LULWORTH STONE

OFFENSIVE CYBER SECURITY

WE NEED DIVERSITY OF THOUGHT IN THE WORLD TO FACE THE NEW CHALLENGES

TIM BERNERS-LEE

INTRODUCTION

LULWORTH STONE HAS BEEN FORMED AROUND A CORE TEAM OF HIGHLY EXPERIENCED **UK INTELLIGENCE OFFICERS** AND **SPECIAL MILITARY UNIT OPERATORS**

Each member of our team has a significant depth of knowledge and skill operating across a broad spectrum of high physical and digital threat environments, both defensive and offensive.

The Lulworth Stone team have worked in the most discreet parts of Government with the highest level of security clearance, providing our clients with absolute assurance of discretion in everything we do.

This unrivalled experience is being offered to exclusive, discreet clients to provide digital and cyber threat awareness, mitigation, and security implementation. With a personal approach and bespoke solutions, Lulworth Stone can provide clients with a trusted team to support all their offensive cyber security mitigation procedures.

A PERSONAL APPROACH WITH BESPOKE SOLUTIONS FOR YOUR ORGANISATION

Our knowledge of existing and emerging technologies, as well as real-world experience at the highest threat levels, provides a unique opportunity to get ahead of all digital threats, especially in the challenging global climate we find ourselves in.

HOW WE **CAN HELP**

OFFENSIVE CYBER SECURITY HOW IS IT DIFFERENT?

HACKERS AND CRIMINALS ARE CONSTANTLY ADAPTING THEIR TRADECRAFT

It is in their interests to find new ways in which they can evade your defences, bypass your security protocols, steal your valuable data and disrupt your operations. The new tactics, technologies and methodologies available to attackers mean the traditional approach of defence only cyber security isn't enough to remain safe.

The classic approach to cyber security takes the defensive stance, where organisations and individuals alike utilise basic Anti-Virus (AV) software and Firewalls to attempt to protect their networks and their data. These methodologies have become out dated as hackers have become more sophisticated.

A DEFENSIVE STRATEGY ALONE WILL NOT KEEP YOU SAFE. YOU MUST GO ON THE OFFENSIVE

Today hackers use techniques and methods that mean a defensive cyber security approach will only hold them at the gate. The modern hacker has become adept at climbing walls and digging tunnels. An offensive cyber security system will seek out vulnerabilties, making an attack far less easy for hackers whilst taking the fight back to the hacker. Using evidential techniques to disrupt an attackers ability to operate and open them up to a criminal investigation by the authorities goes beyond the symptomatic defensive approach and deals with the cause of the criminality.

In the game of cyber security – a defensive strategy alone will not keep you safe. **You must go on the offensive.**

