AN EXCEPTIONAL FORCE IN CYBER SECURITY

Combining knowledge, experience and expertise to deliver protection, detection and reaction

$4BN+ LOSSES,

IRREPARABLE DAMAGE TO BRAND REPUTATION AND A BIG BILL TO PUT THINGS RIGHT

The fate of one US firm due to a single data breach

SETTING THE SCENE…

In addition to any fines that may be levied, data security breaches can have a catastrophic impact on a brand's reputation. This will result in a loss of customer and shareholder confidence, and ultimately have an impact on the bottom line. Which is why, in boardrooms the world over, the risks posed by cyber security breaches are being taken very seriously.

It's been widely reported that all kinds of organisations, from government departments to charities and large corporates, have been subject to data security breaches. This reinforces our view that it is not a question of 'if' but 'when' you will suffer a cyber incident. Organisations are expected to have assessed risks and put in place appropriate security to try to prevent breaches, and also manage them when they occur.

The Information Commissioners Office (ICO) reported that where breaches of the Data Protection Act occurred, only 26% of fines imposed were related to cyber crime. The vast majority of breaches were the result of human error.

With GDPR coming into force in May 2018, it is critical that you manage potential risks and avoid the likelihood of fines.

We put great emphasis on the importance of robust IT management and impeccable cyber hygiene as the foundations needed to successfully manage risk. With this approach we help organisations make the most appropriate investment choices – which give security the priority it deserves, even if it's not seen as the shiniest tool in the box.

Despite the growing threat of attacks, UK organisations are cutting rather than increasing their security budgets, and one in five has no preparation drills in place for cyber attacks.

PwC 'Global State of Information Security Survey' 2017
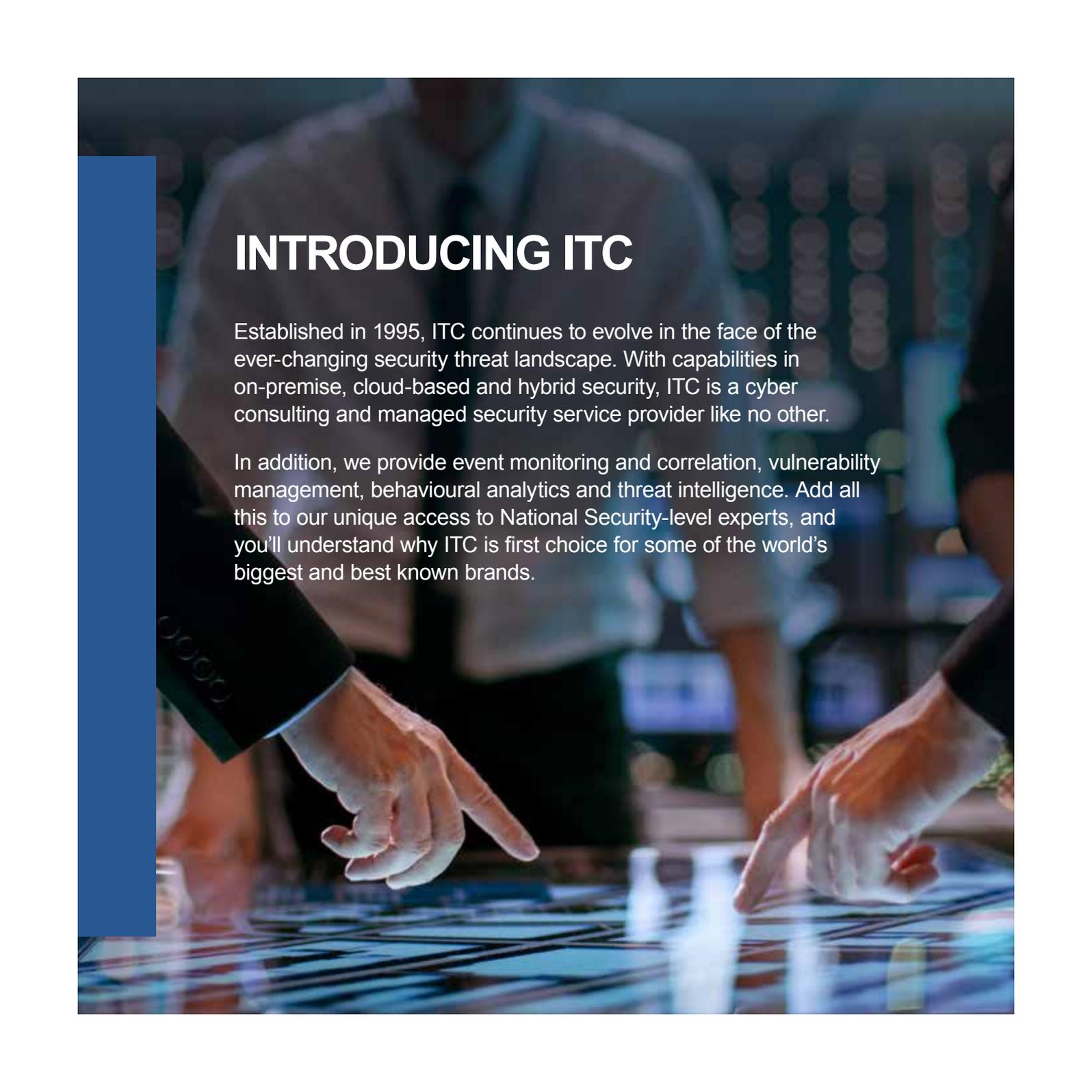
INTRODUCING ITC

