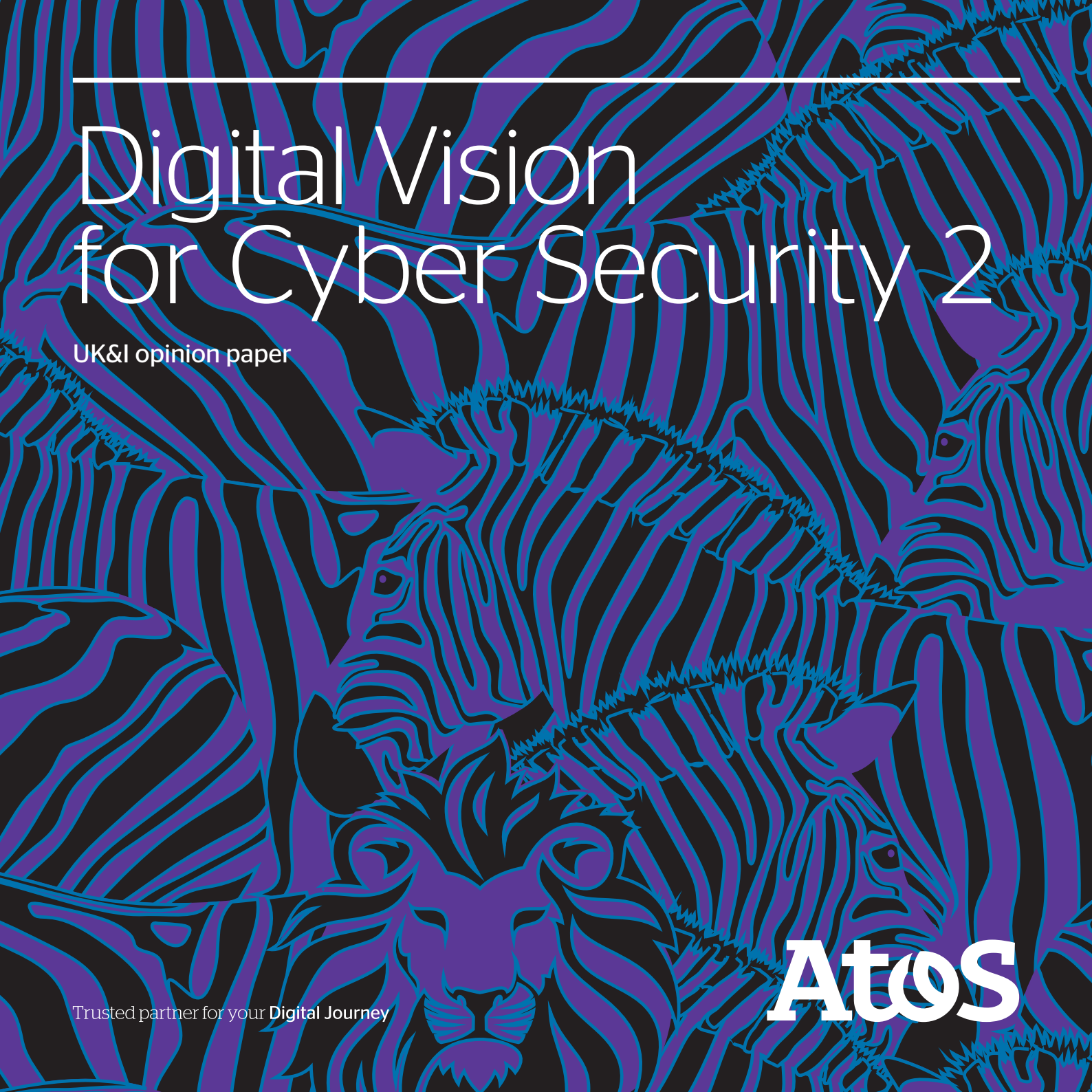
Digital Vision for Cyber Security 2

UK&I opinion paper



Trusted partner for your **Digital Journey**

Atos

Contents

Watch our videos and find out more at **atos.net/dvfcs**

Digital Vision for Cyber Security 2

Adrian Gregory
Senior Executive Vice President, Chief Executive Officer, Atos UK & Ireland

