CYBER STARS

Cyber Stars Initiative

INTQUAL PRO

CYBER
STARS

What is Cyber Stars?

Now delivered in over 30 countries, the Cyber Stars Initiative is an effective and sustainable solution to cyber security awareness. It is estimated that over 90% of successful cyber breaches are facilitated by human error. The Cyber Stars Initiative was developed to help reduce the cyber threat to businesses that is enabled through a lack of employee awareness and confidence to act. The Cyber Stars Initiative is far more than just a training course, or even a qualification, it is proven to support sustainable culture change and increases organisational resilience to cyber threats.

Built upon three crucial pillars, Cyber Stars provides a holistic solution to cyber security awareness in an ever evolving landscape.

- Profile Human Risk and Behaviours – Utilising state-of-art profiling solutions to measure and quantify human risk, Cyber Stars identifies the individuals, departments and locations within your business that are most vulnerable.

- Training to Enable Positive Behaviour Change – The Cyber Stars Initiative has been developed by a combination of technical experts, risk managers and behavioural psychologists to ensure maximum personal engagement and measureable behavioural change

- Sustain Awareness Levels – Cyber threats evolve on a daily basis and it is critical that employees are provided with an opportunity to remain current with threats. Cyber Stars 365 provides an efficient and effective opportunity to imbed cyber security knowledge within everyday working practices without a negative impact on productivity or operations.

Profiling

Cyber Risk Profiling

Understanding your Cyber risk profile is an essential precursor to the implementation of an effective cyber security strategy. Training must be structured, focused and relevant, with clear metrics of success. Our risk profile services allow an organisation to identify high risk user groups, locations and business specific vulnerabilities. With expertise and exposure to the most current cyber threat techniques, our team replicate methods used by cyber threat groups to understand ways in which your organisation is most susceptible to cyber threat.

Digital Footprint Profiles

Social Engineering is the fastest growing Advanced Persistent Threat (APT) technique for malicious actors seeking to exploit individuals across all regions and professional sectors. Over 85% of all successful attacks against businesses, are email based and involve exploitation of digital footprints. Our individual digital footprint grows each year and increasingly provides an opportunity for blackmail, extortion and other types of criminality. Social engineers and cyber criminals have discussed common methodology in terms of “target” identification and many demonstrate that it takes less than 5 minutes to find a range of exploitable opportunities. Malicious actors will exploit those individuals within an organisation that appear most vulnerable, often outweighing a requirement to access specific systems or data sets. This service helps to identify individual vulnerabilities and provides individual and specific remedial training to improve cyber security posture. Our Digital Footprint Analysis is conducted by investigative experts with detailed knowledge of criminal methodology. Footprint Reports are very popular with Board level executives seeking to identify specific and personal vulnerabilities that could lead to them being exploited by cyber threat groups and the report process provides bespoke and personally relevant to the subject of the report.

Dark Beam Cyber Exposure Reports

Dark Beam is a multi-layer search engine (surface, deep and dark web) which enables us to ascertain existing corporate leakage across a range of pre-determined criteria. Dark Beam allows us to see your vulnerabilities as a malicious actor would. By understanding your organisation's footprint and exposure we are able to provide an effective human risk profile across the organisation. Dark Beam is used by a range of organisations to measure their own internal risk, yet also risk factors associated with supply chain and customers. By using Dark Beam we can see the vulnerabilities of your organisation as a hacker would. Regular monitoring of an organisational digital footprint and external visibility of threats allows efficient response and mitigation as new exposure is identified.

Spear Phishing Assessment

At the Cyber Stars Initiative we use state of the art Spear Phishing software to create organisation, role or departmental specific spear phishing emails that far better represent the real criminal threat. We are able to identify your overall business risk, as well as departmental or role specific risks. Our team of cyber risk specialists will analyse your cyber risk profile based upon factors such as geographic distribution, site specific system access and mobile working threat, helping to not only identify training need, but also shape effective policy development and implementation. It is essential to remember that phishing tests should be far more than click rate. Our testing allows us to analyse the risk profile of your business, considering device use, geospatial factors and behaviours of employees with access to critical systems.

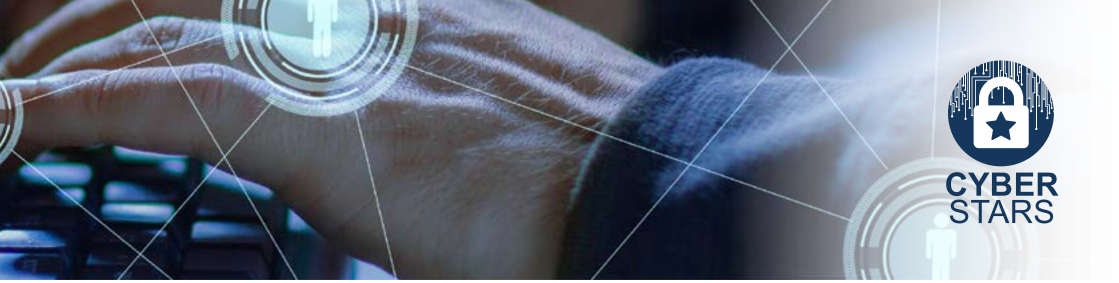
Training

Cyber Stars Content

Cyber Stars training has been delivered successfully in over 30 countries and over 250,000 individuals have participated in one of our training programmes. Each Cyber Stars course is bespoke, as sector and organisational threats are often subtly different. This impacts our curriculum to ensure it is relevant and provides actionable behavioural changes that will make a difference to both the personal and corporate environment. Threat types used and case studies included in the programme will always be relevant to sector and ensure increased levels of engagement through learner recognition of relevance. Regardless of prior knowledge and exposure to cyber security threats, the programmes focus specifically on user behaviour, how to identify, mitigate and effectively respond to cyber threat in both a personal and working environment.

