Opinion paper

Digital Vision
for Cyber Security

Trusted partner for your **Digital Journey**

Atos

Contents

Digital Vision for Cyber Security

Adrian Gregory
Chief Executive Officer,
Atos UK & Ireland

For years, the received wisdom for how to secure technology and data was a firewall, equivalent to a 'lock on the door'. Today the answer is more complex.

In a world where technology has burst out of the comms room into almost every area of life, how do we install walls and locks everywhere? Clearly, our approach to cyber security must adapt. We now need to understand behaviour patterns and pinpoint anomalies and outliers. To be predictive rather than waiting for impacts. This paper offers a range of expert views on the scale of the challenge, with new thinking to foster confidence in the face of a vast array of threats. One thing we can be certain of: our relationship with technology will continue to change at pace, and how we protect ourselves must also move with the times.

Pierre Barnabé
Executive Vice-President, General Manager
Global Division Big Data & Security, Atos

A more automated cyber security approach is essential to address the sheer scale, complexity and volatility of risks in the digital age.

As Robert S. Mueller, ex-Director of the FBI once said, we cannot undo the impact of technology – nor would we want to. We must use our connectivity to stop those who seek to do us harm. At Atos, we believe that data, combined with human intelligence and insight, is key to fighting today's threats. We harness automation and machine learning to understand – and predict – the threat landscape. We're also getting ready for the next digital shockwaves – not least the arrival of quantum computing. Yet with the attack surface expanding, cyber security is no longer just for the IT department. It's an executive leadership issue involving every individual in an organisation.

Gavin Thomson
Senior Vice President, Big Data & Security
UK&I, Scotland, Ireland and Wales, Atos

Large-scale cyber attacks remain a distinct possibility; businesses need to work with their partners and suppliers to integrate effective cyber security across the supply chain.

Cyber space has no borders and today, the lines of defence have moved into every part of our public and private infrastructures. In all sectors, ongoing digital transformation and innovation must have cyber security in-built as an enabler that protects the integrity of every transaction. Cyber security is a challenge that has the attention of every leader who understands the importance of learning the lessons of recent attacks. We need more collaboration on response strategies and we need urgently to address the cyber skills shortage. What experience tells us is that with the right tools, skills and cyber awareness in place, we can respond and stop attacks extremely quickly.

Cyber Security: the business challenge

45%
of businesses view loss of customer trust and confidence as most damaging effect to business

40%
of businesses experience DDoS attacks on a monthly, weekly or even daily basis

300%
increase in ransomware attacks since 2015

4,000
ransomware attacks a day

1.5 million
cyber jobs by 2019

Over 3 million
data records compromised daily

https://media.scmagazine.com/documents/292/corero_infographic_ddos_full_72957.pdf

A sizeable proportion of businesses still do not have basic protections or have not formalised their approaches to cyber security:

61%
of UK businesses hold personal data on their customers electronically

Under two-fifths
have segregated wireless networks, or any rules around encryption of personal data (37% in each case)

A third
have a formal policy that covers cyber security risks (33%), or document these risks in business continuity plans, internal audits or risk registers (32%)

A fifth
of businesses have had staff attend any form of cyber security training in the last 12 months, with non-specialist staff being particularly unlikely to have attended

One in ten
have a cyber security incident management plan in place

6.5%
of UK businesses are aware of the 10 Steps to CyberSecurity

38%
of firms say they have insurance covering a cyber security breach or attack

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

Robert Hannigan, Former Director of GCHQ and chairs the European Advisory Board of BlueteamGlobal

Winning the arms race against cyber crime

Faced with the challenge of transforming their businesses for the digital era, company leaders may see cyber security as an extra, unquantifiable risk. Worse, they may feel that by embracing digital transformation and meeting the challenge of disruption from new technology rivals they are in danger of more destructive disruption by cyber attackers.

But the most successful businesses have understood that these are actually two sides of the same issue. What tech disrupters and cyber criminals have in common is understanding the power and value of other people's digital data. The first step for any Board is therefore to understand their own data, to define what they care about most, and to understand the rapidly-changing nature of the threat. From this platform they can make sensible risk judgements and spend proportionate amounts on securing their networks.

New disruptors

The threat has evolved rapidly in recent years. Those of us who became involved in cyber security many years ago, remember a time when most companies left cyber to the technical specialists. The threat appeared to be from mischievous individuals, amateur criminals or a few states, who were more intent on IP theft than disruption. The worst that a company might experience was an embarrassing denial of service attack or the loss of IP which it would write off as a cost of doing business.

But all that has changed, and very publicly. Organised crime groups, often nested in or partnered with corrupt states, have become the ultimate disrupters. Helped by the low cost of processing they have developed a commodity market in hacking and malware, offering managed cyber crime services as well as specific tools for the more expert. These are not lone individuals but sophisticated organisations with the skills to get inside a company's networks, understand them and their supply chain, and choose which data to monetise and how.

Unintended consequences

The motives here are primarily about profit, but criminals do not mind if an attack has unintended destructive consequences. The 'Wannacry' virus, which paralysed parts of the UK health service and some European businesses, is a good example. More worrying is the fact that some states are willing to use attacks for political effect with reckless disregard for the collateral damage to industry elsewhere. This is a new development and has caught some major manufacturers by surprise.

Companies that once thought cyber attacks were about fraud and financial data, have discovered that ransomware attacks, data deletion or other destructive system attacks, can not only damage reputation but bring their operations to a grinding halt. In short, cyber crime is not only rising in volume but in sophistication, as criminals and state-backed crime groups gain access to better tools, and deploy them more expertly.

Multi-layered approaches

Against this fast-moving threat picture, new EU legislation, notably the General Data Protection Regulation (GDPR), offers an opportunity for companies to look again at cyber security as a Board-level risk. That means getting the governance right and applying the same energy that would naturally be invested in traditional areas of finance and compliance.

The evolving threats also demand a more multi-layered security model than in the past, tailored to the company's needs. Better threat intelligence, secure configuration and network security, malware prevention, improved user policies and awareness, internal monitoring, incident management, cyber insurance and other bespoke capabilities will be required to cover the full spectrum from prevention to mitigation. Some companies will want to manage this blend themselves at enterprise level, others will find buying in a managed service more appropriate.

Confronting the risks

The good news is that recent global headline-grabbing cyber attacks have illustrated that companies and organisations that take cyber seriously can defend themselves effectively and, even if breached, can recover quickly. Good cyber security is becoming a differentiator, as attacks are displaced to softer targets.

> Organised crime groups, often nested in or partnered with corrupt states, have become the ultimate disrupters.
>
> **Robert Hannigan, Former Director of GCHQ and chairs the European Advisory Board of BlueteamGlobal**

Winning the arms race with cyber crime will require the best technology and people. Machine learning and Artificial Intelligence (AI) are already making cyber security more effective and efficient. But human skills remain the big obstacle. Most companies struggle to recruit and retain the right amount of high skills talent. The answer is to keep expanding the pipeline – some of that is up to the education sector, in partnership with industry, but companies will often find undiscovered talent within, which can be developed with the right kind of support.

While public awareness of cyber attacks has never been higher, it has never been clearer that this is a manageable risk which is well within our ability to confront.

Robert Hannigan was Director of GCHQ, the UK's intelligence and cyber security agency, from 2014-17. He established the UK's National Cyber Security Centre in 2016. He has written regularly for the Financial Times on cyber security, chairs the European Advisory Board of BlueteamGlobal, and advises a number of international companies.

Kevin Cooke, Cyber Reconnaissance & Response Manager, Big Data & Security, Atos UK&I

The importance of threat intelligence as a positive tool

With an ever-expanding threat landscape, are you aware of how your organisation could be targeted today?

In the digital economy, the grim reality that every business must accept is that it's no longer a matter of 'if' but 'when' a security breach will occur. Traditional security solutions are not enough to protect against sophisticated cyber criminals who are increasingly successful at getting inside companies' networks and compromising sensitive data. Organisations must recognise that an effective cyber security posture involves not only detection and recovery from compromise, but also a proactive approach to prevention.

Evolution of IoT security

With approximately seven billion devices connected to the internet worldwide today and 20 billion estimated to be connected by 2020, the risk to privacy, information leakage and size of an organisation's attack surface is increasing. Recent research[1] has identified that, globally, the average total cost of a data breach is £2.79 million (£2.39 million in the UK). This does not account for the introduction of General Data Protection Regulation (GDPR) in May 2018, which will command stricter controls around the governance and protection of sensitive data. However, security concerns relating to the Internet of Things (IoT) span much further than purely unauthorised access to data. IoT devices are still in their infancy when it comes to security, which makes them easier to target due to vulnerabilities such as software reconfiguration and default passwords.

Next generation of cyber attacks elevates business risk to a new level

The growth of IoT has led to a notable increase in cybercriminal activity and capability. Malicious actors have capitalised on the ability to quickly establish large-scale botnets. These are wide scale, coordinated attacks that use the IoT to spread through company networks and can result in major disruption called 'distributed denial of service' (DDoS). Sometimes known as 'DDoS of Things' attacks, they have become commonplace, with the most notorious being Mirai and Brickerbot in recent times. Industry analysts predict[2] that ransomware will increasingly migrate to IoT and become a primary threat, potentially leading to significant impact on both commercial and critical national infrastructure.

Why organisations need proactive and strategic threat intelligence

Hacktivists, cyber criminality, state-sponsored attacks and insider threats combine to form a dangerous threat landscape for organisations today - not to mention the ease of access to 'off-the-shelf' attacks (such as malware distribution and phishing campaigns) available in the dark web marketplace. This plethora of threats emphasises the importance of maintaining awareness by effectively using threat intelligence.

Threat intelligence is not new and in relation to cyber security means: 'evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard'.[3]

What is new is the ability to derive actionable intelligence from the sheer volume of threat intelligence now available. The value of threat intelligence is in helping organisations to prioritise actions in proportion to the threat and an analysis of overall risk. Over the years, organisations have attempted to introduce threat intelligence into their security tooling in order to detect and protect against known malicious domains, blacklisted internet addresses and other identifiers. The problem was, this intelligence consisted of millions of indicators that needed filtering and prioritising and were soon out of date.

[1]Ponemon 2017 Cost of Data Breach Study, based on 419 companies across 11 countries and 2 regions who had each suffered a loss of between 2,600 and 100,000 records
[2]McAfee Labs 2017 Threat Predictions Report
[3]Gartner Analyst Rob McMillan
[4]Gartner 2015

In recent times, industry analysts[4] identified three key levels of cyber threat intelligence:

- **Tactical:** technical intelligence such as using threat indicators to proactively hunt for and defend against adversaries
- **Operational:** intelligence focused on the motivations, intent and capabilities of adversaries
- **Strategic:** intelligence about the risks and implications associated with threats used to inform business decisions and direct cyber security investment.

Identifying threats means that organisations can combine different levels and types of intelligence (including human intelligence) to obtain targeted, contextual threat intelligence in relation to their brand, their people and their technology. This proactive and structured approach adds immense value by enabling greater insight into what threats the organisation faces, the tactics, techniques and procedures of its adversaries, and how this can be used to minimise business disruption and reduce the window of opportunity for threat actors.

> “The value of threat intelligence is in helping organisations to prioritise actions in proportion to the threat and an analysis of overall risk.”
>
> **Kevin Cooke, Cyber Reconnaissance & Response Manager, Big Data & Security, Atos UK&I**

Lessons learned – CloudHopper, WannaCry and NotPetya

CloudHopper

When did it start?	Summer 2016
What?	Cyber-espionage (stole personal details; exfiltrated data)
By whom?	A group called APT10 – possibly state-sponsored
Motivation?	Seize trade/business assets and secrets; Compromise confidential data
Targeted at?	Critical national infrastructures and public services via their Managed Service Providers (MSPs)
The cost?	While the extent of the exploitation of these vulnerabilities is unknown, it necessitated a significant amount of remedial work across the public sector and its Managed Service Providers to add additional measures to reduce potential future impact
What's the exploit?	Microsoft Office vulnerabilities
Who was impacted?	UK, US, Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa, India, Thailand, South Korea, Australia
How did it get in?	Spear-phishing
How did it spread?	Harvested system administrators' details
How was it halted?	Major exercises by MSPs to plug vulnerabilities
What did we learn?	Importance of proactive threat intelligence

WannaCry

When did it start?	12 May 2017
What?	Ransom attack (money demanded for return of seized data)
By whom?	Unclear
Motivation?	Unclear: political, financial, anarchical, or even a mistake
Targeted at?	Microsoft environment – specific target a mystery
The cost?	Potentially hundreds of £millions in operational losses
What's the exploit?	Weaponised an exploit called Eternal Blue, originally developed by (and stolen from) the US National Security Agency (NSA)
Who was impacted?	Over 200,000 machines in 150 countries (four most infected countries: Taiwan, India, Ukraine and Russia). Collateral damage to organisations including NHS, Renault France, Nissan UK, Telefonica Spain, Portugal Telecom, MegaFon Russia
How did it get in?	Phishing attack
How did it spread?	Worm spread infection networks
How was it halted?	'Kill switch' discovered by 'MalwareTech', a security researcher
What did we learn?	Vulnerability of critical services with legacy equipment

NotPetya

When did it start?	27 June 2017
What?	Premeditated destructive attack (demanded ransoms – rendered machines unbootable - even if victims paid the ransom, the 'key' to retrieve data did not exist – paying the ransom was pointless)
By whom?	Unclear
Motivation?	Unclear
Targeted at?	Ukraine
The cost?	Hundreds of £millions; One company alone reported £100 million lost revenue
What's the exploit?	Again, used Eternal Blue
Who was impacted?	Companies in Ukraine and global companies with subsidiaries there; collateral damage: a UK ad agency, an Indian container port, a global law firm
How did it get in?	Phishing attacks or compromised source code in financial software used in Ukraine
How did it spread?	Multiple spreading techniques
How was it halted?	Antivirus software; indicators of compromise identified and addressed; security patches
What did we learn?	Even after WannaCry, some businesses were still unprotected

8 key lessons the world learned

1

An attack can come **anywhere anytime**, and can spread wherever it can - not just to specific targets.