Since we published the first Atos Digital Vision for Cyber Security in 2017, much on the cyber security landscape has changed. **Significant new threats have emerged; so too have innovative cyber security solutions. Yet also, key factors remain unchanged: the challenge to stay ahead of our adversaries prevails, as does the need to ensure that cyber security is a board-level priority.**

As Europe's leading cyber security provider and one of the top three in the world, Atos is committed to fulfilling our role at a national and global level. This demands that we continue developing cutting-edge capabilities to protect people and organisations, enabling the full benefits of digital technologies, and supporting the UK as a cyber security world leader. We look forward to working in partnership with our customers and others to keep cyber space secure as the threat landscape evolves.

Pierre Barnabé
Senior Executive Vice President, Head of the Global Division Big Data & Security, Atos

Cyber security is, undoubtedly, one of the most important challenges of our times and a process of continuous adaptation. **As the digital age advances, so too must cyber security to embrace new technologies such as artificial intelligence and automation while continuing to create a cyber vigilant culture and respond to changing regulatory frameworks.**

To deliver effective cyber security, Atos leverages world-leading talent and technologies at our 14 Security Operations Centres; we continue to expand our global cyber security networks, including our recently announced partnership with Ooredoo in Qatar and acquisition of IDnomic, European leader in digital identity management infrastructure. Cyber security is a critical enabler of digital transformation and must be a core function of every enterprise. Most importantly, the role of cyber security in society is to underpin vital trust between individuals and organisations as this exciting digital journey continues.

Gavin Thomson
Senior Vice President, Private Sector and Big Data & Security, Atos UK & Ireland

The last two years have seen threat actors harnessing the vast power of artificial intelligence and automation to launch sustained global attacks on multiple sectors. Increased digitalisation and the growth of hybrid cloud have brought fresh challenges. As a glance at the lexicon in this Digital Vision shows, new risks and responses are occurring all the time and shaping the language of business.

Atos responds to every digital wave with new cyber security solutions. Prescriptive security uses advanced computing to neutralise known threats and release precious human resources for the fight against hidden ones. And as quantum and edge computing reach their tipping points, cyber security controls will be even more agile and distributed. **For every organisation, implementing an effective cyber security strategy is essential, with specialist partners innovating on the frontline to safeguard critical infrastructure, public services, businesses and citizens.**

Phil Aitchison, Chief Operating Officer, Big Data & Security, Atos UK & Ireland

What's changed in cyber security over the last two years?

Since Atos's first Digital Vision for Cyber Security was published in 2017, three aspects of the cyber world have evolved significantly: the legal and regulatory environment; the nature of the cyber threat; and cyber security capabilities.

Legal and regulatory environment

In May 2018, GDPR (the EU General Data Protection Regulation) and the NIS (Network and Information Systems) Regulations came into effect. The former places additional obligations on every organisation in relation to personal data. The latter applies to organisations that operate essential services and specifies requirements for modernised infrastructure and appropriate cyber security.

While each regulation is a step change, the true test will be the extent to which organisations address data and cyber security as a result. Despite GDPR's high profile, it seems many organisations have been slow to make the required improvements. We have, however, begun to see a number of GDPR-related fines levied by the Information Commissioner's Office.

In addition, the National Cyber Security Centre, which opened in 2016, has quickly established itself and is the touchstone for 'what good looks like' in all aspects of cyber security. Providing a wealth of valuable advice and support to the UK economy and society, it has, for example, issued a Cyber Assessment Framework in relation to the NIS Regulations and a Board Cyber Risk Toolkit.

Cyber threat – an overview

When it comes to the cyber threat, a number of major trends have emerged in the last two years, each having impact on different aspects of cyber security.