Established in 1995, ITC continues to evolve in the face of the ever-changing security threat landscape. With capabilities in on-premise, cloud-based and hybrid security, ITC is a cyber consulting and managed security service provider like no other.

In addition, we provide event monitoring and correlation, vulnerability management, behavioural analytics and threat intelligence. Add all this to our unique access to National Security-level experts, and you'll understand why ITC is first choice for some of the world's biggest and best known brands.

1 THROUGH OUR CYBER CONSULTING AND ADVISORY SERVICES WE ASSESS AND ENHANCE YOUR SECURITY POSTURE

We are cyber security experts, focusing on risk management, insider threat analysis, network and user behaviour, vulnerability assessment and, increasingly, issues around compliance.

We provide cyber situational awareness. Combining the observed internal world and the observable outside world to answer the 'So what?' and 'What now?' questions.

Our risk consulting function bridges the gap between business and security risks. We assess our clients' capabilities allowing them to prioritise their spend and put in place the right levels of security.

2 OUR MANAGED SERVICES EXIST TO REDUCE OUR CUSTOMERS' SECURITY RISKS

We deliver service innovation, cyber security and cloud technology from our UK-based, state-of-the-art Security Operations Centre (SOC).

Taking account of threat intelligence, vulnerability management and compliance, we make sense of what your network is probably already telling you.