2

Always keep endpoints **patched** (even after WannaCry attack, some businesses still failed to patch systems).

3

Always run supported **operating systems** and **applications** (many businesses still use unsupported versions of Windows XP and Server 2003 to run the business-critical operations).

4

Establish and test **Security Incident Response** procedures to react to an attack.

5

Ensure employees are properly **informed and trained** to spot suspicious activity.

6

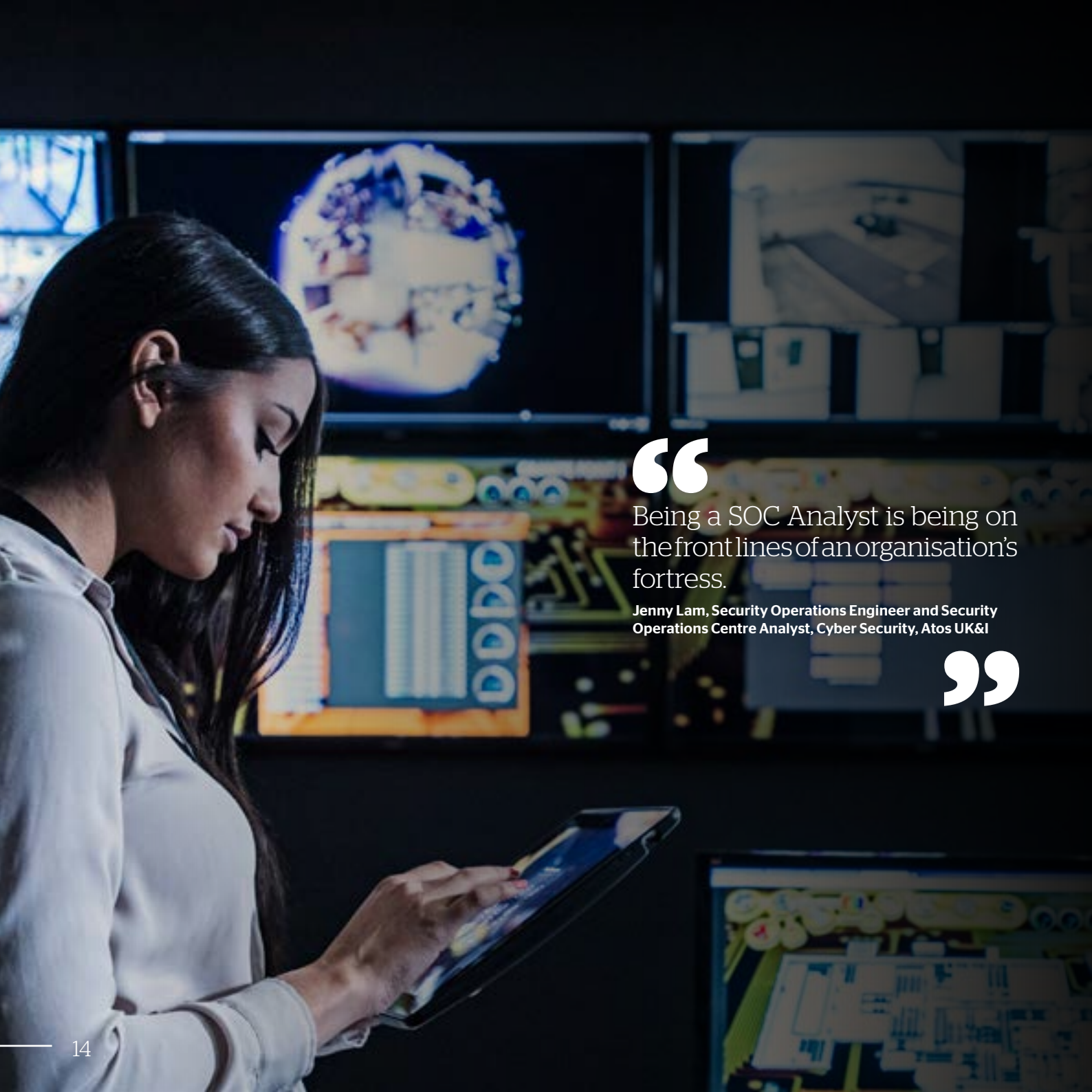
Use **Threat Intelligence and Behavioural Analysis**: using Antivirus software alone is not enough.

7

Implement and test a **backup strategy** to support businesses-critical assets and operational data after a ransomware attack.

8

Establish appropriate **business continuity and disaster recovery** plans and rehearse them regularly to make sure they are fit for purpose.



> Being a SOC Analyst is being on the front lines of an organisation's fortress.
>
> **Jenny Lam, Security Operations Engineer and Security Operations Centre Analyst, Cyber Security, Atos UK&I**

Jenny Lam, Security Operations Engineer and Security Operations Centre Analyst, Cyber Security, Atos UK&I

The changing role of a Security Operations Centre Analyst

As the world transforms into a virtual forest of information, organisations are finding that cyber security has become ingrained into its roots; investing in digital defences has become an essential common practice. Being a Security Operation Centre Analyst is being on the front lines of an organisation's fortress; they are the staff who protect the perimeter, guard the entryways and patrol the virtual corridors.

Advanced threat-hunting

With most businesses relying on their IT infrastructure to function, it has been predicted that by 2020, our digital universe will hold 44 trillion gigabytes of data, which is the equivalent of 6.6 stacks of iPads between the Earth and moon[1]. The incredible rates of data growth mean that Security Operation Centres (SOCs) face the problem of being swarmed by a plethora of security alerts, and SOC Analysts can become consumed by alert management tasks rather than fulfilling the mantle of a proactive defender. The introduction of Prescriptive Security (see page 32), brings in intelligent automation of alerts to enable SOC Analysts to better utilise their time as an advanced threat hunter and security specialist.

I was drawn to a career in cyber security following the shock of learning about the devastating impact that cyber attacks can cause. I started to wonder how it was possible for an organisation to protect itself from an ever-changing threat. My time as a SOC Analyst began in 2015 as a Graduate Trainee and involved being part of a round-the-clock team monitoring a variety of networks and devices. Each set of security devices will inspect the network traffic going to or from the device or zone it is protecting, and trigger an alert based on a set of rules that define suspicious characteristics or behaviour. The Analyst would then inspect the alert created and perform investigations using in-house and open source intelligence tools to determine if the alert is legitimate or a false positive. Legitimate alerts are classified as incidents and require further investigation into the nature of the risk or breach, then the relevant specialist or incident management teams are engaged to resolve the incident.

Power of Prescriptive Security

The modern growth of connectivity and business infrastructure quickly impacted the role significantly. The vast amounts of data and alerts caused the thinly-spread specialised Analyst to prioritise their responsibilities, meaning actively seeking and researching threats took a back-seat. What should have been a partly proactive role suddenly became a heavily reactive one.

Prescriptive Security is based on automating simple threat analysis. Sophisticated machine learning can identify threats, even initiate remediation and clean-up actions in significantly quicker time. Automating the basic tasks of a SOC Analyst frees them to combine the brilliance of a human mind with the supercomputing power of Prescriptive Security. Under this new model, Analysts are returning to detailed malware analysis, researching the latest exploits and spending more time on stopping attacks before they even happen. As advanced technology can draw meaning from huge quantities of seemingly random data, complex patterns and trends emerge which were before unseen, unlocking further potential for accurate foresight to keep organisations one step ahead.

Embracing the change

While not all SOCs work in the same way, they share a common need to mature in order to provide an efficient and effective service. It is no surprise that the more advanced security organisations are embracing the need for change, and realising the requirement to adapt its people as well as technology is equally important. The role of a SOC Analyst is maturing, with the true value of people upheld through the integration of big data analysis techniques with cyber security.

It is said that cyber security progressions are driven by the boardroom, with leading organisations in all industries setting the standards, in turn affecting how SOCs operate. Organisations who invest in intelligent security will advance their asset protection by enabling a proactively focused defence strategy. The SOC Analysts will no longer be burdened with repetitive alert management and instead invest their time and passion into the work and research of a true security practitioner.

[1] https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

techUK

Talal Rajab, Head of Programme, Cyber and National Security, techUK

Securing the Internet of Things: how governments are responding

The Internet of Things (IoT) has transformed the way in which we operate. From healthcare to transportation, farming to construction, the growth of internet-connected devices both at home and at work has increased efficiency, allowing businesses and governments to think differently as to how to deliver services to the public. Such trends are only likely to grow, with some estimates predicting that more than half of all businesses will be run on the IoT by 2020.

With such great opportunities, however, come certain risks as the growth of connected devices also represents a growing attack surface for cyber criminals and hackers. Take the issue of IoT within Industrial Control Systems (ICS), for example. The rapid implementation of connectivity in industrial control processes in critical systems opens up the possibility of devices, which were never vulnerable to cyber attacks in the past, being hacked. Closer to home, barely a month goes by without security researchers finding vulnerabilities in a range of consumer devices from baby monitors to hair trimmers.

Secure by Default

Security is therefore a critical element of IoT deployment, yet it has too often become an afterthought for those designing IoT products and services. That is why the UK Government, through the implementation of its five-year National Cyber Security Programme (NCSP), has endeavoured to work in close partnership with industry to build security into the development of the next generation of internet-connected services through the 'Secure by Default' initiative.

'Secure by Default' is about having security built-in from the ground up, designing hardware so that it is resistant to cyber and physical attacks whilst ensuring that operating systems take advantage of hardware security features. Earlier this year, a project team within the Department for Digital, Culture, Media and Sport (DCMS) was established to take this objective forward. The aim was to take a holistic approach to IoT security by tackling the issue at its root and ensuring that long-term technical efforts are put in place to guarantee that the right security principles are built in to software and hardware.

Cyber education

Crucially, the review is also looking at the equally demanding task of making IoT security functions available and usable in such a way that consumers can readily adopt them. It is commonly remarked that IoT security runs the risk of falling victim to significant market failures, as a lack of cyber education amongst both the purchaser and seller has resulted in neither side prioritising security. And even when designers do integrate strong security features in to their products, getting their users to turn them on and use them can be a challenge. The 'Secure by Default' initiative thus recognises the importance of promoting and encouraging technology which has the best security without the user having to turn it on, or even knowing that it is there.

Wider government initiatives

The 'Secure by Default' initiative is not the only Government-backed initiative aimed at improving IoT security. The Department for Transport (DfT), for example, introduced new guidance for connected and autonomous vehicles in response to the growing cyber threat affecting internet-connected cars. Based on eight key principles, the guidance aims to ensure that those developing connected and autonomous vehicles have cyber security at the forefront of their minds. This will help guarantee that all parties involved in the manufacturing and supply chain are provided with a consistent set of guidelines on security for connected cars.

In the US, a cross-party group of Senators introduced the Internet of Things Cybersecurity Improvement Act, which would ensure that companies selling IoT devices to the Federal Government met a minimum security threshold that loosely revolves around ensuring that products are patchable and prohibiting vendors from supplying devices that have unchangeable passwords.

It is therefore clear that the security of IoT products and services is at the forefront of government efforts to secure cyberspace. The benefits of IoT will only be realised if security is built in by design; the onus should not be on consumers to 'turn on' security features or change default passwords. Industry needs to build in security features so that our increasingly connected world becomes 'secure by default'.

Professor Lizzie Coles-Kemp, Information Security Group, Royal Holloway University of London

Engaging people more actively in cyber security

In the last ten years, there has been increased UK research focus on how to engage people in the everyday aspects of cyber security and the importance of cross-team communication.

This is because improving the quality of the interactions between security practitioners and end users creates a constructive dialogue that helps organisations to protect information and to make the essential links between the protection of information and the protection of individuals, business and society. This kind of more collaborative and proactive approach to engagement helps security practitioners to identify the day-to-day issues and concerns that hinder secure practices and supports more collaboration in designing data protection responses that are more relevant and actionable by staff.

The topic of active engagement has been championed by both the UK's Research Institute for the Science of Cyber Security (RISCS) and the UK's Centre for Research and Evidence on Security Threats (CREST).

Shifting from passive to active engagement

Our creative securities research practice within the Information Security Group at Royal Holloway University of London has developed techniques for active and collaborative engagement using participative visual methods such as cartooning, storyboarding, collage-making and model-building to gather narratives of day-to-day information security concerns.

Our methods are designed to encourage three main shifts in cyber security engagement culture within organisations:

Shift from	To
telling people what makes them secure	discussing with them what their concerns are and what they regard as secure
staff as passive recipients of awareness	staff as active participants in cyber security learning
a monoculture of homogeneous engagement techniques used with all communities within an organisation	a polyculture of diverse engagement techniques that can be adapted to different engagement styles and that encourage participation and discovery as well as subject knowledge communication

Keeping information flowing

We often find that the family of risks related to information not being able to flow across an organisation features as one of the most pressing concerns for staff. Whilst this family of risks may not typically feature highly in a traditional risk register, they are often significant sources of concern to staff.