Early 2017 saw the global phenomena of the Wannacry and NotPetya virus incidents, with recurring variants appearing regularly since then. Key lessons from these focus on the risk of 'collateral damage' – you do not need to be a direct target to be a victim. They also highlighted the risks presented by continued use of out-of-support legacy operating systems. Separately, researchers have located vulnerabilities in computer systems in use for more than a decade, with more ransomware attacks appearing to target organisations likely to have vulnerable legacy equipment, particularly in the public sector. In addition, a series of financially motivated attacks (such as Magecart and its successors) highlighted the risks associated with web developers relying on components that age and don't get patched to protect them from attack, such as recent cases in the aviation and ticketing industries.

Cyber threats and attacks have entered mainstream news and therefore the public psyche. State-sponsored cyber activity is increasingly prevalent, including interference in elections and fake news, and organised crime groups increasingly use targeted and social engineering attacks. Viruses are still being generated in their millions and becoming more sophisticated to evade controls. At the same time, Distributed Denial of Service (DDoS) attacks are still occurring – and can now even be purchased 'as a service' on the dark web, but are less newsworthy than large data thefts or financial crime.

The move to cloud, if not properly secured, has also increased the cyber security risk. Adversaries are actively trying to develop exploits to target data sets on shared cloud infrastructures and we have seen recent examples of attacks being mounted from commercial cloud providers, mostly redirecting traffic to a spoof website they control.

Cyber capabilities to keep pace

In response to the evolving risk, tools to address cyber risks are necessarily evolving to become ever more innovative, effective, affordable and available. For example, user and entity behaviour analytics, together with more intelligent capabilities and analytics at the user end, all help to better understand what is happening across the enterprise.

Cloud Access Security Broker technology has been developed to meet the new challenge of securing data in the cloud. Next-generation Security Incident Event Management (SIEM) capabilities are also rapidly developing, expanding the range of data they can ingest for even more effective analytics.

Yet effective cyber security relies not only on technology: human intelligence and insight are essential. Given the acknowledged cyber skills shortage, more efforts have been made in the last two years to increase and diversify the numbers of people and skills in the UK's cyber security sector – including new injections into the Government's Cyber Skills Immediate Impact Fund. Through this, cyber training providers can apply for funding to ensure that the UK continues to develop the cyber security talent needed to protect the public and businesses online.

Looking ahead

So, what have cyber security specialists learned from all of this? Firstly, most organisations still do not make adequately informed decisions about cyber risk: a risk-based approach must be based on monitoring and threat intelligence. Secondly, compromised static passwords continue to be a problem, as do increasingly targeted phishing emails. Thirdly, traditional virus protection software cannot cope with polymorphic viruses: behavioural and advanced threat protection techniques need to be adopted. Finally, security patching and security testing are now a priority, even where they impact live services.

The solutions to best leverage fast-developing capabilities and the lessons of the last two years are applied through prescriptive security. In essence, this is about using advanced SIEM tools to fuse large volumes of incoming security data, with automation and artificial intelligence to make sense of all that data and auto-remediate wherever possible. From there, talented analysts can be freed up to look ahead and focus on newly identified threats. As the White Queen explained to Alice in Wonderland, "It's a poor sort of memory that only works backwards".

"As the UK's digital economy continues to grow, protecting customers and their data online must be a priority. The Government is working closely with industry to ensure we have the right balance of regulations and incentives to help organisations manage their cyber risk. Our £1.9 billion National Cyber Security Strategy is making the UK the safest place in the world to live and work online so that our digital economy remains fit for the future."

