testing service is conducted in a fully controlled environment, as to not disrupt your services.

CYBER ESSENTIALS

CYBER SECURITY TRAINING

Our comprehensive and tailored security solutions work to protect the technology at the core of your business. Depending on the capabilities and scope of your IT Support MSP, we can blend security controls and defences into every system, process and employee to build effective safeguards.

WHAT WE OFFER

One of the biggest causes of cyber security incidents is human error. By simply focussing on tick-box exercises, traditional training does not target human behaviour to reduce error.

- CybSafe Online Platform ✓
- Bespoke Cyber Security Training - On-Site ✓
- Bespoke Cyber Security Training - Virtual ✓
- Cyber Security Awareness Quizzes ✓

This is why our cyber security training moves beyond traditional methods. Using personalised, scientifically-proven nudges, reminders and support, our program works to build your first level of cyber risk defence and response through your people.

We can provide training for your network administrators, staff and stakeholders to help ensure that the risks are minimised.

Bespoke cyber awareness training can be created and distributed to your organisation via the platform Kahoot! to increase engagement and learning.

Riela Cyber has also partnered with CybSafe to provide NCSC and CIISec accredited cyber awareness training.

CYBSAFE

EMERGENCY RESPONSE

Whether you are an existing client or not, our team are available to help if you or your business suffers a cyber event and need cyber security experience and expertise to guide you to safety. Working with Riela Cyber, we offer a 1-hour free consultation to provide information about the cyber event and recommended courses of action prior to committing to a service agreement.

Our recommendation is to proactively protect your digital infrastructure. Securing a bespoke blend of cyber security services to suit your business will lessen the likelihood of needing to use our emergency response facility. Nevertheless, the threats and risks are always evolving and provide no guarantees that your security measures will prevent all cyber attacks. However, businesses that invest in their cyber security defences significantly reduce the impact and damage a cyber event can have. Particularly, when compared to businesses who do not actively protect themselves, their clients or their data.

STATISTICS

The numbers associated with the impact of cyber security events are sobering. It's reported that:

£87b

the total cost of cyber crime in the UK since 2015.

1.5m

the number of businesses affected by cyber crime in 2019. Up from 755,000 in 2015.

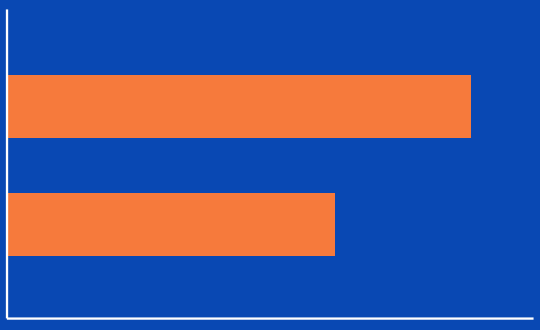
25%

of UK businesses were targeted by cyber criminals in 2019, up from 13% in 2015.

1/3

of all breach responsibility was with the employees, whether it was through malicious intent, neglect, or genuine mistakes.

Accounting for damaged assets, financial penalties and lost productivity, in 2019 cyber events affected:



87% of large companies consisting of at least 250 employees.

62% of small companies consisting of 11-50 employees, rising from 28% in 2015.

Whether it's a spear phishing attack, malware or lack of employee awareness, the impacts of a cyber event can be devastating to businesses of any size. Our mission is to use our experience and expertise to prevent our clients from becoming another statistic.

SOURCE: BEAMING REPORT

GET IN TOUCH

Netcetera
The Dataport
Ballasalla
Isle of Man
IM9 2AP

+44(0) 3330 439 780
www.netcetera.uk
hello@netcetera.co.uk