As part of the RISCS research project Cyber Security Cartographies and the EU FP7 funded TREsPASS project, the Royal Holloway creative securities team developed a number of case studies in organisations in the UK and Australia. These focused on risks related to reduced and blocked information flow because of poor technological infrastructures, mismatches between expectations of information sharing within the supply chain and lack of opportunities for team collaboration. These risks related to the availability of information typically come to the fore when information sharing and collaboration are regarded as critical to the achievement of organisational goals and tasks.

Collaborating on solutions

In these case studies, the storytelling methods we used also drew out the ways that staff collaborate to re-flow information in response to these blockages. These collaborative responses often include:

- rapport-building across and within teams so that people know who to approach for informal and ad-hoc help
- a network of people who direct the digital flow of information (a form of human signposting) between teams, departments and organisations
- the dynamic allocation of human resource to respond to complex cases of information sharing

In this respect, storytelling can be collaboratively used to develop responses to the concerns that the teams can action with the capacity that they have. Storytelling creates the space for staff to voice everyday security issues and concerns and encourages staff to take an active role in responding to these issues.

Further information at www.collectivesecurities.org

“To protect sensitive data, a number of regulations apply, including the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCIDSS).

Our Bull Trustway Suite ensures regulatory compliance by our customers and secures data from exfiltration. Through our technological partner ecosystem, we can meet any business’ encryption needs in every type of environment, in the cloud and on premise. This liberates our customers to focus on their core business with confidence. Protecting data by adhering to regulations is key to minimising cyber risk from May 2018 and beyond.

Data protection regulation is not about increasing cost; it is an opportunity to derive competitive advantage. The data protection mindset will be a critical and evolving part of business.

René Martin, Head of Data Security Products, Atos”

Deborah Dillon, Lead Auditor, Business & Platform Solutions, Atos UK&I

Getting ready for new EU data protection legislation in 2018

The General Data Protection Regulation (GDPR) comes into force across all EU member states on 25 May 2018, requiring organisations' compliance from day one. This is an overhaul of the current Data Protection Act to cover biometrics and genetic data, bringing the regulatory environment up to date in relation to Big Data. The clock is now ticking towards implementation.

Transparency and accountability

The new Regulation is designed to promote and facilitate data-sharing by putting in place appropriate principles and safeguards that protect individuals' privacy and ensure that cyber security is maintained.

Transparency and accountability are key, with extra levels of transparency for individuals around how their data is used and processed, and more rights for people who have questions about their own data.

New best practice will be to combine encryption with the anonymisation of personal information to safeguard personal details and protect against their misuse.

A new code from the Information Commissioner's Office describes the steps that organisations can take to ensure that anonymisation is conducted effectively while still retaining useful data.

Roadmap for compliance

Based on the Information Commissioner's Office best practice, organisations will need to consider the following critical questions as they prepare for GDPR:

- Do you know what personal information you hold, and on which system it resides?
- How will the 'right to be forgotten' impact your organisation?
- Will data portability have an impact?
- Do you have a Data Protection Officer that reports at board level?
- Do you have complaints from the Information Commissioner's Office and undertake root cause analysis on each case?
- Are all your Data Privacy policies updated on a regular basis and how do you check that they are effective?
- Do you delete personal information in line with a retention schedule?
- Are your models for obtaining consent in line with GDPR requirements?
- How would a GDPR fine of up to €20million affect your organisation?

Our specialists have already undertaken a detailed Data Protection Act gap analysis for organisations against their current provisions, with improvements and areas of good practice highlighted. These have been mapped to GDPR provisions to identify high-risk areas that need extra focus in the run-up to implementation and to develop a practical, prioritised roadmap for this important area of compliance. We have a wealth of cyber security tools that can assist organisations, such as encryption, prescriptive security and threat management to meet the high level of security as required by GDPR.

With these preparations in place, organisations can confidently state that they have mitigated the risks associated with the new Regulation, and can ensure data protection is built into data and analytics projects from the start. If followed correctly, the Regulation won't hinder the use of data; it will enable its wider use by helping organisations to address any risk and ensure the transparency and security of data that is needed in the digital age.

"Atos Information Governance, Risk and Compliance Consulting (IGRC) division draws on multi-sector client reach and experience."

Deborah Dillon, Lead Auditor, Business & Platform Solutions, Atos UK&I

Graham Watson, Managing Director, The Advanced Engagement Company

Risk management – the cost of the risk

It's clear that not identifying and managing cyber security risk can be costly for an organisation. Regardless of whether a share price recovers, there are painful costs associated with responding to a breach and there is undoubtedly instability within the organisation post-breach while lessons are learned.

What is less clear are some of the costs associated with implementing an effective risk management regime in order to steer an organisation away from serious impact.

Maturity

Information risk management can be a complex subject which becomes useful through the implementation of processes. Like any business process you cannot expect maturity in the short term. Maturity in risk management means that the processes are sufficiently documented, are repeatable and have permeated throughout the organisation. To reach a level of maturity where risk is sufficiently managed takes sustained effort. With maturity comes better comfort that cyber risks are managed effectively.

Culture shift

The management of risk is usually formally assigned to a small number of people within an organisation. But that's not to say that responsibility should stop there. Everyone in an organisation is responsible for risk management whether through identifying potential risks or putting in place measures to mitigate risks.

Top-level risks that are discussed at Board meetings are at least inaccurate, and at worst incomplete, if local risk issues (which bubble through various risk governance mechanisms) aren't recorded properly in, for example, departmental risk registers.

To ensuring that everyone contributes as required (not just those with formal responsibility) requires training and a cultural transformation akin to that required in a 'Digital Transformation'. Good risk habits need to be embedded throughout and this includes making sure staff are aware of cyber security threats through awareness training and other activities.

Appetite

Some of the least effective risk management regimes come about through lack of investment in engagement with senior leadership. Agreement over what is acceptable in terms of risk, through risk appetite statements, needs to be set; this can only be achieved by engaging with those who are ultimately responsible.

If there is misalignment over risk appetite, an organisation can sleep-walk into a breach that can have calamitous consequences. With well-defined risk appetite, it is easier to understand when unnecessary risk is to be avoided, mitigated or transferred.

The investment in effort to engage senior management often requires an additional element of education. While an expectation of zero security events is clearly unachievable, having an appetite for zero security breaches that lead to material impact on the organisation (where material is a defined as a value or regulatory sanction) is, as the cost of mitigations can be weighed up against this statement.

Advice

Advice in the form of consultancy, or contract staff, to fill a skills gap is likely to be required if an information security risk management regime is being implemented for the first time or if a capability is being enhanced significantly.

The cost of this can be hard to quantify in terms of a return on investment as it is not often that the implementation programme stays active long enough to understand the benefit. This might be best achieved by measuring the improvement in risk position over time once the risk management capability is in place. But even this measure is an approximation of the benefit as the impact of costly breaches will never be felt.

Putting a price on risk

Implementing an information risk management regime to avoid serious harm has a number of associated costs; aside from robust cyber security controls, the key areas to invest in to ensure your organisation is appropriately protected are culture shift, articulating appetite, and advice in order to reach an appropriate level of maturity. Measuring the benefit will give you comfort that you've spent wisely.

Christophe Moret, SVP Cyber Security Services, Atos

How organisations can protect themselves in the cyber security era

Everybody needs to be on board. Today, there are basic steps that businesses can take to protect themselves and their data against cyber attacks.

One of the simplest things to implement is to educate all staff on password etiquette and on how to be cyber aware – because everyone needs to be on board with cyber security policies, not just those working in IT.

Secondly, security should be part of the development process; systems must be designed with cyber security in mind, right from the start and not as an afterthought.

And finally, firms must assume that the right security isn't just something you can buy over the counter. Forward-thinking businesses appreciate the need for dedicated, outsourced security professionals whose full-time job it is to protect against cyber attacks.

With the right security measures in place, including maintaining appropriate levels of patching, and staying abreast of the latest threats, businesses can protect themselves and avoid becoming the next brand to hit the headlines for the wrong reasons.

Richard Vinnicombe, Practice Leader, Information Governance, Risk and Compliance, Atos UK&I

Is your organisation cyber aware? Key questions for businesses

With the protection of key information assets critically important to the sustainability of organisations, they need to be on the front foot when it comes to cyber preparedness. Too often, we see cyber security treated as an IT issue rather than the strategic risk management challenge it really is.

Businesses traditionally invest in managing risks across their enterprise, drawing effectively on senior management support, risk management policies and procedures, a risk-aware culture and the assessment of risks against objectives. When it comes to cyber security, there are many benefits to adopting a risk management approach, including:

- **Financial benefits.** These are realised through the reduction of losses and better 'value for money' potential
- **Strategic benefits.** Corporate decision-making is improved through the high visibility and understanding of risk exposure, both for individual activities and major projects, across the whole organisation
- **Operational benefits.** The business is prepared for most eventualities, with the assurance of adequate business continuity and contingency plans.

Atos' Information Governance, Risk and Compliance (IGRC) team has produced a set of questions to help any organisation to examine its cyber security risks, specifically to ensure it has the right safeguards and culture in place.

Key questions for businesses

Protection of key information assets is critical

1. How confident are you that your organisation's most important information is being properly managed and is safe from cyber threats?
2. Are you clear that your organisation is likely to be targeted?
3. Do you have a full and accurate picture of:
   - » the impact on your organisation's reputation, share price or existence if sensitive internal or customer information you hold were to be lost or stolen?
   - » the impact on the business if your online services were disrupted for a short or sustained period?

Exploring who might compromise your information and why

1. Does your organisation receive regular intelligence from the Chief Information Officer/Head of Security on who may be targeting your organisation, their methods and their motivations?
2. Do you actively encourage your technical staff to enter information-sharing exchanges with other organisations in your sector and/or across the economy to benchmark and learn from others facing the same challenges and help you to identify emerging threats?

Proactive management of the cyber risk at Board level is crucial

1. The cyber security risk can impact share value, mergers, pricing, reputation, culture, staff, information, process control, brand, technology and finance. Is your organisation confident that:
   - » an information security policy is in place, which is championed by the Board and supported through regular staff training? Are you confident the entire workforce understands and follows it?
   - » all key information assets are identified and thoroughly assessed for their vulnerability to attack?
   - » responsibility for the cyber risk has been allocated appropriately? Is it on the risk register and reviewed regularly?

Taking a top-down approach to mitigating and effectively managing cyber security is a must in today's connected world. Is your organisation cyber aware?

“After a series of high profile hacks in recent years, with serious consequences in terms of both reputation and the bottom line, no business has any excuse to ignore cyber security. But while firms know it is important to secure their data and devices, still too many small companies are leaving themselves exposed. Only just over half of IoD members have a formal cyber security strategy in place.

As data becomes more important to businesses of all types, and the regulatory environment becomes stricter, it’s vital that all companies make sure they have fully assessed the cyber risks they face. The good news is that the organisations that get on the front foot and prepare will be more resilient if they do suffer an attack, and will be able to win, and keep, the trust of customers.”

Edwin Morgan, Interim Director of Policy, Institute of Directors

McAfee

Paul Heath, Regional Sales Director, UK&I Public Sector, McAfee

Transformation, not just security!

Most cyber security environments are a patchwork of products accumulated and implemented over many years. They're complex, cumbersome, and frustratingly difficult to manage. Worse, they're typically fragmented and have gaps that are open invitations to cyber adversaries. Security that is so complex that it doesn't truly secure you, is just as dangerous as a cyber adversary.

Imagine a cyber environment with an open integration fabric that allows all your disparate products to co-exist, communicate, and share threat intelligence with each other. Where machine automation is converged with human intelligence so you can streamline workflows more efficiently. Where your team is freed from unnecessary operational burden and is empowered to strategically fight adversaries. Where you can monitor all things security through a single management system. Where all your security products work synergistically across the threat defence lifecycle – protection, detection, and correction – by skilfully adapting to new threats. So your workforce leaps forward in productivity and your business surges ahead confidently. It's the power of cyber security products working together, working for you. So, what do we need to focus on?

- **Cooperation first.** No one vendor or technology can do this alone. Best of breed isn't going away, nor should it. But you need product vendors and system integrators that acknowledge security is too fragmented, and are working cooperatively to build meaningful integrations.

- **Automation is key.** Automation is the future of security. It eliminates routine tasks, enables faster new hire onboarding, and frees your strongest talent to tackle your hardest problems. The IT landscape is too vast and threats are evolving too fast to rely on manual process alone.

- **Better architecture.** You need a better architecture, not just another product. To transform fragmented security, you need a unifying architectural approach that delivers a fundamental integration and management layer which is freely available and vendor agnostic.

But to achieve this we need to fundamentally change the way we are thinking about Security. Often we find it is an afterthought, a 'bolt on' or thought of as just another compliance issue (which is the case sometimes with General Data Protection Regulation (GDPR)). Open Integration, automation and an orchestrated platform approach will provide the building blocks to transform organisations in an era of ever increasing threat and ever reducing available human resource. However, it will enable visionary organisations to reduce the impact of cyber threats, do more with their human cyber resource and perhaps use things like GDPR as a transformational catalyst and a way of providing enhanced and beyond-compliance secure services to citizens and consumers.