Matt Warman MP, Parliamentary Under Secretary of State (Minister for Digital and Broadband), Department for Digital, Culture, Media and Sport

Recent evolution in cyber security

2016

October
UK's National Cyber Security Centre (NCSC) established

November
UK's National Cyber Security Strategy 2016–2021 published

2017

February
NCSC officially opened by Her Majesty the Queen

May
WannaCry virus attack

June
NotPetya virus attack

October
Atos's first Digital Vision for Cyber Security launched

2018

January
Spectre & Meltdown cryptojacking vulnerabilities made public

February
Largest Denial of Service (DoS) attack ever recorded

May
GDPR & NIS regulations implemented

June
Magecart attacks hit ticketing and airline industries in UK

November
NCSC Cyber Assessment Framework published

2019

March
NCSC Cyber Security Toolkit for Boards published

July
Lone hacker attack on large financial organisation

October
Atos's Digital Vision for Cyber Security 2 launched

Cyber security: the business challenge

63%
of UK consumers say recent cyber attacks have made them more aware of cyber security as an issue that may impact their daily lives[1]

71%
increase in the average annual cost to UK businesses that lost data or assets after breaches since 2017[3]

67%
of UK consumers say they would trust an organisation more if they knew it was investing in advanced cyber security technology[5]

24%
of UK consumers take active steps to stay informed of potential cyber threats[2]

16%
of UK businesses have formal cyber security incident management processes in place[4]

10.52 billion
malware attacks recorded globally in 2018[6]

217.5%
increase in attacks on the Internet of Things globally between 2017 and 2018[7]

1.8 million
unfilled cyber security jobs globally by 2022[8]

66%
of UK consumers expect organisations to fully protect their customers[9]

Around 80%
of current successful breaches are facilitated either by weak passwords or stolen credentials, with details often available to criminals on the dark web[10]

Atos at a glance

- Atos is Europe's **No.1 security provider** and **top 3 worldwide**
- **Recognised leader** in cyber resiliency services by NelsonHall
- **5000 +** security professionals in Atos globally
- **125 million** security events managed per hour
- **14** Security Operations Centres worldwide

[1] The currency of cyber trust, Atos, 2018
[2] The currency of cyber trust, Atos, 2018
[3] Cyber Security Breaches Survey, Ipsos MORI, 2019
[4] Cyber Security Breaches Survey, Ipsos MORI, 2019
[5] The currency of cyber trust, Atos, 2018
[6] Mid-year update:2019 SonicWall Cyber Threat Report
[7] Mid-year update:2019 SonicWall Cyber Threat Report
[8] https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage
[9] The currency of cyber trust, Atos, 2018
[10] Verizon Data Breach Investigations Report (DBIR), 2019

John Hall, Head of Portfolio, Atos UK&I and Scientific Community Expert

Digital dilemmas and cyber security

It is amazing just how dependent people have become on digital technology – and I don't just mean our love affair with smartphones. Businesses, governments and societies at large can no longer operate effectively without the instant connections that new technologies offer.

Yet while the benefits of these are vast, so are the risks. We have only to consider the impacts of even short-term IT failures in banking, airport baggage or electricity power grid systems to catch a glimpse of the vulnerabilities we now face in our everyday lives.

Art of the permissible

Digital interactions are becoming inherently more open, collaborative and interdependent. At the same time, trust has become one of the single biggest factors in the adoption of digital systems: trust both in the operational resilience of systems and in the integrity of underlying processes and data. Establishing and maintaining this trust is an increasingly complex challenge at the heart of the cyber security agenda.

In 2018, the Atos Scientific Community published our new vision for technology in business and society in the paper, Journey 2022[1]. This introduced the concept of 'digital dilemmas' that arise when technology advances at such a rate that the digital 'art of the possible' is no longer aligned to the real-world 'art of the permissible'. These dilemmas often relate directly to cyber security risks: yes, it is possible, for instance, to connect billions of objects via the Internet of Things, but should that ever be done without the assurance that malicious actors won't be able to hack into them? Taking control of a connected fridge may not pose too extreme a threat, but an autonomous vehicle or smart medical implant are completely different prospects.

