UPGRADE
IT expertise that saves you time & money

in partnership with

ecsc
more secure

UNDERSTANDING YOUR CYBER SECURITY CHALLENGES

04:00
San Francisco
07:00
New York
08:00
São Paulo
12:00
London
13:00
Berlin
GUARDED: Under Investigation
Automated dumb scans against systems
Identified malicious activity with low impact.
New malware samples identified.
LOW: Routine

1 DEALING WITH A CYBER SECURITY BREACH

> Thank you for the **fantastic response** to our emergency this morning...to have an engineer on site within two hours is quite astonishing
>
> **Business Support Manager, Legal Practice**

YOUR CHALLENGE

Before you can even think about effectively managing a potentially damaging cyber security breach, it is worth simply understanding what your detection capabilities really are. With so many breaches discovered too late to prevent data loss, the benefits of early detection are clear.

Whether you are planning ahead of time, as is recommended, or in the middle of an incident, having the right team with genuine breach response expertise is critical. For most organisations, having this expertise in-house is very unlikely.

With GDPR bringing mandatory breach reporting within 72 hours, you now have no option than to engage with the Information Commissioner's Office (ICO), and deal with their increasingly technical investigations.

As more and more breaches become public, you will also need to build expertise in communication with the media, your staff, customers, and other organisational stakeholders.

THE ECSC APPROACH

With over 18 years' breach response experience, ECSC can help manage all aspects of breach investigation, containment and recovery.

The foundation of ECSC's incident response service is a full 24/7/365 response service, accessible through retainers and levels to fit all organisation sizes.

An incident response can be from straightforward telephone and email advice and guidance, to a full on-site team, equipped with the latest cyber security technologies that link your systems to the ECSC 24/7/365 Security Operations Centres.

The ECSC team help co-ordinate all aspects of breach response, including essential communications with all stakeholders, including the ICO.

KNOWING HOW SECURE YOU ARE

2

> We searched for leaders in the field of Information Security and found ECSC... we conducted a review of suppliers and ECSC came out **far ahead** of the other organisations
>
> **Operations and Security Management, Fleet Management**

YOUR CHALLENGE

For many organisations, the operational IT team do not have sufficient understanding of cyber security to assess the adequacy of your current cyber security protection. Often, where expertise does exist, communication to management to establish clear priorities for improvement never effectively happens.

Also, most organisations have little or no cyber security breach detection capability, assuming simple anti-virus protection will do the job. A simple 'we have never had a breach' statement often covers ignorance as to real weaknesses and breaches that have remained undetected.

Many systems have never had meaningful cyber security penetration testing, and, in many cases, testing results are not properly assessed and acted upon.

Following a serious breach, with data loss, the worst possible finding for the ICO is that the organisation knew about security weaknesses and had not acted upon this knowledge.

THE ECSC APPROACH

The starting point of any effective cyber security assessment is to understand your organisation, your critical systems, and the realistic threats that you face.

Then, a prioritised programme of testing can be implemented to give you clear, objective information regarding your vulnerabilities, whether technical or people related.

ECSC has, over many years, pioneered new approaches to cyber security testing, from being the recognised authority in social engineering testing, to clear technical pass/fail reporting, and custom Cyber Security Review methodologies.

In addition, the 'full service' approach of ECSC means we can also help you with critical vulnerability remediation.

3 FINDING TECHNOLOGIES THAT ACTUALLY DELIVER

> A UK Government survey found **93%** of large businesses say cyber security is a **high priority**
>
> Cyber Security Breaches Survey

YOUR CHALLENGE

We live in a world where the IT product and solution hype isn't always matched by the reality. Cyber security is no different, with magic solutions promising to remove the need for employing experts appearing (and disappearing) every year.

It is worth remembering that 'new' and 'proven' are very different. Designing an impressive product demo is quite easy; giving you meaningful improvements to your cyber security is a different challenge.

Many products are mis-sold, without the necessary supporting management expertise to help you maximise their effectiveness in your environment. Vendors tend to focus on 'feature count', rather than adding meaningful cyber security improvements that work in real-life environments.

The golden rule of cyber security is that you cannot replace the need for real people expertise applied to understanding your systems, the threats you face, and the strategies necessary to make you more secure.

THE ECSC APPROACH

With 18 years of experience in the development and management of cyber security solutions, ECSC has an unmatched depth and breadth of experience.