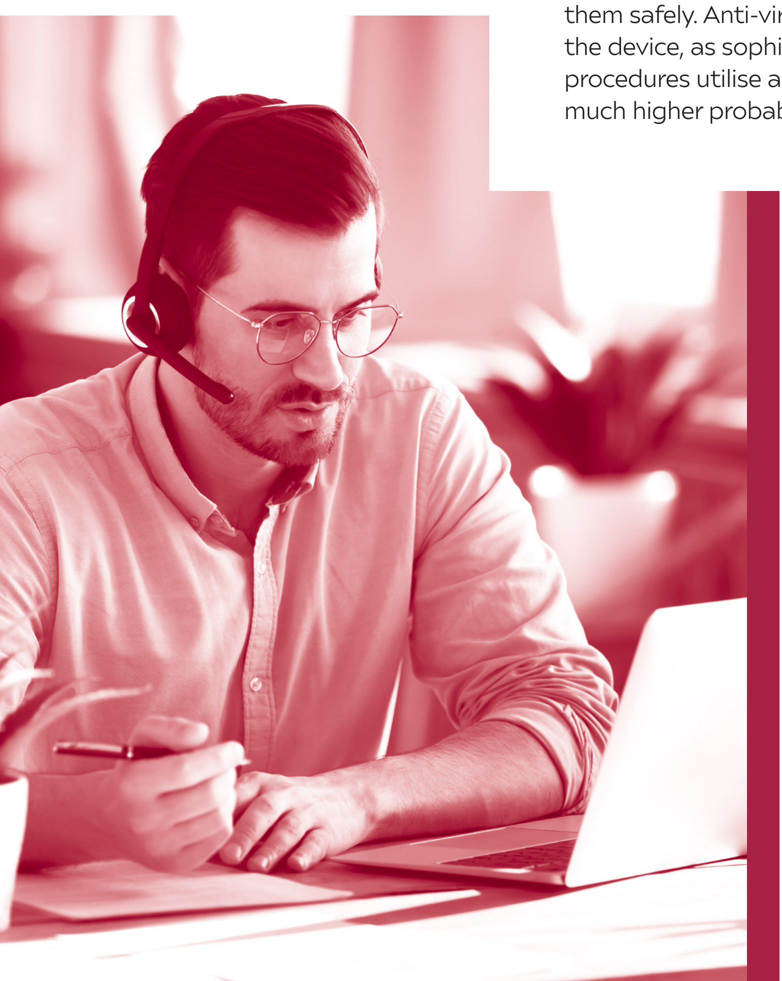
HOW LULWORTH STONE CAN DELIVER FOR YOUR ORGANISATION

Lulworth Stone's collective experience of delivering offensive cyber techniques defending our national security means that we are uniquely placed to provide security and assurance to clients in the commercial world.

VULNERABILITY ASSESSMENT

In this post-COVID world, it is very common for individuals to work remotely, which is an enormous opportunity for hackers. Malware can often masquerade as legitimate processes running on digital devices, so finding **Indicators of Compromise (IOCs)** can be challenging. Lulworth Stone operatives deliver a holistic service that begins with a vulnerability assessment.

Our experienced team know where to look for these IOCs and how to remove them safely. Anti-virus software should not be relied on as the sole defender of the device, as sophisticated malware can evade the techniques used by AV. Our procedures utilise a layered approach with a vulnerability assessment that has a much higher probability of finding malware.



WE CONDUCT THIS ASSESSMENT AT ALL POTENTIAL NODES INCLUDING:

- Across all networks
- All company computers and servers, including those external to the company premises that bridge the firewall
- All company phones and tablets, including any that cross the firewall
- Online presence and cloud servers
- In the home where it connects to work (especially important for seniors who oftern work from home and where individuals work remotely)

ENSURING THE NETWORK IS ROBUST FROM POTENTIAL ATTACKERS

NETWORK VULNERABILITY

With the average number of devices connected to a home network increasing due to the proliferation of the Internet of Things (IoT) and smart devices, so too has the attack surface for malicious actors to leverage.

Many smart devices are configured to plug and play for consumer ease, but this usually means default passwords that rarely, if ever, get changed. We can offer a service to check the resilience of any network and make the necessary changes to ensure the network is 'hardened' to attacks.