Find out more about how McAfee and Atos are working together here: https://www.mcafee.com/uk/resources/case-studies/cs-atos.pdf

Phil Aitchison, Head of Cyber Security & Mission Critical Systems, Atos UK&I

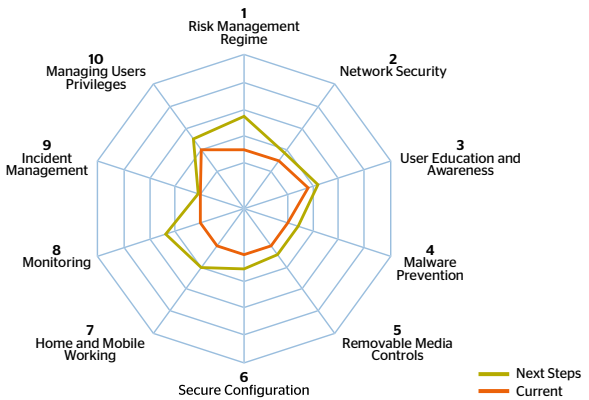
Understanding your exposure to the evolving cyber threat

The explosion in the numbers of connected devices and the Internet of Things presents a radical expansion in the attack surface of organisations already vulnerable to a cyber attack. No longer can a network perimeter be defined or protected. We live in a world where inter-connectivity and open collaboration is the norm. While today's systems are often more complex, the legacy of 20th century IT includes swathes of vulnerable code and insecure data exchanges.

It's not just about compliance

The assorted tools and techniques available for compromising sensitive data are well documented. Attacks are increasingly tailored towards the internet footprint of individual employees or targeted at specific systems. What is less clear is why cyber threats are evolving so fast. To combat this evolving threat landscape, organisations must move away from a compliance mentality where they report on where data is stored, monitor who has access to it and react to cyber events (malicious or accidental) to become more risk-aware and intelligence-led.

To this end, the National Cyber Security Centre arm of GCHQ has published 10 Steps to Cyber Security written in plain English to help businesses to understand the practical steps required. Atos uses this guidance to judge how well an organisation is currently protected by overall services from existing supplier contracts. The maturity of this protection can then be measured to identify gaps and ascertain if additional work is required.



Cyber Security Maturity Model
(based on NCSC Ten Steps to Cyber Security)

Essential capabilities

Business leaders, shareholders, employees, politicians and citizens all look to organisations to act in their best interests to safeguard personal data. With the arrival of the General Data Protection Regulation (GDPR) and the significant penalties that could result from a security breach (up to 4% of annual turnover), a successful attack could significantly impact the bottom line, affect the share price or even compromise an organisation's very existence.

In this context, organisations need to fully understand the business impact of the evolving cyber threat. Sure, they must deploy security controls that will defend sensitive data against specific threats; but they must also ensure the overall cyber resilience of the organisation itself. In essence, that means being able to:

- not only detect the presence of a compromise, but also to react to the rapid escalation of a successful cyber attack
- test the organisation's ability to recover mission-critical operations from a cyber incident and optimise basic IT hygiene such as regular patching, version control and asset control
- quantify cyber risks faced by the organisation and structure accordingly to safeguard the interests of citizens, customers, employees and shareholders.

Atos supports its customers on this journey to improve their resilience in response to the changing threat landscape. We offer an end-to-end solution to help our customers detect, react and recover operations from today's continuous and evolving cyber threats.

“

It’s absolutely crucial that UK industry is protected against this [cyber] threat - because our economy is a digital economy. Over 95% of businesses have internet access. Over 60% of employees use computers at work. The internet is used daily by over 80% of adults - and four out of five people in the UK bought something online in the past year. And we know the costs of a successful attack can be huge.

My message today is clear: if you’re not concentrating on cyber, you are courting chaos and catering to criminals...This is one of the reasons we created the new National Cyber Security Centre, which aims to make the UK the safest place to live and do business online.

”

IoD conference 2017

The Rt Hon Matt Hancock MP, Minister of State for Digital, UK Government

Expecting the unexpected

Securing the Olympic Games Rio 2016

The Olympic and Paralympic Games have – once again – seen unprecedented feats of strength, resilience and focus. With many new records set, we've seen record figures of our own. The number of IT security events detected at the Olympic Games Rio 2016 were a staggering 570 million, which means 400 per second. While this is a breath-taking figure in its own right, it's also double the equivalent figure from the London 2012 Olympic Games.

When it comes to providing water-tight IT security in environments with immovable deadlines and zero tolerance for failure, the trick is to expect the unexpected. The ingenuity and sophistication of cyber-criminals demands to be taken seriously – every day hackers work to come up with new ways to disrupt IT systems, and in return corporations have to keep one step ahead to ensure their systems and data remain secure.

We left absolutely nothing to chance. Prior to the event, we undertook 200,000 hours of testing and full 'dress rehearsals', testing literally thousands of different scenarios. During the event, our team of experts in the Technical Operations Centre in Rio worked 24/7, diligently scrutinising everything flowing through the network. We collected and analysed more data than ever – which was exactly what we had prepared for.

With a large increase in "digital noise" at this year's Olympic Games it was imperative that we were able to cut through it, to identify genuinely suspicious behaviour. This involved a combination of using the very latest complex-data analytics to look for patterns, flagging the right items for our team of experts to make a "human call" on, and then feeding all of it back into the mix, in real-time, to strengthen our learning and to continue to stay ahead.

Having the confidence that everything was secure, accurate and reliable allowed our other teams to get on with using the vast amounts of complex data being generated by the events themselves. The Atos team, in conjunction with our partners, worked tirelessly to ensure that this information was delivered successfully, allowing the world to share in real time in the most connected way yet.

We expect that PyeongChang 2018 and Tokyo 2020 will once again break records and go further. And we're already preparing!

Over
500M
security events

400
security events per second

23,000
significant events processed by the Technology Operations Centre

20
critical events stopped

0
incidents impacted live games


20:44:28

Zeina Zakhour, Distinguished Expert, Global Chief Technical Officer, Cyber Security, Atos

Prescriptive Security: using the haystack to find the needle

In our increasingly data-driven world, organisations are engaged in a race to gather operational and customer data and apply analytics to transform that data into valuable business insights. Yet one important application that is still rarely addressed is cyber security data analytics.

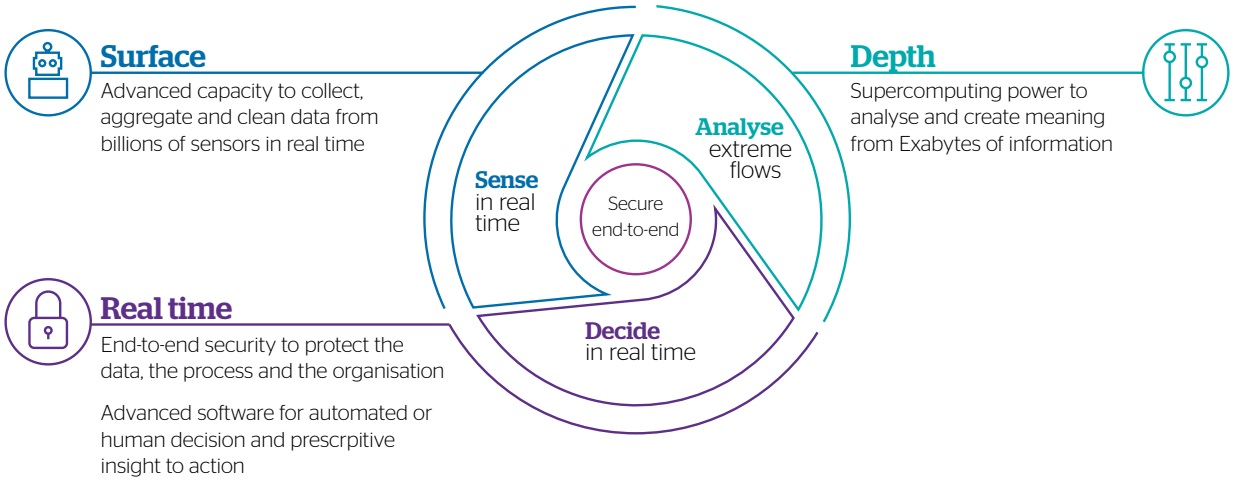
From proactive to prescriptive

We regularly hear about major cyber security breaches and wonder whether they were preventable. Prescriptive Security is about exactly that: preventing breaches from happening by leveraging big data and supercomputing capabilities. As technologies advance, cyber security is shifting away from a reactive and proactive model to a prescriptive model that can analyse analytics patterns in order to identity the next threats and to automate the security control responses.

While cyber security has been focused on finding the needle in the haystack, Prescriptive Security instead uses the haystack to find the needle by leveraging big data and machine learning analytics and utilising all data generated within the organisation and outside the organisation, in order to bring 360° security visibility and eliminate all potential blind-spots.

With a Prescriptive Security Operations Centre (SOC), organisations will be able to:

- **Face the ever-evolving threat landscape:** The threat landscape has been increasing exponentially as the adoption of new technologies such as Internet of Things (IoT), big data and cloud computing are expanding the attack surface. Every three months, over 18 million new malware samples are captured, with zero-day exploits (malware that goes undetected by traditional anti-virus software) expected to rise from one per week in 2015 to one per day by 2021. With Prescriptive Security, threat intelligence is no longer a separate technology-watching process managed through alert bulletins, but an integrated part of the SOC where threat intelligence feeds give actionable risk scorings and can detect unknown threats before they even reach the organisation



- **Significantly improve detection and response times:** Time is on the side of any adversary who is patient, persistent and creative. We're fighting human ingenuity and attackers aren't playing by the same rules as we are. Prescriptive SOCs can change current operational models and considerably improve detection times and response times. Instead of thinking in days and months to detect and correct threats, with machine learning and automation we can neutralise emerging threats in real time and prevent future attacks

- **Optimise cyber security resources:** While cyber attacks are growing in volume, complexity and pervasiveness, organisations will need to counter these using limited resources. The latest research estimates that by 2020, over 1.8 million cyber security jobs will not be filled due to a shortage of skills. Prescriptive Security, by introducing artificial intelligence and automatic response, will optimise the use of cyber security professionals who will be able to automate responses to common cyber attacks and focus on the more complex and persistent ones. It will also introduce new cyber security roles, such as cyber security data scientists to integrate statistical and mathematical models and provide innovative mechanisms to detect future cyber attacks.

Next-generation infrastructure

Prescriptive Security advances a tri-dimensional paradigm by increasing the detection surface, increasing the velocity of response and decreasing the reaction time. By using big data, analytics and supercomputing, it also effectively optimises the cost factor (human resources cost plus storage/compute power costs).

Prescriptive Security SOCs will be the next-generation cyber security infrastructure that the digital economy needs to enable and engender confidence. With this in place, organisations will be able to effectively protect their business assets including valuable business data and customer personal data.

Role of a Security Operations Centre (SOC)

A SOC is a secure facility equipped to function as the central hub for cyber security incident prevention, detection and response capabilities. SOCs are usually manned 24 hour a day, 7 days a week, 365 days a year by SOC Analysts and Incident Response teams. Atos has a network of 14 24x7 Security Operations Centres worldwide providing cyber security services to national and global clients across all sectors.

Crispin Keable, Distinguished Expert for High Performance Computing, Atos UK&I

Why is AI suddenly a thing, and do we need machine ethics?

Artificial intelligence (AI) as a science has been around since the dawn of the computer era. Yet, while computers have transformed almost every domain of business, leisure and human endeavour, AI has not managed to climb out of the laboratory. The early claims of AI could be considered hubristic, with researchers in the 1970s expecting computers to do the work of the average human within a few years!

AI's leap: learning from experience

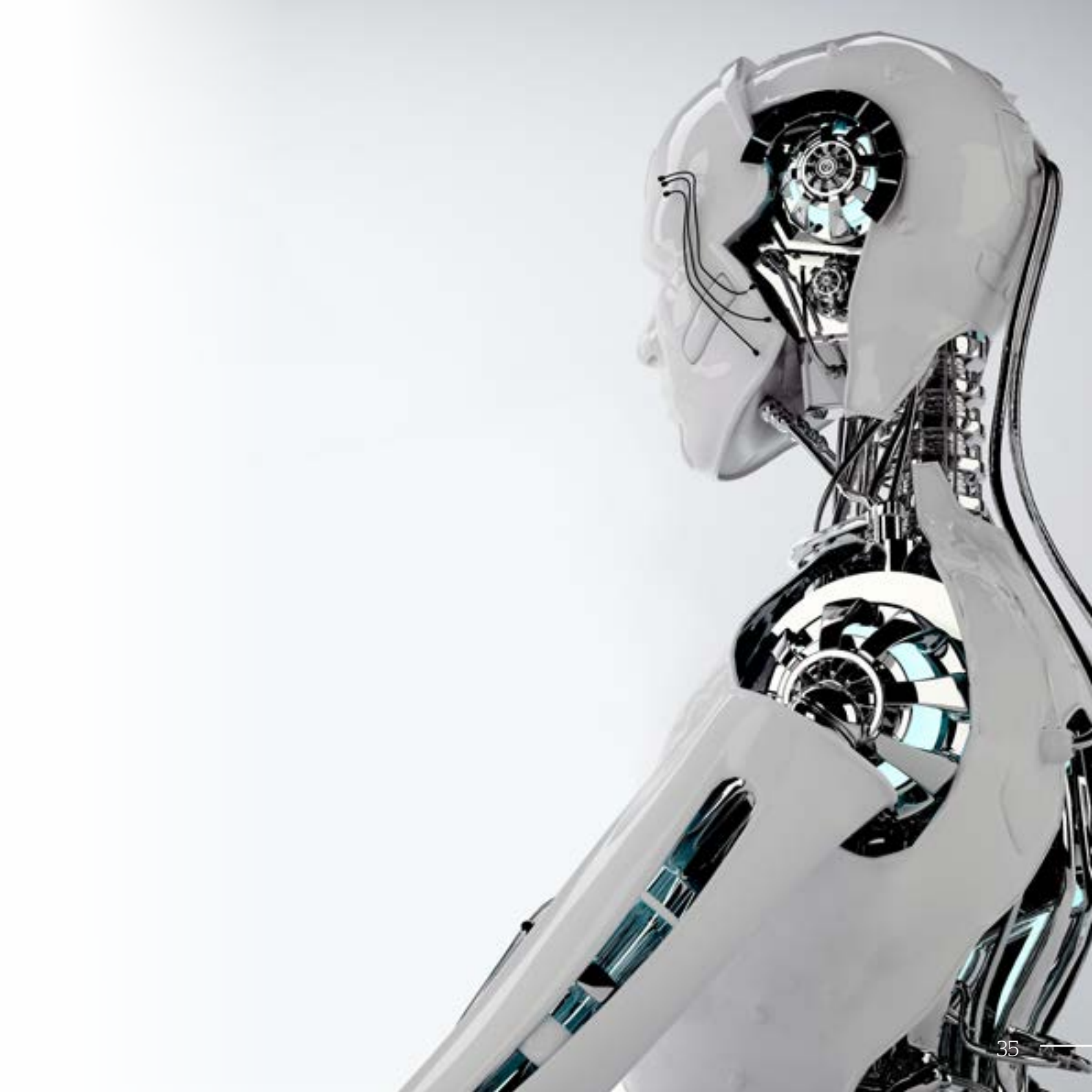
Many apparently-simple human problems, such as recognising a face or crossing a room without bumping into things, are fantastically complex feats of computing. In the real world, everything depends on everything else, which means that the number of relationships between things rapidly outstrips '70s' era, or even contemporary, computing. Computers that address this problem using traditional IT methods of 'if this happens, then do that' are bound to fail as the number of 'ifs and thens' balloons exponentially. Even humans, with the 100 billion neurons in our skulls (that's one neuron for every star in the galaxy) can't do *that*.