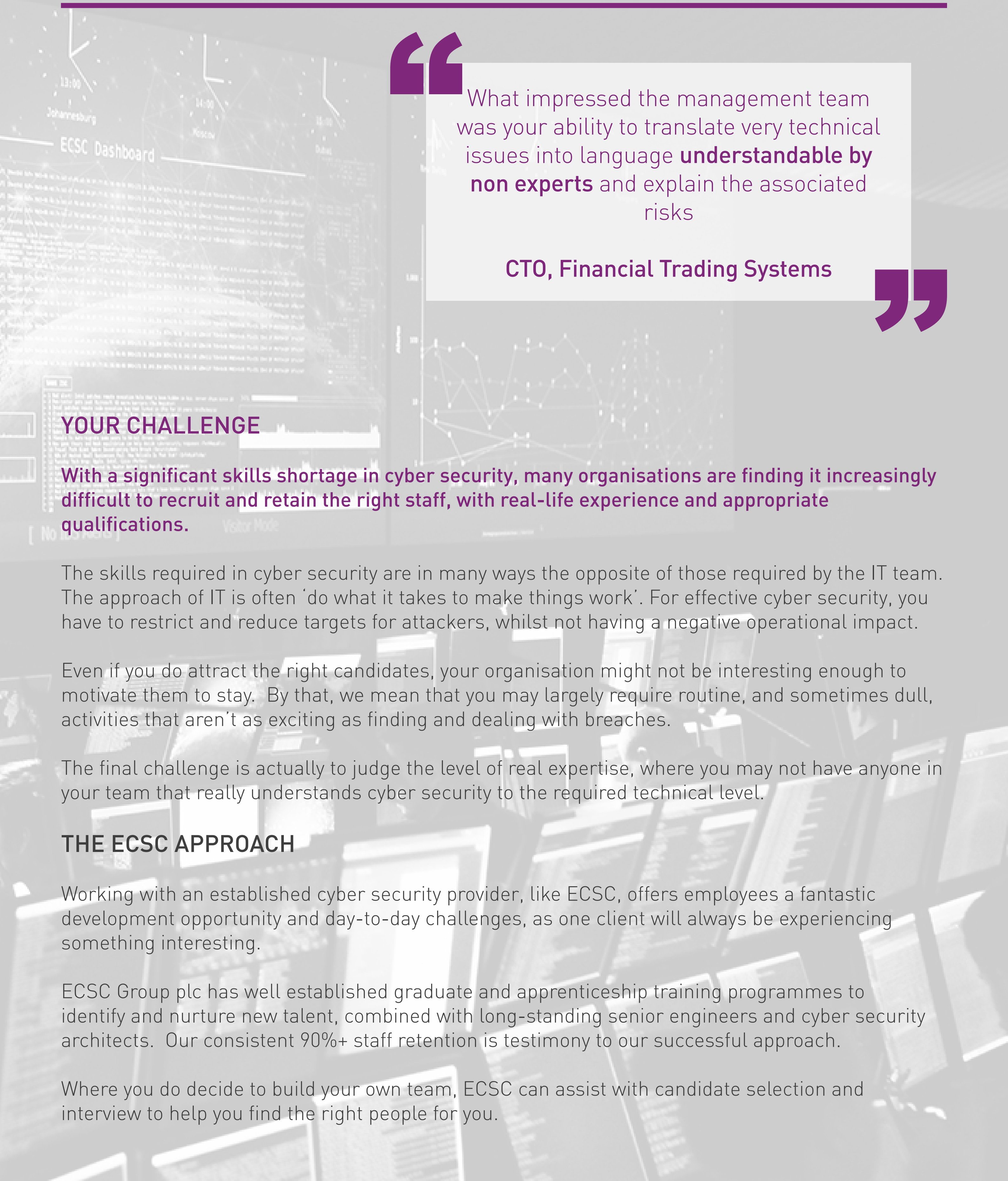
From being one of the pioneers of secure Linux kernels, to the latest Artificial Intelligence (AI) Security Operations Centre (SOC) technology, we innovate and deliver effective results.

ECSC technology solutions are all fully managed, and designed to integrate with our 24/7/365 global SOC coverage delivered from the UK and Australia. We ensure that the right technology is managed and monitored by real people, expertly focused on your cyber security.

Where you decide to self-manage, we can help you with our Vendor Select programme of established cyber security products.

