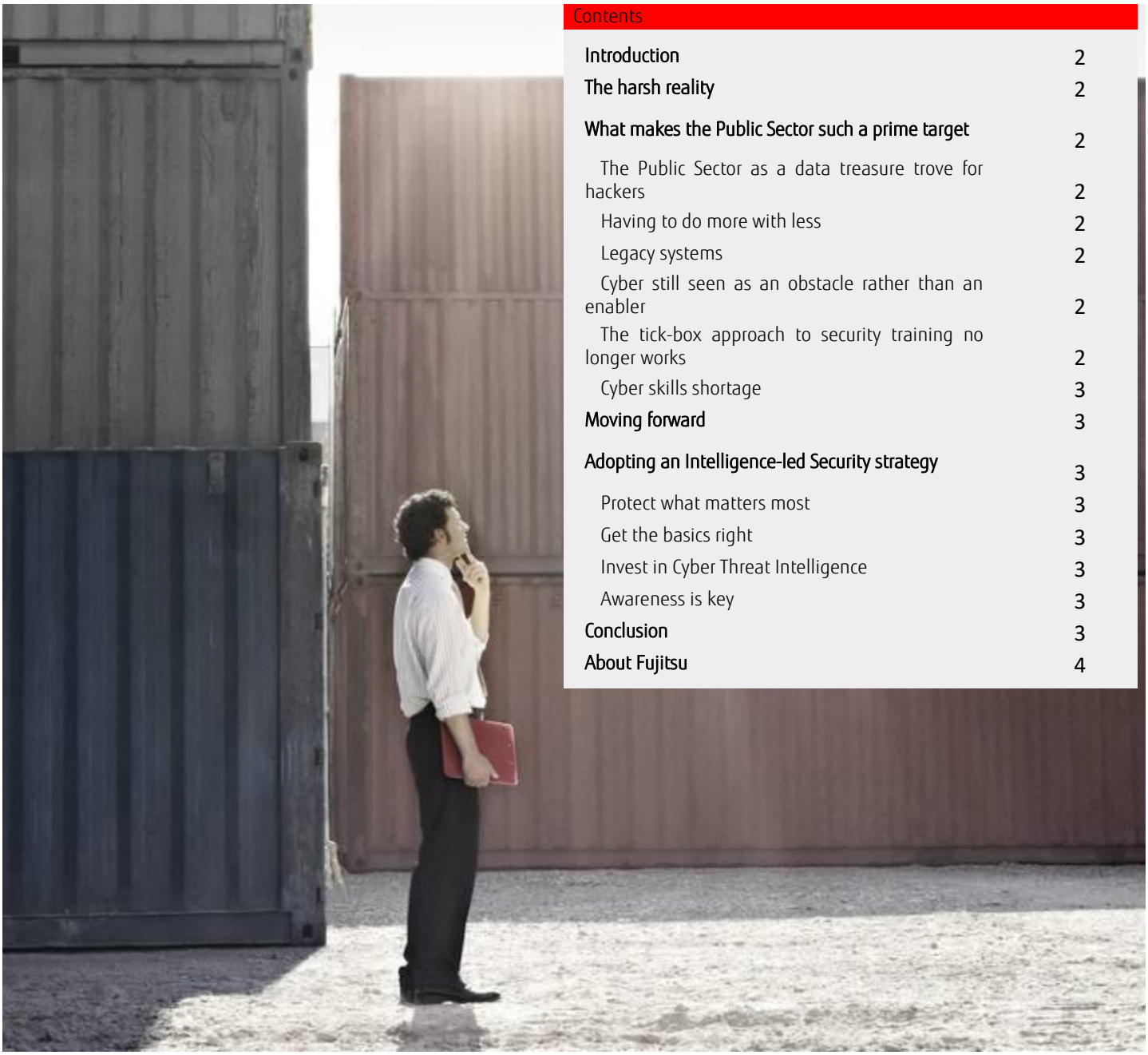
Helping deliver a cyber-resilient Public Sector

How can the UK Public Sector improve cyber-resilience while embracing digital transformation and disruption and also ensure that systems and data are kept safe from a cyber-attack?