Our industry-leading NetSure360° product offers infrastructure and security management as a service, providing visibility, control and assurance over your key assets 24x7x365.
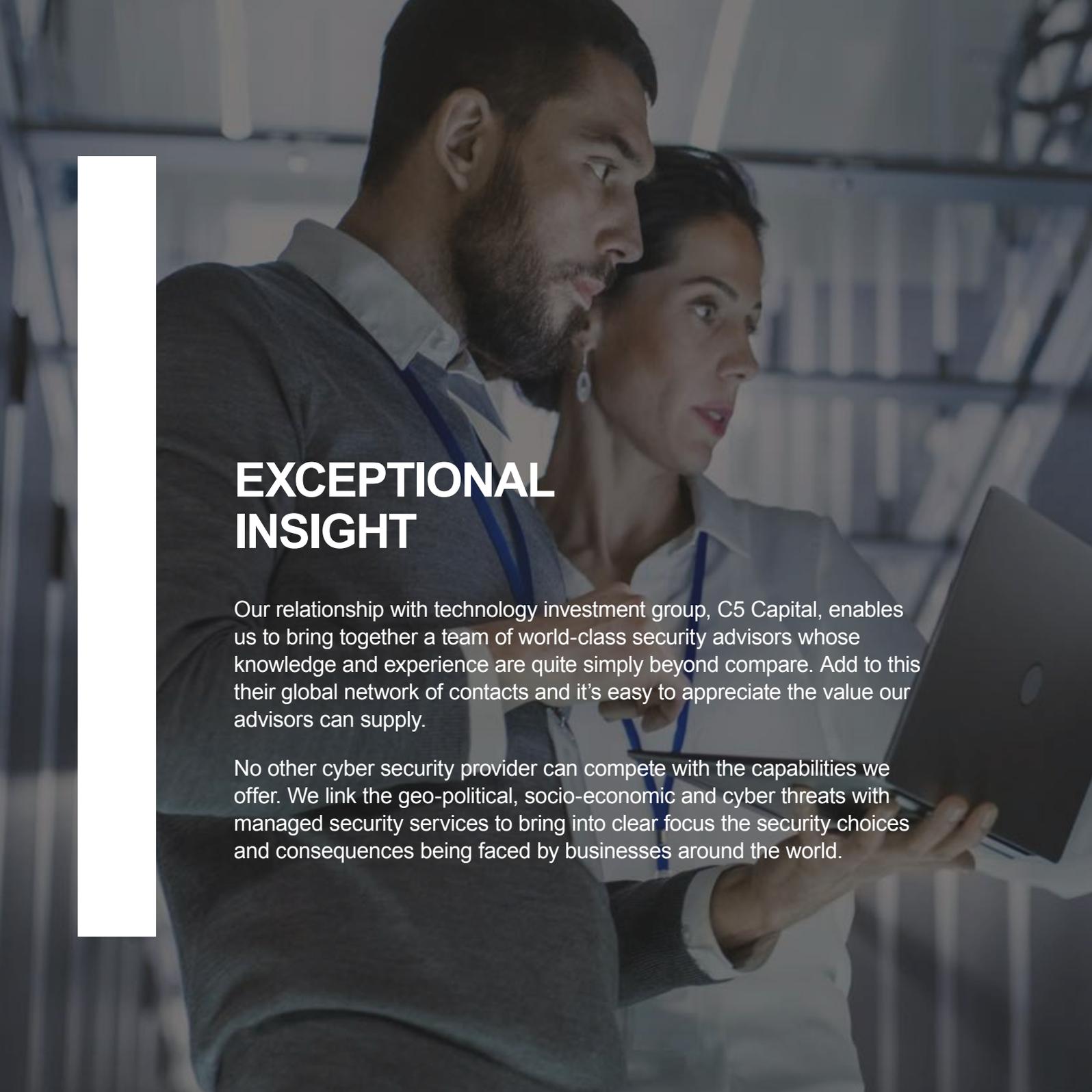
EXCEPTIONAL INSIGHT

Our relationship with technology investment group, C5 Capital, enables us to bring together a team of world-class security advisors whose knowledge and experience are quite simply beyond compare. Add to this their global network of contacts and it's easy to appreciate the value our advisors can supply.

No other cyber security provider can compete with the capabilities we offer. We link the geo-political, socio-economic and cyber threats with managed security services to bring into clear focus the security choices and consequences being faced by businesses around the world.

THE SECURITY ADVISORS

Admiral
Michael G. Mullen

17th Chairman of the Joint Chiefs of Staff and 28th Chief of Naval Operations

Sir Iain Lobban

Former Director GCHQ, the UK's signals intelligence and cyber defence agency

Lt General
Sir Graeme Lamb

Former director of UK Special Forces and Commander of the British Field Army

Ron Moultrie

Former Director of Operations, National Security Agency

CYBER RISK CONSULTING

Our consultants will help you through the full lifecycle of risk management to ensure you know the right things to do for your business, how to implement them and how to run them effectively.