RECRUITING AND RETAINING THE RIGHT EXPERTISE

4



> What impressed the management team was your ability to translate very technical issues into language **understandable by non experts** and explain the associated risks
>
> **CTO, Financial Trading Systems**

YOUR CHALLENGE

With a significant skills shortage in cyber security, many organisations are finding it increasingly difficult to recruit and retain the right staff, with real-life experience and appropriate qualifications.

The skills required in cyber security are in many ways the opposite of those required by the IT team. The approach of IT is often 'do what it takes to make things work'. For effective cyber security, you have to restrict and reduce targets for attackers, whilst not having a negative operational impact.

Even if you do attract the right candidates, your organisation might not be interesting enough to motivate them to stay. By that, we mean that you may largely require routine, and sometimes dull, activities that aren't as exciting as finding and dealing with breaches.

The final challenge is actually to judge the level of real expertise, where you may not have anyone in your team that really understands cyber security to the required technical level.

THE ECSC APPROACH

Working with an established cyber security provider, like ECSC, offers employees a fantastic development opportunity and day-to-day challenges, as one client will always be experiencing something interesting.

ECSC Group plc has well established graduate and apprenticeship training programmes to identify and nurture new talent, combined with long-standing senior engineers and cyber security architects. Our consistent 90%+ staff retention is testimony to our successful approach.

Where you do decide to build your own team, ECSC can assist with candidate selection and interview to help you find the right people for you.

5 DETECTING CYBER SECURITY BREACHES 24/7/365

> “I have been using ECSC for 7 years now and not had any issues in that time, **perfect service**
>
> Operations Manager, Systems Integrators”

YOUR CHALLENGE

It is now understood that hackers don’t work office hours. Night, weekends and public holidays see peaks in attempted attacks. So, watching 40 working hours in a 168 hour hacking week isn’t good enough.

Unless you can employ at least 6 qualified security analysts, with appropriate management coverage, you cannot deliver a 24/7 service. In addition, night-shifts are unattractive and work against staff retention, so you need a global spread of employees.

Having found the people to cover the full week, you then need to invest in the right monitoring and detection systems to give them the information they need to uncover breaches before damaging data loss occurs.

With over 14,000 new cyber security technical vulnerabilities discovered in 2017, a few individuals will struggle to maintain the appropriate threat intelligence necessary to detect breaches.

THE ECSC APPROACH

Having provided managed cyber security services for 18 years, ECSC has proven recruitment, training, and retention processes to find and develop the best people in the industry.

With two global Security Operations Centres, located in the UK and Australia, we have a ‘follow the hacker’ 24/7/365 operation. This includes an 8-hour threat intelligence assessment cycle to review new vulnerabilities.

In addition, the 2018 launch of the ECSC KEPLER Artificial Intelligence engine, at the heart of our managed services technology, keeps ECSC at the forefront of incident detection.

ACHIEVING CYBER SECURITY STANDARDS

6

> We have been working with ECSC for many years and the relationship is **excellent**
>
> **Network Security Manager, Sporting Organisation**

YOUR CHALLENGE

There are times when you need to certify your security, usually to demonstrate to external stakeholders that your cyber security is sufficient for your organisational process and the threats you face.

Whilst, within the UK, there is currently no GDPR certification, two standards are often recommended by the ICO as well established:
ISO 27001 – the international management standard for information security. Suitable for medium to large organisations with some internal expertise and capability.
Cyber Essentials – a UK government-backed standard for small organisations, usually without much in-house IT expertise. Although basic, the mandatory technical controls help prevent 90%+ of breaches.

For organisations storing, processing, or transmitting payment card data, the Payment Card Industry Data Security Standard (PCI DSS), is mandated, and gives a comprehensive set of technical controls to protect critical data.

THE ECSC APPROACH

With increased ICO focus on breach prevention, and mandatory GDPR breach reporting, it is increasingly important that you build a 'defensible position'. Certifications can plan an important role in this development.

With more than 15 years' certification experience, backed by our own extensive suite of certifications, ECSC has helped hundreds of organisations achieve an efficient route to certification. Our pragmatic approach is particularly valued by clients.