This opinion paper explores the issues faced by the Public Sector in relation to cyber resilience. The viewpoints in this document explore a number of observations based on Fujitsu's experience as a technology service provider and a system integrator in the Public Sector.



Contents

Introduction

The UK Public Sector may not have a visible share price as a performance indicator but they have stringent service level targets and budgets to meet, all of which can be impacted by a major cyber-attack, as seen with the Wannacry incident last year.

While Public Sector continues to embark on its digital transformation journey, cyber resilience needs to remain core, especially since the Public Sector touches almost every aspect of our daily lives, whether that be going online to update tax information with HMRC or updating driving license details with the DVLA.

Furthermore, the Public Sector is rapidly moving towards cloud-based services, investing in Office 365, Microsoft Azure and Amazon Web Services, in many cases, without an overarching organisation-wide strategy that considers the new security and privacy risks being introduced by this cloud approach. As confidential and sensitive data is increasingly stored and accessed on cloud services, devices and equipment – for example, operational systems – embedded devices and consumer technologies, there will inevitably also be a greater risk that the security of this data may be compromised.

"How can the UK Public Sector improve cyber-resilience while embracing digital transformation and disruption while also ensuring that their systems and data are kept safe from a cyber-attack?"

The Harsh Reality

The UK Government identifies 'cyber' as one of six tier 1 threats to national security while experts at the World Economic Forum classified the threat of a cyber-attack as one of the top probable global risks of 2018, along with extreme weather events and natural disasters.

Cyber-crime has become far more organised than ever before, and last year it even overtook the drug trade to become the most profitable illegal industry (http://fortune.com/2015/05/01/how-cyber-attacks-became-more-profitable-than-the-drug-trade/).

Technology and cyber security are fast becoming key drivers for Public Sector, making government departments more effective and public services accessible for those who rely on them. Major Public Sector bodies are heavily reliant on security to underpin interactions that are made with millions of UK citizens on a daily basis. At the same time, cyber-criminals are finding more security gaps to abuse, whether they are present in existing public-facing technologies or in new developments such as Internet of Things (IoT) solutions.

Threats stem from opportunistic hackers as well as sophisticated and well-funded nation states keen to get their hands on valuable data.Cyber-attacks like those against UK Parliament and the NHS in 2017 show that the Public Sector is as much a target for cyber criminals as private companies. There is a cost associated with breaches but, aside from the financial impact, breaches can bring about lawsuits and regulatory penalties and (in the health sector) compromise not only patient data, but patient care as we saw with the Wannacry outbreak.

What makes the Public Sector such a prime target?

The Public Sector as a data treasure trove for hackers

The large volumes of personal information held by Public Sector bodies such as healthcare, social services and education institutions that can be used by others for financial or other gain – whether that's medical information, criminal records, or confidential civil service details. The UK Government holds a huge amount of data, often on vulnerable systems, making it an attractive target for cyber-criminals.

Having to do more with less

It is no secret that the Public Sector is grappling with significant budgeting challenges. Across all Public Sector bodies; IT teams are increasingly finding themselves tasked to do more with less often within the restrictions of a tight budget and complex regulations. Most of the sector has found it challenging to deal with cyber security issues, leaving it vulnerable to attacks. As a result, basic security hygiene (e.g. patch management, security training, cyber incident response) has always been an Achilles heel for Public Sector organisations.

Legacy systems

While the UK Government has long acknowledged the need to update its old IT systems, a large number of government services and operations still rely on legacy infrastructure and back-end systems which present huge vulnerabilities that make it easier for hackers to use older exploits with only minor modification. Public services that rely on legacy infrastructure can be decades old and often beyond compliance regulations, which means it is either too expensive or not technologically compatible to update or augment with existing architecture. Many organisations wish to 'sweat their assets' beyond end of life and therefore are exposed to security holes that are no longer being corrected. Protecting legacy systems and infrastructure against cyber-attacks should be a key priority for the Public Sector as it moves forward towards a digital transformation. To protect legacy systems, Public Sector bodies must have complete visibility into their environment and the capability to detect and respond vulnerabilities and threats.