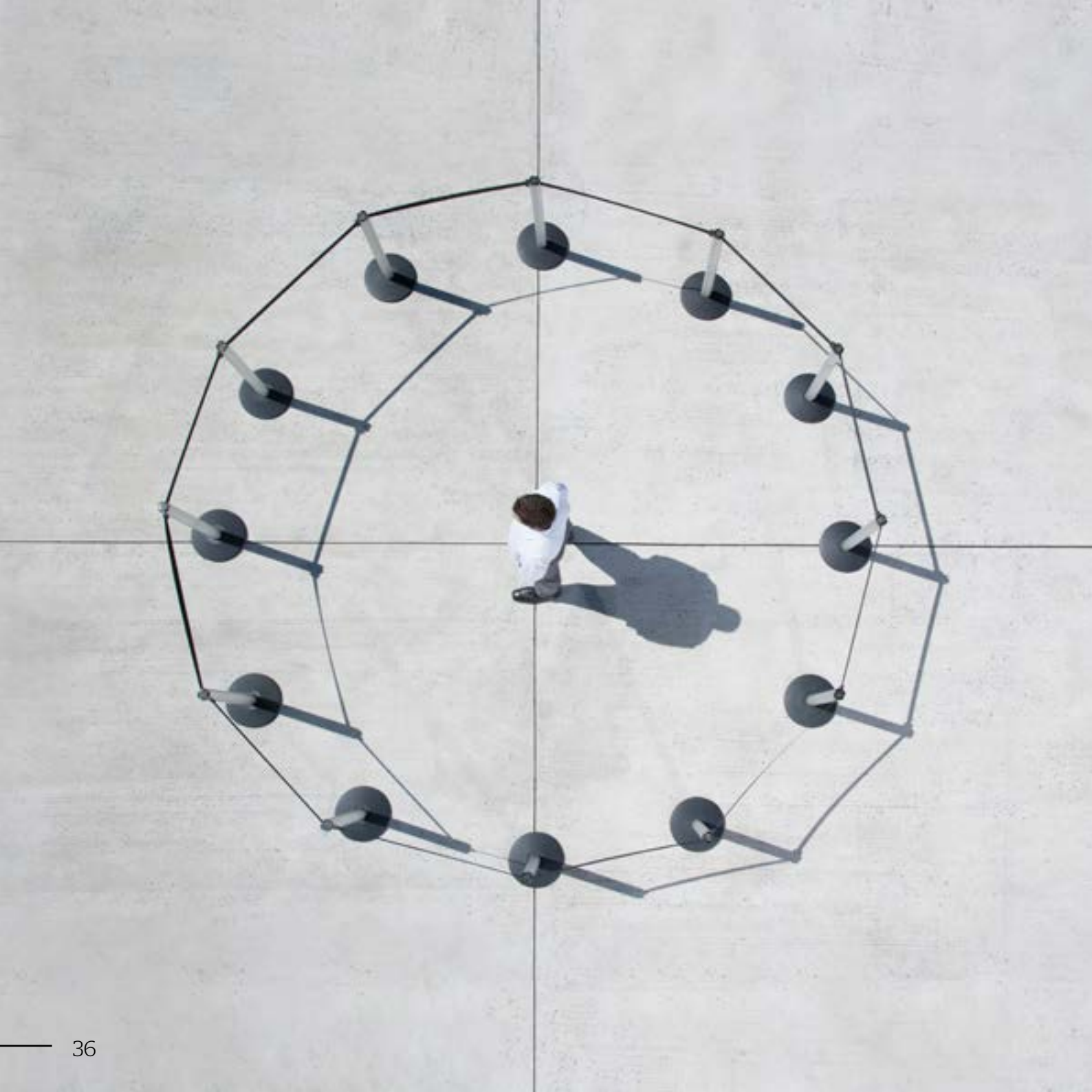
What people have evolved to do, and what we are beginning to see in AI systems, is the ability to learn from all the 'what ifs' on the basis of experience. This is what you spend your early years doing, and why AI systems need very large training datasets in order to 'learn'. Through the internet, the sheer volumes of data available to work with have risen dramatically. This, by itself, did not lead to the leap in performance needed to make AI useful. The key to improving performance was to expand the scale and power of the AI systems used (called deep learning) and then remove the processing bottlenecks using high performance computing. This has produced more complex and useful applications of AI, such as image analysis or use of voice controls: think Siri, Cortana, Google Assistant and Alexa.

Ethics of learning

While there are higher-value applications of these capabilities (such as systems that can identify tumours from mammograms at least as effectively as the best doctor can), there are also new challenges about what these technologies 'learn' from the training datasets. Recent media attention has focused on big failed AI projects like a US court system which over-predicts re-offending by people of colour (racist AI!), and an experimental Microsoft chat-bot that had to be switched off after 24 hours after it started spewing ultra-right-wing propaganda (fascist AI!).

Does the answer lie in an ethics module for AI systems? Almost certainly not, since AIs are engineered systems that only work according to their design parameters. They don't have intention or goals of their own, so the idea of an ethics module has no meaning. What is required is a re-think of how these systems are engineered and consider not just 'is this system powerful enough?'. But also 'what moral or ethical norm is impacted here?'. What is certain is that these questions will be addressed not only by data scientists and engineers, but also CEOs and politicians; and the question of ethics will evolve to a question of trusting those in authority to use or allow the use of such computing power within a framework that is appropriate and societally acceptable.





DARKTRACE

Mariana Pereira, Director, Darktrace

The advent of the self-defending network

Cyber security is one of the greatest technical challenges of our day. Nation states, enterprises and individuals are routinely outpaced both by sophisticated attackers and internal threats who are successful not only in infiltrating fortified network borders, but also in going unnoticed inside systems for long periods of time.

Changing threat landscape

The danger is not just the classic scenario of information being stolen, or a website being defaced, but also the quiet and unseen threat – attackers that creep in and can change your systems at will, or install kill switches ready to be activated. These attacks are sophisticated, using previously unseen custom code, only crossing the boundary defences once, never sending information out. They may only be active for a few seconds a year, but when commanded to act, they are fatal. At the other end of the threat spectrum, we have seen the proliferation of brute-force attacks that can spread across organisations in mere minutes, leaving virtual ashes in their wake.

The reality is that the old approaches of looking at yesterday's attack to predict those of tomorrow are failing. Attempt to stop threats at the network boundary by pre-defining the threat in advance is futile in the face of 'unknown unknown' attacks – Petya/NotPetya was able to wreak considerable havoc, despite being only a slight variation of WannaCry, which had incapacitated organisations across the globe only a few weeks prior.

In addition, due to the exploding complexity of today's businesses, attempting to define the network boundary is virtually impossible; the rapid spread of Internet of Things (IoT) devices, bring-your-own-device policies and distributed infrastructures mean that organisations often lack full visibility into their networks with security professionals routinely underestimating the number of devices on their networks by as much as 25%. Insider threat, both malicious and inadvertent, adds another dimension to the challenge of cyber security. In an age of limitless data and complex networks, there is simply too *much* happening, too *quickly*, for legacy information security methods to be able to deal with.

Digital immune systems

Instead of trying to predict the hallmarks of the next WannaCry, organisations are increasingly turning to the latest advancements in probabilistic mathematics and artificial intelligence to defend their networks from the inside out. This new class of technology mimics the self-learning intelligence of the human immune system to autonomously detect and respond to emerging attacks in real-time, augmenting security teams and arming them with the tools to stay ahead of both fast-spreading, brazen attacks, and stealthy and silent threats that lie low in networks.

The Artificial Intelligence (AI) algorithms self-learn the 'pattern of life' for every user and device on a network and use that constantly evolving understanding to identify and halt in-progress attacks by generating a precise, targeted remedial action akin to 'digital antibodies'. Acting as a force multiplier for the security team, these 'immune system' technologies can autonomously slow down or stop a threatening connection, preventing infections such as ransomware from spreading and inflicting damage until the human team has been able to catch up.

Unlike traditional security tools, this machine learning approach thrives on the complexity of networks and the vast amounts of data running through them. It does not rely on any data training or human intervention, but intelligently learns what is 'normal' for every different network it is deployed in. This fundamental power of the technology to build a sense of 'self' for the health of an organisation and leverage that knowledge to autonomously take proportionate remedial action marks the advent of the first self-defending networks that can inoculate themselves against threats from within, including 'unknown unknowns'.

Atos cyber security expertise

Phil Aitchison
Head of Cyber Security & Mission Critical Systems, Atos UK&I

Role
Phil leads the team responsible for the design, build and running of Atos UK&I's cyber security portfolio. Currently, he is executing our strategy to work with clients to apply cyber security controls into the digital transformation of public services and private sector organisations.

Qualifications
Phil has 15 years' experience in developing and delivering mission-critical infrastructure, cyber resilience and surveillance solutions for critical national infrastructure clients. Educated in Scotland at Strathclyde Business School, Phil holds a First-class Masters Degree in Business & Technology from University College Dublin.

Hobbies
Cycling, running, swimming and skiing.

How would you define cyber security?
For me, cyber is all about securing your digital transformation. Granted, every organisations must improve how they detect, react to and recover from cyber compromise. However, effective cyber cannot be an afterthought, it needs to run through how organisations will operate in the digital world.

Zeina Zakhour
Distinguished Expert, Global Chief Technical Officer, Cyber Security, Atos

Role
Zeina creates innovative solutions to stay a step ahead of cyber criminals. She covers the full spectrum of cyber security, from security advisory to security integration, managed security services and IoT and Big Data security. She works closely with Fortune 500 companies to advise them on their security strategy, secure their infrastructure and protect their data.

Qualifications
Bachelor of Engineering in C.C.E from Notre Dame University Lebanon, M.Sc. from Telecom Sud Paris and an Executive MBA from HEC. Also a Certified Information Systems Security Professional (CISSP) and a certified ISO 27005 Risk Manager.

Hobbies
Snorkelling, Phoenician civilisation, astronomy, piano.

How would you define cyber security?
Cyber security is about building trust: trust in the digital world of today, trust in disruptive technological innovations to come.

Sandy Forrest
Client Executive, Cyber Security, Atos UK&I

Role
Responsible for coordinating end-to-end cyber security capability (advice, services and products).

Previously, Sandy oversaw delivery of IT Services to the UK's National Security and Intelligence sector. For the London 2012 Olympic Games he was the liaison between Atos (as Worldwide Information Technology Partner for the Olympic Games), the Intelligence Agencies and the Olympic Security Directorate. He currently sits on the Mayor of London's Cyber Security Advisory Panel.

Qualifications
30 years in law enforcement and eight years as Atos Client Executive in the field of cyber and national security.

Hobbies
Motorcycles and skiing.

How would you define cyber security?
Cyber Security is currently seen as an overhead. For me, it should instead be seen as a secure business enabler that can deliver competitive advantage.

Big Data & Security Division

4,500
security professionals in Atos globally

14
Security Operation Centres worldwide

100
million sec events handled per hour

Atos is
No.1
in Europe

Alison Devenish, Head of Workforce Management, Atos UK&I

Cyber security skills gap: a UK view

The challenge to create and sustain a modern, skilled cyber security workforce affects integrators, vendors, managed service providers and their end customers all over the world.

According to Cisco, there are now around one million unfilled cyber security jobs worldwide, with Symantec predicting that by 2019 the number will be 1.5 million[1]. The demand for cyber security skills is reported to be strongest in Israel, Ireland and the UK; only in the US and Canada does the supply exceed more than 50% of the demand.