Emerging dilemmas

There are plenty more examples. How can we be assured of the provenance of digitalised news stories, digital evidence submitted in court, personal credentials or digital currency, to name but a few? As the world becomes more digitalised, the growing and changing potential 'attack surface' demands a rethink of cyber security if businesses and governments are to avoid user distrust or even rejection of particular digital solutions.

For the most part, humans can no longer respond on their own to the variety, complexity and rate at which cyber-attacks can be launched. As this Digital Vision reveals, artificially intelligent and automated solutions are required, not only to identify threats and suggest appropriate responses but also to anticipate threats before they occur.

But how far might this extend, and does this automated approach create its own set of digital dilemmas? Is it acceptable to anticipate criminal behaviour and act on that insight? Could we be running the risk of a dystopia of the kind seen in the film, Minority Report, where technology is used to identify individuals as criminals even before any crime is committed?

Resolving the tensions

Insights from data analytics can reveal much about human and machine behaviours and threats, but at what point might they be seen as personally invasive by encroaching on individuals' data privacy rights? Who sets the boundaries of acceptability and how can security remain effective when cyber criminals have access to the same digital technologies but do not operate to the same ethical standards?

To build and maintain essential trust, it is clear that we must address the balance between 'could we?' and 'should we?'. Journey 2022 called for a recognition and resolution of the tensions between the digital and physical worlds to build fairness into digital business models: to ensure, for example, that society approaches data insights and automation in a way that respects human rights.

[1] atos.net/journey-2022

Resolution and collaboration

New techniques in data encryption, the use of blockchain and similar solutions, digital forensic technologies, artificial intelligence and quantum computing are all expected to be instrumental in the fight to maintain the resilience and integrity of digital networks. While, as this Digital Vision makes clear, new approaches to cyber security are demanded, cyber security experts, governments and organisations need to work together to ensure that these approaches are applied without disproportionately impacting the very benefits that the related technologies bring.

The future will not be dystopian if, together, we are all aware of the emerging nature of cyber threats and their implications. With that awareness, organisations, political leaders and cyber security specialists can discuss and co-create appropriate strategies, standards and regulations to resolve human beings' digital dilemmas as our connected world fast evolves.

About Atos Scientific Community

The Atos Scientific Community is a global network comprising 150 of the top scientists, engineers and forward thinkers from across Atos. It aims to craft Atos's vision for the future of technology in business, and anticipate the upcoming trends and technologies that will reshape businesses and society in the years ahead.

Knowledge of, and control over data is necessary to design and feed the future algorithms that will play an ever-increasing role in our lives. Those who can develop the most relevant algorithms are those who can tap into the greatest depth of data. And we need to keep anticipating future changes that will affect how this data is generated, processed and stored.

We know that, in the foreseeable future, the ocean of data will keep growing larger and larger. And today, 80% of it is processed in data centres and private or public clouds. That leaves 20%, which is being processed outside: in our smartphones, in connected devices, in cars, and so on.

Five years from now, it will be the exact opposite: 20% of the world's data will be stored in data centres or in the cloud, and 80% will be somewhere else.

Why? Because a significant part of this data will be handled locally. And this means it will come with security risks. For companies, it means specifically that their risk surface will expand.

In the meantime, our volumes of data will keep growing. Today, the global information space comprises 40 thousand billion billions of data. And we make this volume double every 18 months.

The new challenge for us, through what we call edge computing – whereby data is processed as close as possible to the source – is to protect data and ensure it creates value as soon as it's produced, wherever this happens.

Thierry Breton
Former Chairman and CEO, Atos

techUK

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

A new strategy to help protect the UK from cyber attack

The key objectives of the UK Government's five-year National Cyber Security Strategy, published in 2016, are to defend the UK from cyber attack, deter cyber criminals from targeting the UK, and develop our country's sovereign cyber security capabilities while cooperating at a global level with cyber security defences.

Given its initial investment of £490 million into the National Cyber Security Strategy, later increased to £1.9 billion, there's clear recognition by the Government of the changing cyber security landscape, particularly the growing numbers of automated attacks against multiple sectors.