Cyber still seen as an obstacle rather than an enabler

Many Public Sector bodies still see cyber security as an additional cost or obstacle, with minimal return on investment. This is an oversight, especially as millions of UK citizens trust the Public Sector to keep our data secure.

Cyber resilience shouldn't only be seen as a real risk to the Public Sector, but also an essential enabler helping underpin digital services and operations that all organisations now rely upon and a priority investment to ensure that the necessary protective measures are put in place. To keep pace, the Public Sector must embrace a holistic approach where security is an 'integral enabler' of a strategy that promotes risk management and the development of digital trust on an ongoing basis.

Tick-box approach to security training no longer works

Hackers are finding new ways to access information and data, which is why creating a culture of consistent awareness of threats is so important. People and not technology are often the weakest link in security.

The vast majority of malware/ransomware attacks are being caused by employees opening unsafe email attachments, referred to as "Phishing". Other common errors can include failure to adhere to policy requirements when it comes to selecting a secure password, or connecting to a network with an unsecured device. Security training needs to focus on awareness and recognising when something is not quite right. Cyber attackers have a keen understanding of human error and the kind of mistakes ordinary people can make when confronted with an official-looking email.

The traditional once-a-year computer-based training was always seen as a tick-box exercise to evidence an organisation had completed its training, but did not necessarily show if an organisation and its staff had the behaviours and mind-set to prevent a cyber-attack.

While training courses are important, the focus should be on aiding cultural change to promote a shift in attitudes and behaviour.
CxOs in the Public Sector need to ensure that every employee is aware of the potential cyber-threats they could face, whether it's a phishing email, sharing passwords or using public Wi-Fi to transmit sensitive data. More importantly, security training should be tailored according to job role e.g. The Executive Team should not receive the same security training content as a software development team.

Cyber skills shortage

The rapid transition from physical to digital means that the Public Sector is also faced with a widening cyber security skills gap, with industry estimates suggesting that there could be up to three million unfilled jobs in the cyber security industry by 2021 (https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html). A complete overhaul in how cyber security talent is developed should play a key part in defending the Public Sector from cyber-attacks.
Fujitsu is leading the way on addressing the cyber skills gap by launching the *University Technical College (UTC) Cyber Security Group*, which looks to prepare students aged 14-19 for the cyber security jobs of tomorrow. Working with cyber UTCs across the country, along with the help of leading edge Security and Private Sector organisations, the group looks to bridge the security resource and skills gap that organisations face, to help better protect today's society from cyber-threats. The group will aim to equip students with the right cyber-skills to be able to hit the ground running when they start employment, and to better prepare those moving into Higher Education.

Moving forward…

Whilst things are improving there is still a lot of work to be done to ensure our vital public services can remain resilient to a serious cyber-attack, and also stay one step ahead of the criminals responsible. The current UK government Cyber-Security strategy (https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021) based around three core foundations of *defend*, *deter* and *develop*, has set the wheels in motion, but to keep pace with sophisticated and highly motivated attacks, the Public Sector must adopt a dynamic, nimble security strategy that builds resilience from the inside out, while further enhancing resilience through additional initiatives such as:

- Enhanced intelligence and law enforcement activity to identify, anticipate and disrupt cyber-adversaries
- Investment in academic and industrial research and innovation, including start-up companies, measures to raise public awareness of cyber security, to support cyber training in different formats in education
- Working with communications service providers and industry to make the internet more secure
- More support for CNI operators such as sharing threat intelligence and best practice, and conducting joint exercises to test and develop their cyber resilience
- The potential for increased regulation.

Adopting an Intelligence-Led Security Strategy

While generic technical controls around firewall implementation, encryption, back-ups, network monitoring and penetration testing are good examples of baseline technical controls, the Public Sector must seek to take an *intelligence-led* approach sponsored by senior stakeholders who will 'buy-in' to a long-term intelligence-led security plan aimed at delivering Public Sector outcomes, as opposed to responding tactically to every single new cyber-threat out there.