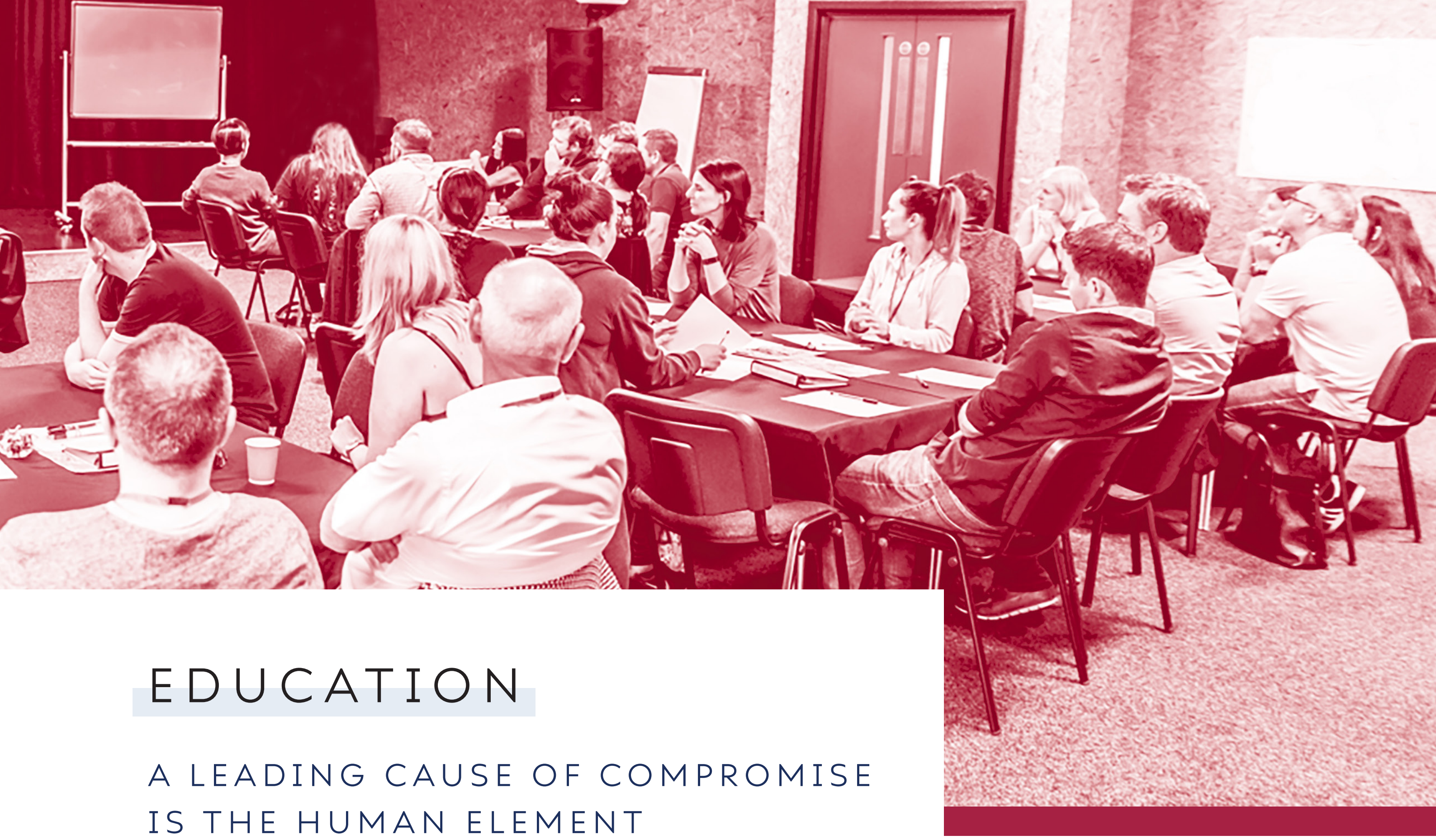
- Home network security including IoT
- Virtual Private Network
- Computer/Laptop security uplift
- Mobile device security uplift and addition of security applications
- Full secure system and device backups in the event of loss or compromise

SOFTWARE VULNERABILITY

Not applying security updates, known as patching, is one of the leading reasons why devices are compromised. With the sheer volumes of applications running on modern devices it is easy to neglect vendor updates when they are released. We can implement monthly patching policies to ensure that all devices have the best protection in place.

- Monthly compromise assessments and updates

IMPLEMENTING POLICIES TO ENSURE THE BEST PROTECTION



EDUCATION

A LEADING CAUSE OF COMPROMISE IS THE HUMAN ELEMENT

The most sophisticated hackers engage in low technology solutions but conduct detailed social engineering using social media and phishing techniques that lead to the compromise of your networks. People are commonly aware of the classic phishing attempts, whether through email or text messaging. These types of hacking attempts are relatively easy to see through, however, high profile examples such as the attack on BAE SYSTEMS and the NHS show how these can be highly targeted on specific individuals working within those organisations.