National Cyber Security Strategy

In the UK, where employer demand for cyber security jobs has exceeded candidate interest by more than three times, the Government's 2016 National Cyber Security Strategy[2] highlights the potential impact of this on our economy, with a collaborative approach to addressing it, involving a range of participants and influencers across the Devolved Administrations, public sector, education providers, academic bodies and industry. At Atos, we would go further and argue for closer collaboration across supply chains led by relevant regulators. The Government's Strategy concludes that this will require action over the next 20 years and will entail integrating cyber security into the education system. It also recognises a substantial gender and diversity imbalance in cyber-focused professions. The National Cyber Security Centre, which was launched earlier this year, has a key objective to develop the UK's cyber skills, and projects have been established to encourage that at all levels, from the CyberFirst programme for teenagers to professional certification for professionals.

Societal change

This is not a short-term skills gap; it is a societal change whereby stakeholders join forces to capitalise on the advantages of digital transformation whilst addressing the inherent risk of universal interconnectivity. This requires a root-and-branch approach to nurturing cyber skills from the early stages of education through to re-skilling traditional workers to equip them to protect the integrity of the digital economy. The UK Government's aspiration is that by 2021, cyber security is taught effectively as an integral part of relevant courses from primary to post-graduate level, by which time the UK will have strengthened its position as a world leader in cyber science and technology.

How Atos is responding

Atos has recognised the extent of the cyber skills challenge and already embarked on a proactive future-skilling programme with our UK workforce.

- Our cyber security skills programme was initiated with an internal recruitment campaign inviting employees to join our Cyber Security practice and participate in a Cyber Academy to equip them with the knowledge to complement their existing skills and experience to take up new roles in cyber security. We have successfully reskilled 30 Atos employees who are now in their second year of operating within our Cyber Security practice.

- We are also proactively developing future skills within our workforce through our 'Future Fit' programme, which invites employees to join a Digital Growth Network in Cyber Security. This enables them to follow a long-term curriculum of learning (including certification), alongside their current roles, to keep in-step with the evolving cyber threat and benefit from mentoring from our more experienced cyber security professionals. All this accelerates the readiness of employees to apply for cyber security roles across UK.

- Given the Government Apprenticeship Levy to increase the number of apprentices, Atos, in conjunction with our learning partner QA, offers opportunities to complete training and certification that will result in apprenticeship accreditation at different levels. We provide a pathway to enable technical graduates coming straight from numerate disciplines, experienced professionals looking to change careers, degree apprentices or non-tech graduates converting to technology roles to pursue the learning and certification needed to develop a career in cyber security.

[1]http://www.itproportal.com/2016/01/14/uk-government-gets-serious-developing-security-skills-in-2016
[2]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf and
[2]https://www.ncsc.gov.uk/information/cyberfirst-courses

Women in cyber

A diverse set of backgrounds and talents is essential to build the cyber security workforce of the future, yet women make up only 11% of the cyber workforce. Why is this? Is it due to differences in educational background, less support for women to advance in the profession, or a simple lack of awareness of career opportunities in the field?

Atos attends career fairs through STEMNET (Science, Technology, Engineering and Maths) at schools and universities, actively encouraging young women to consider a career in technology. While roles like security analysts are in high demand, the cyber security field has a complete ecosystem of positions, from human resource professionals to designers, business strategists and product developers.

Awareness programmes such as STEM Ambassadors, #IBMCyberDay4Girls, GenCyber and Girls Who Code can make all the difference by reaching girls at a young age. Collaboration is also key: cyber security leaders need to take an active role in working with educators to drive awareness and training for the next generation of security professionals. In addition, ongoing development and support is important to attracting, developing and retaining women in cyber security. The Gender Network provides advice as well as mentoring for women across Atos.

Laura Rutter, STEM Ambassador, Atos UK&I

Developing the next generation

In response to the growing demand for cyber security skills, Atos recently established its Cyber Security Academy.

Ember Ellis, Security Operations Centre Cyber Security Specialist

Current Role: *Work in the Atos Big Data and Security UK&I division Operations team at the Moray Security Operations Centre (SOC), providing services to clients in the public and private sectors. First point of contact for the Security Operations Analysts within the SOC for nominated accounts, deputising for the SOC Manager when required.*

I joined Atos as an Apprentice Information Security Specialist in March 2015, working in the Moray Development and Innovation Centre in Forres. My apprenticeship started with an intensive training programme with courses ranging from Network and Information Security Fundamentals to Malware Analysis and Penetration Testing. This gave me all the valuable skills needed to get up and running in the world of cyber security. After completing my apprenticeship coursework, I achieved a Scottish Credit and Qualifications Framework Level 8 Diploma for Information Security Professionals and began working on live work, providing services to clients. I've learned to utilise a range of tools and systems to monitor customer networks for malware and intrusion attempts, conducting investigations when required to maintain the security of our customers' IT systems.

As a result of this, I was promoted to SOC Cyber Security Specialist. I also studied for and passed the exam to become a Systems Security Certified Practitioner and I have recently accepted an offer to study for a GCHQ certified MSc in Advanced Security and Digital Forensics with Edinburgh Napier University. I would like to work on threat intelligence and, in the future, forensics.

Cyber security is currently a male-dominated area. I want the representation of women in the industry to be higher and for women to see that cyber security is an amazingly interesting field to work in that offers tremendous opportunities for development.

Lewis Currie, Security Operations Analyst

Current role: *Part of the Atos Big Data and Security UK&I division in the Moray Security Operations Centre (SOC), working for customers in the public and private sectors. Duties include monitoring security systems, maintaining and checking the health of networks and servers and compiling security reports.*

I joined the Atos Moray Security Operations Centre (SOC) in Forres as an Apprentice Information Security Specialist in March 2015. It has been a fantastic opportunity, enabling me to build up a variety of skills and successfully integrate into the workplace.

As a young person straight out of school, I've gained great experience and insight into the work environment and, from the start, I was made to feel part of the team. The training I received has built and developed my cyber security skills immensely and helped me into the role of a Security Operations Analyst. Some of these skills include: a deep understanding of security and computer networks, knowledge of monitoring and Security Information and Event Management (SIEM) software, and a new grasp on security reporting and data filtering. I feel that I have come a long way in my knowledge of security systems and the cyber security landscape as a whole. During my training, I engaged in a variety of interesting courses including: Cisco Networking Fundamentals, Penetration Testing, Linux Fundamentals and ITIL. As well as this, there were team building exercises which allowed me to get to know my colleagues.

So far, the work I have undertaken has provided constant challenges, enabling me to push my new-found skills and apply them to adaptive and dynamic situations. I am aware that more challenging cyber security work is in the pipeline and I look forward to working towards new horizons.

Kulveer Ranger, Vice President, Strategy & Communications, Atos UK&I

How secure is my cyber security? And who will protect me?

From out of the shadows, the real and perceived issue of cyber vulnerability has rocketed up the public, political and business agenda and is clearly one that is not going away. For IT providers and the broader technology industry, keeping customers safe and secure is as fundamental as effective service delivery and good design architecture.

The changing dynamics and growing awareness of system and network security mean that the entire technology sector must continue leading the war against globalised and agile cyber-criminal opponents while also minimising the impacts of any attack. However, we must also work to establish a broader understanding and narrative that can generate trust and confidence for our customers and their customers in the face of this threat.

A new dimension

It is often said that the first duty of any government is to keep its citizens safe. So if cyber security is an issue for us all, what is the role of government and how can it protect us from the globalised threat of cyber crime? No hard borders, no physical visibility, no known location: this threat exists in a new digital dimension and our collective vulnerability is increasing in line with the exponential growth of technology and its assimilation into every facet of our lives.

It feels as if the question of who is responsible for our cyber security is migrating away from the individual. I am sure we can all recall the days when we simply downloaded anti-virus software to our personal computer, and organisations established 'firewalls' around their networks to keep them safe. Now things are significantly more fluid. Our data is located in 'clouds'. We carry out financial transactions anywhere. Social and work-based communication networks overlap. We operate our own 'personal digital ecosystems' of devices, networks and connectivity in trains, planes, offices, homes, coffee shops – basically, everywhere!

Scrutiny and confidence

Politicians have become increasingly apt, and rightly so, at calling industry to account. The ethics of business and the rights of customers to get a fair service regularly face the disinfecting light of political scrutiny.

The relationship of workers with large global corporates has also become so stretched that the analogy of David and Goliath is no longer nearly enough to describe the gulf that exists between people and some businesses. So, politicians are stepping in to protect individuals, redress the balance and ensure that the contract between customer and corporate does not snap.

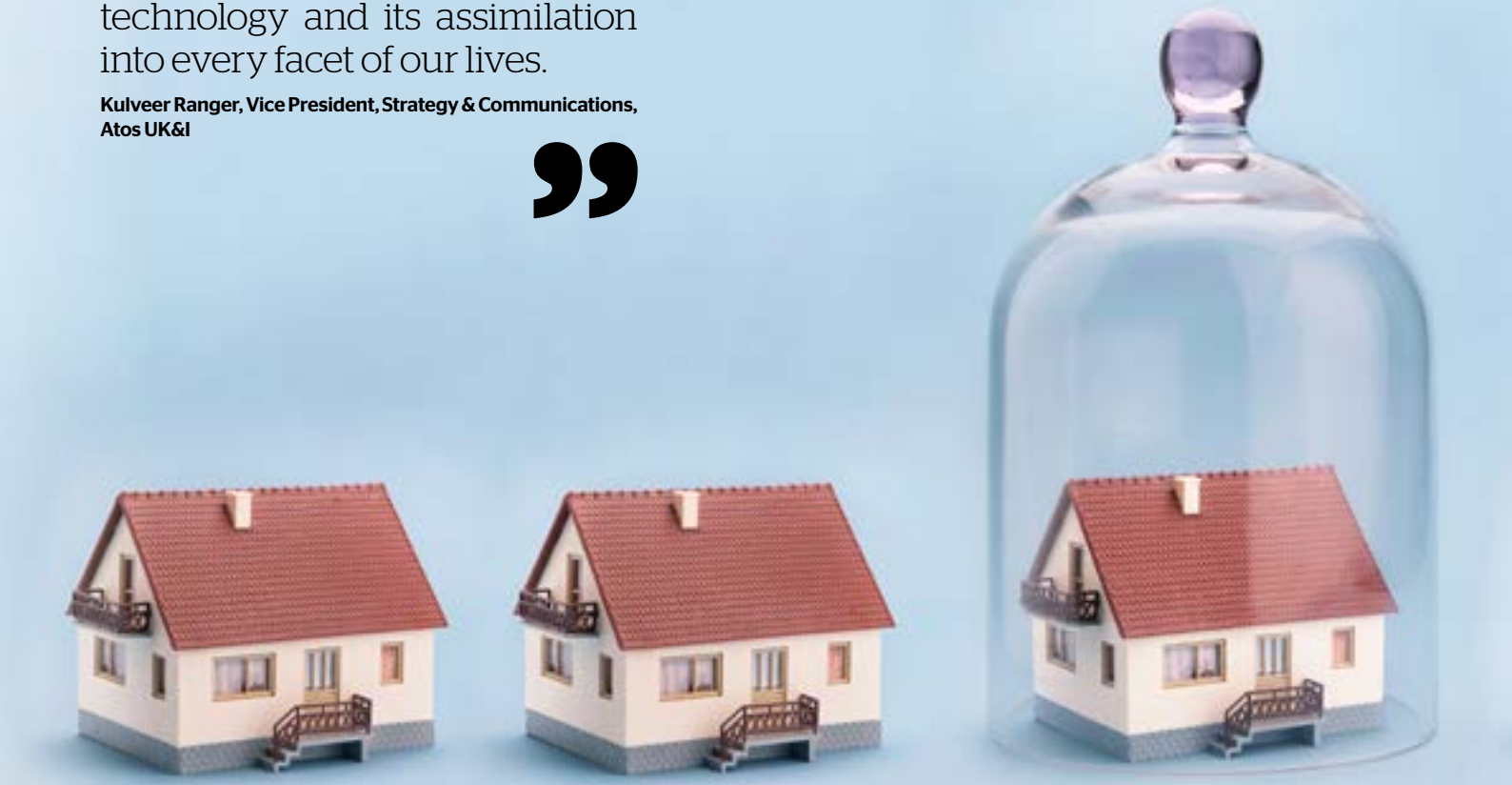
The private sector, obviously, wants to play its part. Businesses thrive on confidence and trust; both consumer and political confidence are essential as the technological revolution continues to accelerate. Companies are working hard on transparency, establishing more governance and better codes to demonstrate their moral compass and sense of responsibility. But the silent antagonist, the villain who doesn't care about any of the rules – and is in fact determined to break them – is the cyber criminal.

National strategies

The question of how we are protected from this prevailing threat of our times involves no one individual, politician or organisation. There is no linear answer. Like any fight against crime, this will be a demanding and ongoing battle that will require national leadership, the best expertise and closer collaboration. We must look to both industry and the public bodies to seek to establish new strong structures. While the National Cyber Security Centre and supporting government strategies are a start, going forward we will require much more. The day is nearing when we will need the formation of a National Digital Security Force. Where we can report cyber crime, whether it is theft of crypto currency or 'bots' carrying out phishing attacks to try to corrupt our digital accounts. A new protection service that can investigate larger-scale crime and provide us all with the thin blue digital line of confidence in the ever-expanding and exciting cyber world we now increasingly inhabit.

> This threat exists in a new digital dimension and our collective vulnerability is increasing in line with the exponential growth of technology and its assimilation into every facet of our lives.

Kulveer Ranger, Vice President, Strategy & Communications, Atos UK&I



Edinburgh Napier UNIVERSITY

Professor Bill Buchanan OBE, FBCS Leader, The Cyber Academy, Edinburgh Napier University

Securing citizen-centred public services

In 10 years' time, we will look back to 2017 and think how old-fashioned businesses were in not closing the gap between technologies and the needs of users. Over the coming years, the experiences of users will transform – not least when it comes to the delivery of public services.