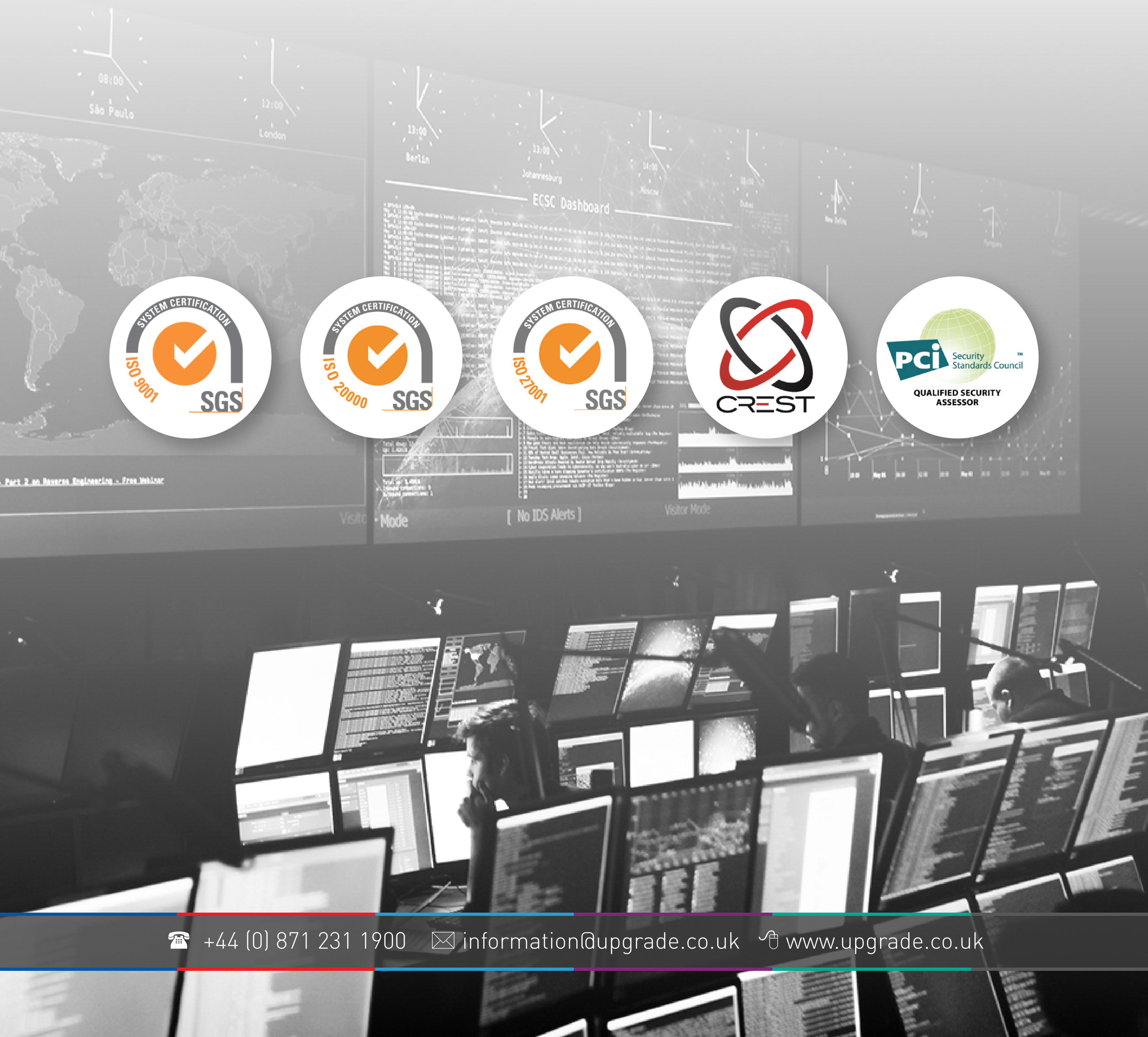
Starting by understanding where your priorities are, in achieving 'the badge' quickly or delivering more meaningful security improvements, we assess your current position and create plans towards successful outcomes.

ecsc
more secure

With almost two decades of experience, ECSC is the UK's longest running, 'full service' information and cyber security service provider, offering a complete range of cyber security solutions and services to all sectors.

Our ever-expanding client list ranges from e-commerce start-ups to global organisations, and our consultative, business-focused approach has led us to proudly count 10% of the FTSE 100 among our clients.

Please feel free to get in touch to see how we can help you.



☎ +44 (0) 871 231 1900 ✉ information@upgrade.co.uk www.upgrade.co.uk