Key learning topics include:

- The Scale and Evolution of Cyber Threat
- Threat Actors and Motivations
- Threat Techniques (Social Engineering, Malware, Network Attack, Physical Access)
- Home and Mobile Working Threats (Wifi, VPN, Encryption, USB, password security)
- Social Media Safety (Digital footprint leakage and protection)
- Incident Response and Business Continuity (in scoping with organisation for messaging)
- Supply Chain Threat (if relevant to business model)
- Policy Development and Implementation (in scoping with organisation for messaging)



Cyber Stars "Lite"

Not every employee needs to be a Cyber Star, indeed the Initiative was developed to ensure that Cyber Stars spread threat knowledge and create a natural culture of awareness within the workplace, yet there is still a requirement for others to be effectively trained and enable them to engage with cyber risk. We have found that traditional mandatory training is rarely effective or retained and have developed this programme to provide a more modern, current and engaging alternative to mandatory awareness training. A fully accredited programme, Cyber Stars Lite involves education through fully immersive film. Through 45 minutes of film based education, learners will engage with a range of cyber security subjects in a manner that maximises engagement, understanding and retention. With the completion of an assessment we are able to provide a clear metric to an organisation of where individuals have achieved or any areas in which require more specific development.

Cyber Stars Lite is available in 12 languages and has currently been delivered successfully to 200,000 learners in over 25 countries.

Cyber Stars 365

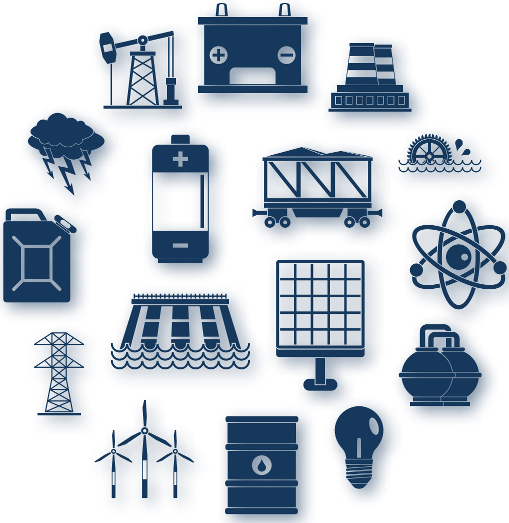
It is a common misunderstanding to think that we must retrain all of our staff each year in exactly the same way, often generating increasing resentment and reduced levels of engagement. With cyber security, there is a requirement to provide metrics for understanding, which does not necessarily require a repeat of training. With this programme of continuous assessment, staff receive three questions per week across the breadth of cyber security topics. As questions are answered correctly, the system will recognise the level of knowledge retention and gradually reduce and then stop asking questions. For those that answer questions incorrectly, individual pieces of specific education can be provided to increase understanding and retention and then questions repeated in the following weeks. Cyber Stars 365 allows an organisation to provide a snapshot of understanding and risk at any given time, identifying those with legitimate training needs, without providing additional unnecessary training to those that already can demonstrate an effective level of competence. Cyber Stars 365 engrains awareness culture within the workforce yet requires minimal interaction or operational disruption, whilst providing 365 day metrics to stakeholders that provide visibility of engagement and cyber security knowledge, visualising human risk factors and driving broader engagement strategy.

Cyber Stars CNI

(Critical National Infrastructure)

Cyber Stars is the first education and awareness programme with an official qualification in cyber security awareness for those working within Critical National Infrastructre. As the cyber threats to CNI continue to increase and evolve it is essential that those with access to and responsibility for keeping Operational Technology secure, to fully understand cyber security threats within the relevant and specific context. Generic IT based cyber awareness training often misses the requirement for those working in more operational technology roles and our curriculum has been developed with leading providers of CNI in the United Kingdom to ensure complete relevance to those working in role. Cyber Stars CNI curriculums are specific to individual sector risks and support NIST Directive requirements associated with cyber security awareness within CNI.

Two Cyber Stars OT programmes are now available, delivered by experienced cyber CNI experts and practitioners at both Awareness and Advanced levels.



Cyber Stars CNI - Foundation Level

1 day programme covering:

DAY 1

- Defining the difference between IT and OT
- Evolution of cyber threats
- Threat groups (inc insider threat)
- Defining vulnerabilities (regular and zero-day)
- OT Cyber risk assessment
- Vulnerability identification and cyber attack chain
- Social Engineering attacks
- Network attacks
- Supply chain and Third Party
- Systems and Data and the consequences of their loss
- Compliance and Regulatory Frameworks

Cyber Stars OT – Advanced Level

Each course is specific to organisational needs, key content often includes:

DAY 2

- Understanding attack tools and methodology
- Shodan
- SCADA Stranglelove
- What resources are available to understand the vulnerabilities?
- Threat intelligence
- Network segregation (airgaps, Industrial IoT)
- Incident response
- Optimising OT networks
- Wireshark

DAY 3

Practical use and application of the below:

- Kali Linux
- Metasploit & Metasploitable
- Nmap
- OpenVAS
- John the Ripper
- Aircrack-ng

For more information please contact

enquiries@intqual-pro.com

www.intqual-pro.com/cyber-stars