Empowering and protecting citizens

Digital giants such as Google and Facebook can pinpoint users across the world on any device with the purpose of targeting advertisements at them. Yet many of our interactions with government are still done on paper. Bringing our public services fully into the 21st century requires public and private sector partners to work together to re-engineer infrastructures in a way that empowers citizens while keeping data secure and respecting the privacy of the individual. Some cities show signs of starting to create a more citizen-centred infrastructure, for example London's e-Red book for monitoring a baby's progress (replacing the old paper version). However, this is far from the future of an integrated digital health and social care record owned and controlled by each individual citizen.

The level of transformation that is now needed depends on moving IT systems to the cloud as a massive computational resource. Once systems and data are cloud-based, public bodies can deliver much easier, faster, more efficient and seamless online services in a way that has never before been possible. To achieve this, there are three major cyber security challenges: building a more trustworthy internet; protecting critical infrastructure and data; and defining a common framework for cyber-related skills.

Building a trustworthy internet

The internet that has been created up until now brings inherent risks that new cyber security strategies can address. Today, the relative lack of security protocols online means that we often cannot tell if the email we have received is really from the person who appears to have sent it and that no-one has read or tampered with it. At the same time, a fully secured online signature is much more secure than a wet signature or a traditional photo ID, yet still we use wet signatures for many important transactions and we will mark a piece of paper with an X at a polling station.

Looking forward, it is encryption that will enable us to keep things confidential and to validate the trustworthiness of objects and people. Unfortunately, there is no single encryption technique that can provide all these things; often different encryption techniques must be combined; and there are complexities in using encryption for data that is at rest, on the move and being processed, and in how we use digital signatures to prove identity. We need to develop a deeper understanding of how encryption can not only protect the privacy of data, but also improve the trustworthiness of everything that happens in a connected world.

Protecting critical infrastructure and data

The arrival of the General Data Protection Regulation (GDPR) is prompting many businesses to look hard at what personal data they need to store and how access to their data is controlled. Along with GDPR, we see the Network Infrastructure Systems (NIS) directive, which will fine organisations for a failure to protect critical systems such as energy, health, transport and water.

While all data needs to be secure, not all of it needs to be stored in the same way as personal data. As more businesses move to the cloud, cyber security needs to be in-built into the new infrastructure. As part of this, it's important to classify data according to business need, anonymise data where appropriate, and strengthen control of who has access to what types of data. To reduce complexity, the approach needs to become more 'event-driven', defining rules for how data and access are controlled according to different events.

Creating a cyber-ready workforce

To maintain cyber security, we need to create a workforce that is cyber aware and be able to match training, education and skills developments into a common framework which academia, industry, law enforcement and the public sector can all refer to and understand. In this, National Institute of Standards and Technologies (NSIT) have excelled with their

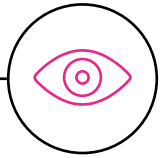
[1]National Institute of Standards and Technologies, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF)," NIST Spec. Publ., p. 130, 2016.

National Initiative for Cybersecurity Education Cybersecurity Workforce Framework[1]. Within it they define: seven categories; 33 specialty areas; and 52 work roles, and then map these to 1,007 tasks, 374 skills, 630 knowledge areas and 176 abilities. This is the first-ever mapping which starts to work through roles and can be used to understand how to develop training programmes and how academic programmes can be developed.

> “A fully secured online signature is much more secure than a wet signature or a traditional photo ID, yet still we use wet signatures for many important transactions and we will mark a piece of paper with an X at a polling station.”
>
> **Professor Bill Buchanan OBE, FBCS Leader, The Cyber Academy, Edinburgh Napier University**

Phil Aitchison, Head of Cyber Security & Mission Critical Systems, Atos UK&I

What keeps me awake at night?



I see plenty of media coverage lamenting the arrival of the General Data Protection Regulation (GDPR) and with evocative tales of the growing cyber threat. Whilst I understand that this is not necessarily scaremongering and that every business must wake up to the realities, my own view is very different. I see cyber security as an enabler for organisations to achieve their digital dreams. I see the cyber security industry as an entrepreneurial hothouse where hungry SME start-ups are revolutionising decision-making at cyber security operating centres using machine learning technology. Cyber security is a risk. And if we truly understand risk, we can apply the controls needed to achieve our business goals.

What worries me most about cyber?

I've heard it said that sleep liberates the mind from previously held truisms. I have three major gripes about cyber security.

1. Businesses lock themselves into bleeding-edge technology.
Decisions made about cyber security need to be expressed in business terms, not technical jargon. Cool new cyber technologies will regularly burst onto the scene then fade into the background. This is a good thing. Staying relevant to the evolving cyber threat requires innovation at pace. But care should be taken to stick to the fundamentals. Businesses who take evidence-based decisions to reduce their overall risk must buy services which deliver outcomes, not individual products. This avoids vendor lock-in and outsources the technology obsolescence risk to vendors. It also enables businesses to optimise the quality and coverage of service, rather than funding individual technology roadmaps.

2. The scarcity of skills and experienced people.
Plenty of educational courses, recruitment drives and reskilling programmes already exist. Industry must look to work together to take existing collaboration to a new level. Pooling of threat intelligence, shared incident investigation and remediation should happen across supply chains, not just within individual organisations. As stakeholders, we are all in this together.

3. An improved balance must be found leveraging both automation and human insight.
Granted, not everybody can afford detailed threat analysis or the latest behavioural analysis tools, but all organisations need to apply some combination of auto-remediation and specialist human experience to combat their cyber threat. Technology can instantly block well known threats, or alert based on activity that is similar to what has been seen before. This allows rapid flagging of novel threats for human intervention. The magic is in 'learning' how to move as much of the latter group into the former group, so-called machine intelligence. The Atos response to this is an end-to-end solution which continually learns and orchestrates automated security actions to quickly resolve current threats and anticipate the ones to come, at scale and across global enterprises.

How to create value from these ideas?

Against this backdrop is the reality that businesses must commit ongoing investment to cyber resilience as a cost of doing business. Secure by design is an oft-abused term, however the failure to adhere to such a notion would see organisations fail to attract external investment, or worse, be no longer regarded as economically viable. The answer lies with technologies knitted together into end-to-end solutions which enable organisations to realise their digital transformation ambitions.

Sandy Forrest, Client Executive, Cyber Security, Atos UK&I

Game changers for cyber security

While digital transformation delivers enormous value to business and society, it is only sustainable if it is achieved in a secured cyberspace.

We now have a far more connected world, with the exponential growth in the Internet of Things (IoT) and more sharing of data between information and operational systems. At the same time, cyber crimes such as data theft and ransomware that spread across corporate networks are endemic, with the motivation and perpetrators often unknown; and the Dark Web is awash with stolen credentials for sale.

Cyber space without borders

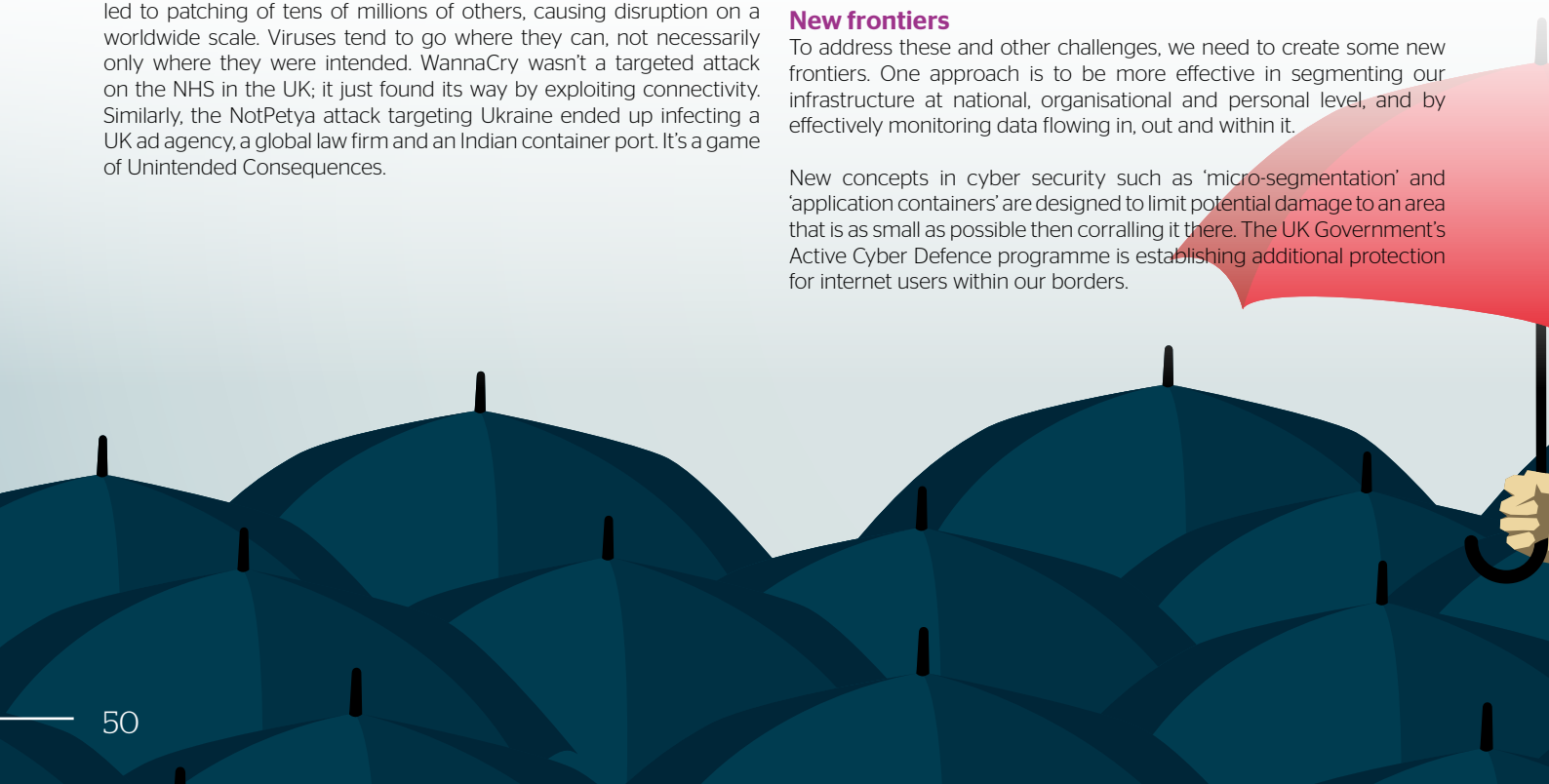
In recent global cyber incidents, it wasn't just the effect that was important, it was the impact. One attack infected 100,000 servers and led to patching of tens of millions of others, causing disruption on a worldwide scale. Viruses tend to go where they can, not necessarily only where they were intended. WannaCry wasn't a targeted attack on the NHS in the UK; it just found its way by exploiting connectivity. Similarly, the NotPetya attack targeting Ukraine ended up infecting a UK ad agency, a global law firm and an Indian container port. It's a game of Unintended Consequences.

Cyber space has no borders. The ability for cyber criminals to attack has been expanded dramatically through the leaking of state-developed tools, the open sharing of exploits by hackers, the re-purposing of penetration testing software by criminals, and the uncontrolled circulation by 'researchers' and 'bug bounty hunters' of vulnerabilities they have found. Cyber attacks are by their nature 'asymmetric', which means they can come from anywhere: you don't need many original skills to mount a successful one – the necessary advice and tools are available on-line.

New frontiers

To address these and other challenges, we need to create some new frontiers. One approach is to be more effective in segmenting our infrastructure at national, organisational and personal level, and by effectively monitoring data flowing in, out and within it.

New concepts in cyber security such as 'micro-segmentation' and 'application containers' are designed to limit potential damage to an area that is as small as possible then corralling it there. The UK Government's Active Cyber Defence programme is establishing additional protection for internet users within our borders.