Protect what matters most – It can be difficult to secure everything, so Public Sector bodies must aim to identify and prioritise critical and sensitive information assets and enhance security around them.

Get the basics right – Before investing in expensive solutions organisations need to take time to assess if they have the basics covered such as patch management and privileged access. Poorly managed privileged access management can lead to unauthorised access to systems and sensitive data.

Invest in Cyber Threat Intelligence (CTI) - The Public Sector uses many monitoring tools and consumes many sources of threat data, but these technologies do not necessarily provide evidence-based context, implications and all other information to turn information into 'actionable intelligence'. CTI can help Public Sector bodies turn unknown threats into known and mitigated threats helping answer questions such as:

- What threats are changing over time?
- What are the threats to our citizens?
- What types of threats are occurring in the industry?
- Who might want to steal our intellectual property and how will they likely try to do it?
- What threats affect our partners, suppliers or competitors?
- Will the newly published exploits affect our sector?

Awareness is key – Ensure employees are aware of the risks and understand their responsibilities – remember, cyber is not just an IT-level responsibility. A key aspect of this is to educate the executive team about the necessary investments that need to be made in new solutions, new skills and in properly implementing organisation-wide culture of cyber security awareness, capable of continually evolving and adapting to evolving cyber threats. To foster this culture and move closer to a state of digital trust, security training must consider how employees are using their technology and the kind of tools they use on a regular basis.

Conclusion

The pressing need to invest in having the right people, processes and technology with dedicated attention from Public Sector senior stakeholders is crucial to achieve a secure and cyber-resilient Public Sector at a time when budgets are already being cut. It is crucial to address the need to ensure that the Public Sector can continue to safely serve citizens and maintain the trust of the nation.
Public Sector bodies should ask themselves the following ten key questions:

1) Have we identified our 'crown jewels' and the high-value assets we should be protecting?
2) Is cyber security featured on our corporate risk register?
3) What security KPIs/metrics are we receiving?
4) Have we prepared and tested our cyber incident response plans through cyber incident scenario planning?

5) Which, if any, board oversees cyber security activity and policy.
6) How are we educating our staff about cyber-security threats and how do we know that our security training programme is effective?
7) When did we last test our business continuity process and is there an order of which systems to restore or sustain? (E.g. social care functions first, frontline customer service hubs, etc.)
8) What reporting mechanisms are in place for staff to report security concerns?
9) How effective is the cyber threat intelligence we receive?
10) Are all plans accessible and comprehensible in the event of an attack?

About Fujitsu

Fujitsu is an international technology provider and has enabled Public Sector organisations to thrive globally for more than 40 years. As an established Service Integrator and ICT provider within the Public Sector Fujitsu has made a considerable investment in deploying technical and service orientated security solutions to support the next wave of change. Fujitsu is one of the only technology service providers to achieve ISO22301 certification for its entire UK and Ireland business. By working with Fujitsu, Public Sector organisations are able to rapidly embrace and leverage leading practice and expertise to help build a relationship of trust and confidence that the underlying ICT infrastructure will continue to deliver the essential services they rely on.

Contact

Email: askfujitsu@uk.fujitsu.com
Call: 01235 79 7711
Ref:3869

About Fujitsu's Enterprise & Cyber Security Practice

At Fujitsu, we believe new threats call for new ideas and ways of thinking. Through our intelligence-led approach to cyber security, we offer a new way to understand and respond to threats. With over 4 decades as an IT security service provider, Fujitsu has a wealth of experience and knowledge that we applying to improving the security for all customers.
Fujitsu can keep Public Sector organisations ahead of threats and vulnerabilities by:

- Providing the robust management of cyber security platforms
- Assessing cyber risk and developing strategies to improve cyber resilience
- Delivering comprehensive visibility of events for early threat detection
- Routinely scanning your systems to detect vulnerabilities before they become critical
- Offering actionable threat intelligence and context from our industry leading experts