Social engineering and human targeting are the secret weapons in the hacker's arsenal and its use is becoming more prevalent, especially in consideration of how much information, both private and commercial, people share online.

Staff may also inadvertently connect their compromised devices to estate networks, which could lead to a compromise of that network.

The best way of combatting this threat is by educating your staff to understand what the threat is, how it relates to them and what they can do about it.

We have developed several courses, from Introduction to Cyber Security for representatives of your organisation to annual check-ups, that mean we can shore up the significant risk posed to your business through social and human engineering.

Within large corporations, staff training is seen as an integral element of protecting the business from a cyber-attack, but employee size should not be a limiting factor when protecting your network. We can train your staff to be vigilant to the indicators of compromise and how to best establish good cyber hygiene throughout the estate. We can also carry out an assessment of your online presence. This will include a report on open-source information that will highlight if your credentials have ever been compromised and are available to the hacker community.

COURSES DESIGNED TO DEMYTHIFY AND AID UNDERSTANDING OF THE ONLINE SPACE

- Understanding of systems networks and cyber threats
- Best practise cyber security procedures to work with the clients' requirements
- Client online exposure, data breaches and potential threats
- Staff training protocols and procedures of training to ensure staff can keep themselves safe and secure

COMPROMISE PROCEDURES

SHOULD THE WORST HAPPEN, LULWORTH STONE CAN HELP YOU MITIGATE ANY POTENTIAL HARM

If a cyber incident comes to fruition, it is imperative to contain the issue and seek professional assistance as soon as possible.

We will follow ACPO (Association of Chief Police Officers) guidelines around maintaining evidence should it be required for any subsequent legal investigations. In this instance, our service will rapidly deploy to conduct a forensic investigation.

We use bespoke software packages that finds the provenance of an attack, where our operatives can ultimately identify its source. Not only does this form an evidential chain which would be useful to a police investigation, but also gives us the opportunity to launch our own disruptive methodologies to ensure that the hackers are unable to continue their operation.

Our systemic approach fortifies your business continuity as secure back-ups are made available rapidly, we will aim to provide replacement devices and reinstate the back-ups to allow you to continue to operate with minimal disruption.

- Quick reaction deployments to assist in any cyber security breaches
- Forensic investigation of compromised devices
- Securing of the evidential chain to offer best chance of prosecution if attribution can be identified
- Source new devices and install the backup to ensure, a return to business as usual as quickly as possible.
- Recovery of data from old devices where passwords have been forgotten

HOW WE WORK FOR YOU

BESPOKE SOLUTIONS TO SUIT ANY COMPANY OR ORGANISATION

Trust is a significant element of our work. We develop a close working relationship with our clients and to ensure we are not only delivering the best possible outcome, but to give peace of mind that your sensitive data is not compromised. Our clients are diverse, ranging from UK Government agencies to small business enterprises with only a few members of staff. No one client is the same and we adapt our offer to meet your specific needs.

Companies that work in the digital space with cutting edge technologies and limited numbers of employees need a very different offer to large complex process orientated businesses with high numbers of employees and older administrative systems.

STEP ONE

VULNERABILITY ASSESSMENT

Our initial offer is a vulnerability assessment. We provide an in-depth assessment of your organisation and highlight areas that need to be addressed.

STEP TWO

OFFENSIVE CYBER SECURITY PROPOSAL

Based on our findings, we build a bespoke proposal that offers the most cost effective methods to keep your organisation safe in an increasingly hostile digital environment.

STEP THREE

IMPLEMENTATION

We deliver on our bespoke proposal, from training courses to practical services, to keep your organisation safe from malicious cyber threats.

ARMED FORCES COVENANT

PROUDLY SUPPORTING THOSE WHO SERVE.

LULWORTH STONE

TACTICAL TRAINING SYSTEMS

WWW.LULWORTHSTONE.COM