Shared responsibilities

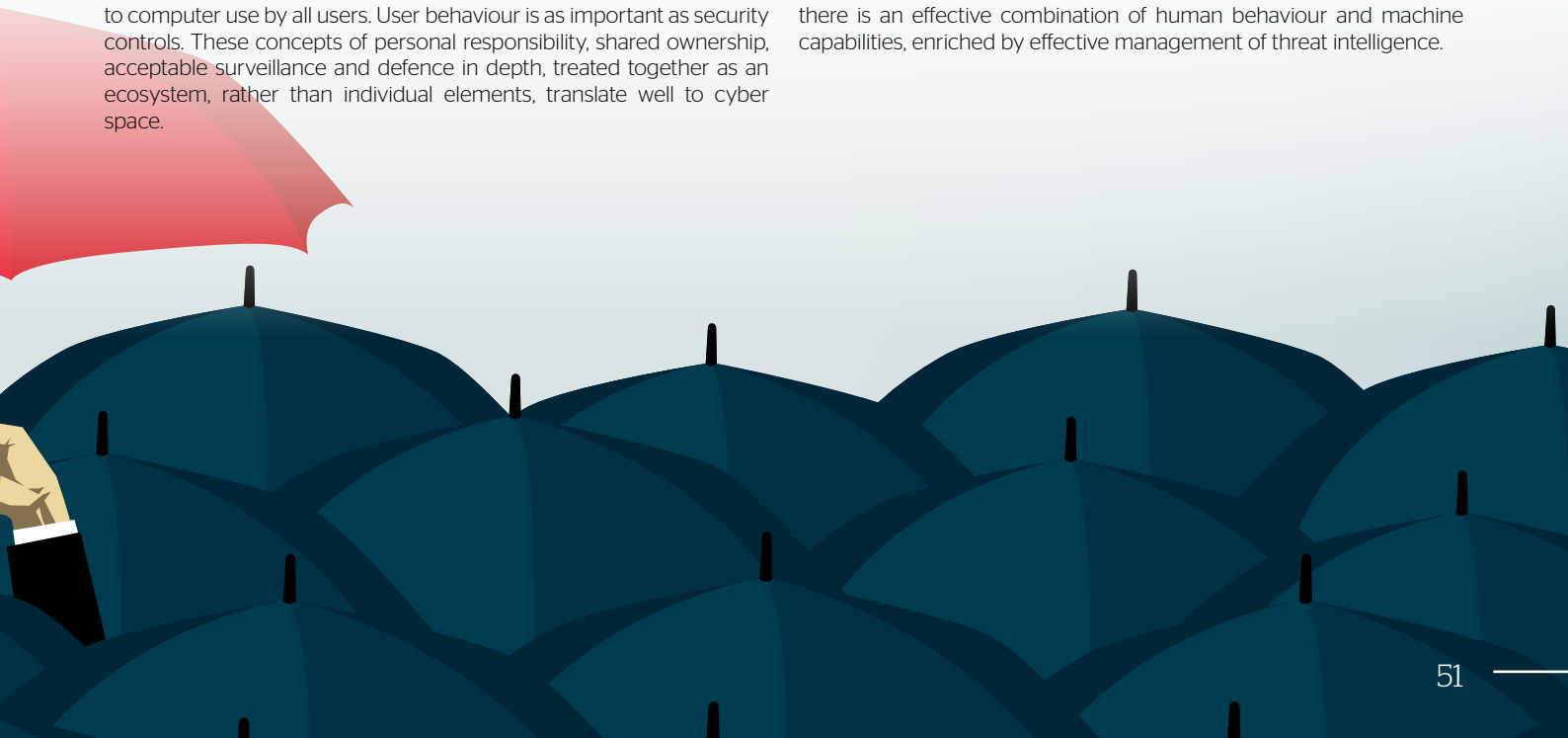
In the 1970s, the concept of Secured by design advanced our understanding of how to make communities safer, by creating "a residential environment whose physical characteristics – building layout and site plan – function to allow inhabitants themselves to become key agents in ensuring their security" (Oscar Newman – *Defensible Space* 1972). This thinking can even now provide valuable insight for our new cyber world and how to make it safe. Common areas (the internet) belong to everybody, so we all have a vested interest in securing them.

We can put controls in place to reduce the potential for harm, but these will be ineffective if not matched by a responsible and informed attitude to computer use by all users. User behaviour is as important as security controls. These concepts of personal responsibility, shared ownership, acceptable surveillance and defence in depth, treated together as an ecosystem, rather than individual elements, translate well to cyber space.

Prescriptive Security

With porous external boundaries, we need a more granular approach that creates boundaries inside the network: reducing the target area, and preventing illicit lateral movement and exfiltration of data. We also need to evaluate risk based on evidence. That evidence comes, in the main, from cyber security monitoring systems combined with collated, actionable intelligence about threats.

Atos' vision for cyber security recognises all these interdependencies – and encourages a more balanced approach to Protection, Detection, Reaction and Recovery, with a move to Prescriptive Security. This means that in addition to powerful computing and sophisticated analytics, there is an effective combination of human behaviour and machine capabilities, enriched by effective management of threat intelligence.



Lexicon

Algorithm: A set of rules or instructions for solving a problem or carrying out a calculation, especially using computer.

Atos Codex: A suite of business-driven data, analytics and Internet of Things (IoT) solutions and services.

Behavioural Analytics: Looking for aberrant behaviour by an individual or a computer that may suggest there is a risk that needs to be addressed (eg that a user may have become an 'insider threat' or a computer may have been compromised)..

Botnet: A large number of computers compromised in a concerted way in order to spread a virus, send spam or flood a network with messages to carry out a denial of service attack (eg the Mirai Virus used for major attacks).

Brute Force: A sustained attack that tries all possibilities, one by one, until it is successful.

Computer Emergency Response Team (CERT): An organisation that studies computer and network information security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

Day Zero (or Zero Day): The day that a new vulnerability appears which systems are not protected against using existing anti-virus software. A 'zero day exploit' is an exploit for which no patch is yet available.

Denial of Service attack: An attack that stops authorised access to systems or data, or delays technology operations. If more than one source is used to mount the attack, it becomes a distributed denial of service (DDos) attack.

Encryption: A process to convert data into code that conceals the data's original meaning to prevent it from being accessed, understood or used.

Exploit: a code that finds a vulnerability in a machine or network and exploits it

Firewall: A security system that prevents unauthorised access to systems or data on a private network.

GDPR (General Data Protection Regulation): The EU's data protection regulation that comes into effect in May 2018 and places obligations on organisations in relation to the protection of personal data and requirements to report data breaches..

IP (Internet Protocol) Address: A unique numerical identifier for every device connected to the internet which serves both to identify and locate the device.

Malware: A generic term for software that is developed with a hostile intent, for example to damage or gain unauthorised access to a device or network (eg worms, viruses, Trojan horses).

NCSC: The UK's National Cyber Security Centre, part of GCHQ, established to enable the UK to manage the cyber threat.

OSINT: Open source (ie publicly available) intelligence that can be added to other intelligence feeds to enrich understanding of the threat.

Patch: A discrete update released by a software vendor to fix vulnerabilities and bugs in existing programs.

Penetration: Circumventing a system or network's security controls in order to gain unauthorised access.

Phishing: A cyber crime in which individuals or companies are contacted by email, text or phone by someone posing as a trustworthy source in order to trick the recipient to disclose personal or financial details. This can also be an automated process. It is called Spear Phishing if specifically targeted or Whale Phishing if targeted at senior people.

Predictive Security: Capability that analyses network traffic to identify potential threats.

Prescriptive Security: Capability that uses machine learning and artificial intelligence to identify a potential issue, and then takes action to prevent the threat developing.

Plaintext: Raw text before it has been encrypted or after it has been decrypted.

SIEM (Security Incident Event Management): Tool that collates and analyses log data coming from a variety of sources to help manage security threats.

SOC (Security Operations Centre): Facility where analysts work with security tools and threat intelligence to monitor what is happening in the network and take remedial action if issues arise.

Trojan horse: A type of hidden malware that is designed to look useful or benign, but is developed and used with malicious intent.

Virus: A type of hidden malware that self-replicates (by copying its own source code) and infects other computer programs by modifying them. A virus cannot run by itself; it requires a host in order to spread. Once infected, computer programs and machines are compromised.

Worm: A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

In association with SANS:
https://uk.sans.org/security-resources/glossary-of-terms

Acknowledgements

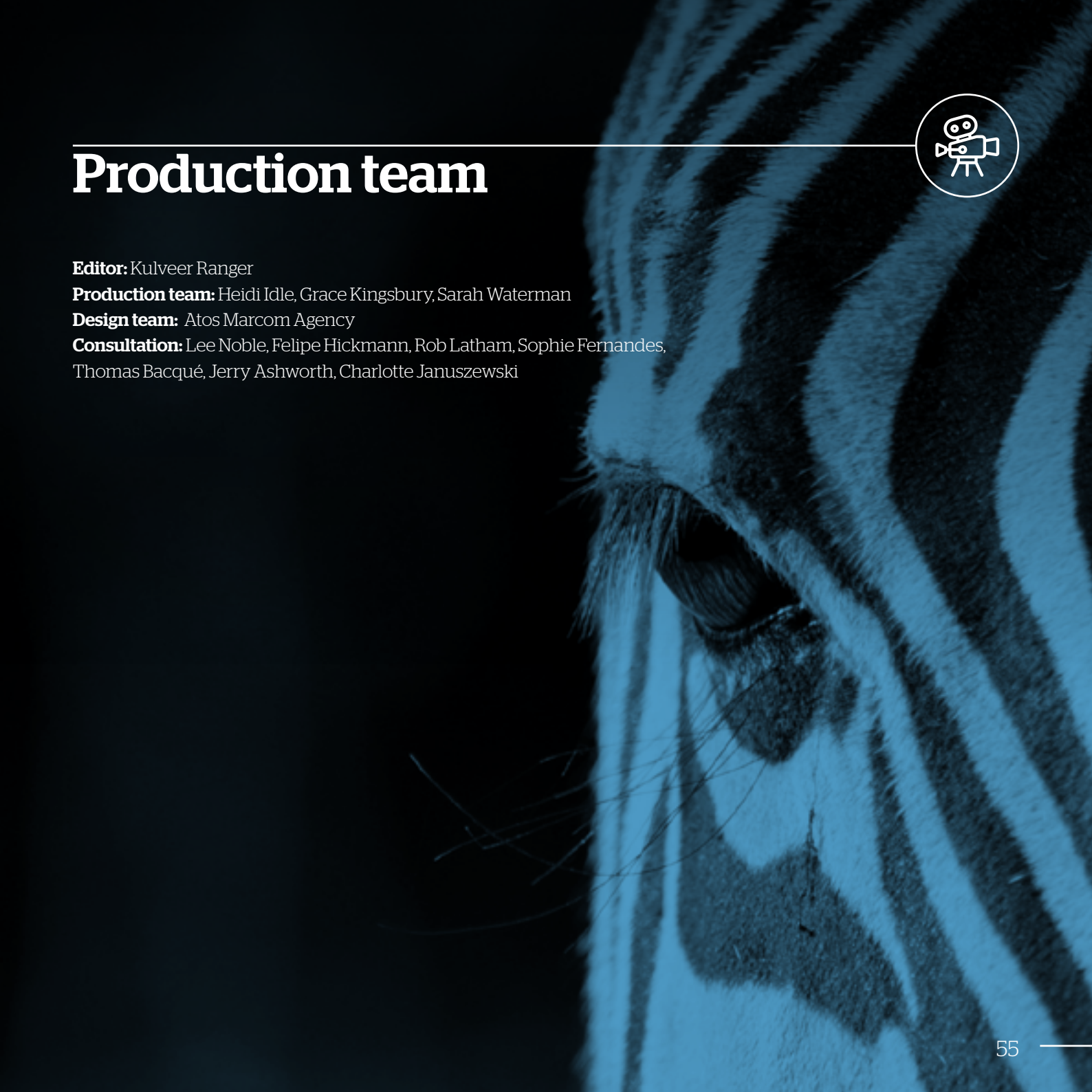
We would like to thank the following contributors. If you wish to send feedback, please tweet using **#DVfCS** or email: **AtosDigitalVisions@atos.net**

In order of appearance

Adrian Gregory	Chief Executive Officer, Atos UK & Ireland
Pierre Barnabé	Executive Vice-President, General Manager Global Division Big Data & Security, Atos
Gavin Thomson	Senior Vice President, Big Data & Security UK&I, Scotland, Ireland and Wales, Atos
Robert Hannigan	Former Director of GCHQ and chairs the European Advisory Board of BlueteamGlobal
Kevin Cooke	Cyber Reconnaissance & Response Manager, Atos UK&I
Jenny Lam	Security Operations Engineer and Security Operations Centre Analyst, Cyber Security, Atos UK&I
Talal Rajab	Head of Programme, Cyber and National Security, techUK
Professor Lizzie Coles-Kemp	Information Security Group, Royal Holloway University of London
René Martin	Head of Data Security Products, Atos
Deborah Dillon	Lead Auditor, Business & Platform Solutions, Atos UK&I
Graham Watson	Managing Director, The Advanced Engagement Company
Christophe Moret	Senior Vice President, Cyber Security Services, Atos
Richard Vinnicombe	Practice Leader, Information Governance, Risk and Compliance, Atos UK&I
Edwin Morgan	Interim Director of Policy, Institute of Directors
Paul Heath	Regional Sales Director, UK&I Public Sector, McAfee
Phil Aitchison	Head of Cyber Security & Mission Critical Systems, Atos UK&I
The Rt Hon Matt Hancock MP	Minister of State for Digital, UK Government
Zeina Zakhour	Distinguished Expert, Global Chief Technical Officer, Cyber Security, Atos
Crispin Keable	Distinguished Expert for High Performance Computing, Atos UK&I
Mariana Pereira	Director, Darktrace
Alison Devenish	Head of Workforce Management, Atos UK&I
Laura Rutter	STEM Ambassador, Atos UK&I
Ember Ellis	Security Operations Centre Cyber Security Specialist, Atos UK&I
Lewis Currie	Security Operations Analyst, Atos UK&I
Kulveer Ranger	Vice President, Strategy & Communications, Atos UK&I
Professor Bill Buchanan OBE	FBCS Leader, The Cyber Academy, Edinburgh Napier University
Sandy Forrest	Client Executive, Cyber Security, Atos UK&I

Production team

Editor: Kulveer Ranger
Production team: Heidi Idle, Grace Kingsbury, Sarah Waterman
Design team: Atos Marcom Agency
Consultation: Lee Noble, Felipe Hickmann, Rob Latham, Sophie Fernandes, Thomas Bacqué, Jerry Ashworth, Charlotte Januszewski



About Atos

Atos is a global leader in digital transformation with approximately 100,000 employees in 72 countries and annual revenue of around € 12 billion. The European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, The Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.

Find out more about us
atos.net
ascent.atos.net

Let's start a discussion together

For more information: **AtosDigitalVisions@atos.net**

CT_170915_AS_DigitalVision-for-Cybersecurity_v9