Risk management

Starting with the objectives of your business, we'll help you assess realistic security risks and understand how they could potentially impact your goals. We then review your current security posture, identify areas of weakness and advise you on strategic, governance, policy and control developments that are needed.

Cyber due diligence

Supporting both private equity businesses concerned with assets and organisations wanting a view of their third-party suppliers, our due diligence capability can give speedy insights into potential security issues.

GDPR consulting

We design the governance processes needed to support ongoing GDPR compliance, and provide a full set of industry-leading tools which automatically discover, classify and manage your data.

CISO as a service

An effective way of using our industry-recognised Chief Information Security Officers to provide security leadership to organisations who are either developing their capabilities or are challenged in attracting or retaining in-house skills.

MANAGED SECURITY SERVICES

NetSure360° sets us apart from other providers. It delivers security and information management as a service, and ensures around-the-clock visibility, control and assurance across your entire IT security, network and cloud infrastructures.

Traditional security services

Our industry-leading services focus on the critical assets of your business. Covering centralised logging platforms, network access control, firewalls and intrusion prevention. They allow businesses to manage risk and stay informed.

Cloud

ITC is at the forefront of the Cloud revolution. We make it possible for our customers to transition critical business services and functions into the Cloud and the Hybrid Cloud while maintaining strict security governance.

Intelligent SOC

By assessing human behaviours in real time – not just anomalies – artificial intelligence allows us to automatically analyse and detect threat behaviours as they emerge, to learn from on-going activity and fight back against subtle, stealthy attacks inside the network.

Threat intelligence

Using detailed risk-based profiling and bespoke tools to search the Surface, Deep and Dark Web for relevant intelligence, we provide visibility of potential threats and advise clients on how to mitigate them.

SOME OF THE WORLD'S LARGEST BRANDS CHOOSE ITC

We have partnerships with key players such as Cisco and Micro Focus. And our long list of customers includes: BT; the Financial Conduct Authority; Schroders; BAT and Coca Cola.

Our focus is always on obtaining the right outcomes for your business. We achieve this through our "consulting-first" approach. This enables us to deliver the optimum levels of security and ensures you get the best return from your security investment.

One shipping giant declared a $300M hit relating to a single ransomware attack, with the estimated economic cost much higher at $850m. A perfect example of why you should talk to the cyber experts at ITC.

On Friday 12 May 2017 an unwitting computer user allowed the WannaCry virus into an organisation's system. Utilising a repurposed cyber-spying tool, EternalBlue (reputably stolen from the US National Security Agency and leaked online), it quickly went viral.

Business case, activity and time line

By 0100, 13 May, ITC had advised all its customers of the threat and provided remediation advice. One particularly large organisation with 50,000+ employees across 1,000+ global locations faced a formidable challenge. Fortunately, we were able to assess their complete network, and deliver the assurance and action required to mitigate risk to the business.

By 0130, we'd gained approval to scan their entire global network, some 120,000 IP addresses. By 0330 we'd identified 2,000+ systems vulnerable to WannaCry and had provided this information to the CISO to commence the remediation plan.

By 1630 Monday, all systems across the globe had been patched, and at 1730 we declared the customer clear and at low risk to further WannaCry attacks. Our risk assessment not only supported vulnerability identification for WannaCry, but also ensured the customer was prepared for any further ransomware attacks.

Project history

We started the global vulnerability assessment audit for the customer in 2015. It was a huge undertaking, running data discovery and risk analysis across known infrastructure and the network outsourced to third-party providers.

Following this complex audit, which took nearly two years, patch management was implemented and security maturity and risk exposure report was presented to the board.

When WannaCry hit, the ITC Security Operations Centre identified the threat immediately and the benefit of the full audit and patching became clear. The infection didn't penetrate the customer network. Where risks were identified, through the detailed audit, we were forensic in our patching, every hole closed, every risk thwarted.

itcsecure.com

Boatman's House, 2 Selsdon Way, London E14 9GL, United Kingdom

LLOYD'S REGISTER - LRQA

ISO/IEC 20000-1