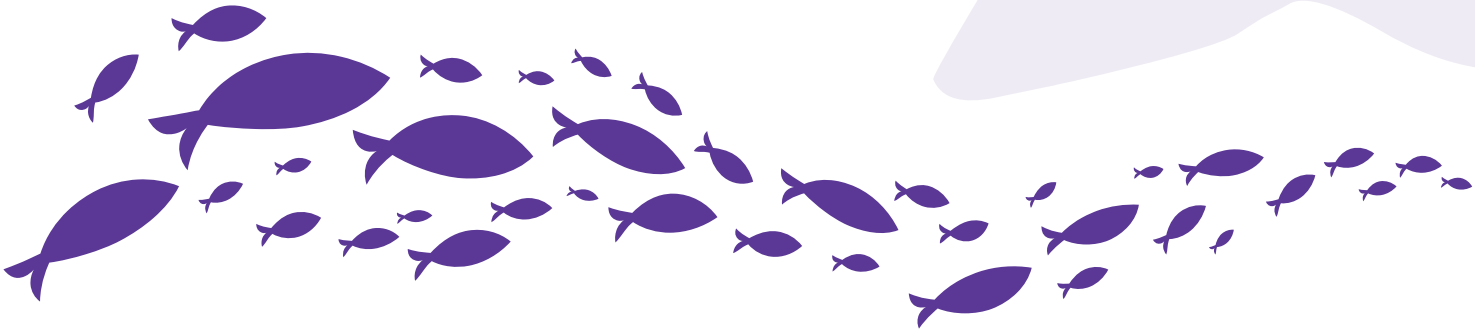
In the wake of Wannacry, with Government seeking a more focused, holistic approach to cyber security, the establishment of the National Cyber Security Centre (NCSC) as the UK's technical authority in 2017 was a game-changer. Since then, the NCSC has played a proactive, hands-on national role giving advice and guidance to organisations and individuals.

To build on this success, and as the cyber threat continues to advance, what steps should any future strategy set out to secure our cyber space once the current strategy ends?

Protecting public services

One area of critical importance is further investment in the security of local and central government departments. As public services are increasingly digitalised, they must be inherently cyber secure. Local government agencies in particular have been subjected to base-level attacks such as ransomware incidents; these have sparked public concerns that personal data might be at risk.

In response, the focus on public sector cyber security needs to be increased, with healthcare being another key area. With hundreds of local councils and health bodies nationally, these fragmented structures can make it more difficult to adopt a holistic approach. There are inevitable pressures on budgets and skills, for example for local councils in rural areas; there should not be a postcode lottery when it comes to how effectively citizens' and businesses' data is secured.



Upskilling and developing capacity

Work is underway in this area to address any gaps. At techUK, we've been working with local councils to build their cyber resilience; and the Department for Communities and Local Government is delivering a programme to upskill public bodies in cyber security. A buddying programme, for example, is currently being piloted through which larger, more experienced councils can transfer knowledge to smaller organisations in how they maintain cyber security. techUK is providing further support through the Local Government Association to share learning and best practice, especially with IT staff without previous relevant experience who now have cyber security as part of their brief.

Upskilling is also required within law enforcement. High volumes of low-impact cyber crime, such as phishing attacks and low-level fraud put a huge strain on police resources and, inevitably, can erode trust in organisations and the police among local communities. To address these challenges, further investment in UK law enforcement's cyber response will build the skills and capacity to deal with digital crime among a new generation of police officers.

> As we enter the 2020s, even those businesses which were not born digital will have data as their core, either as IP, or the likes of user data. While this data may act as the business' greatest asset, effective business leaders realise it can also be their greatest vulnerability. Unfortunately, the changes in the cyber landscape are not only refusing to slow down, they stand at a precipice in which AI can potentially act as the ignition to a whole new era of cyber warfare.
>
> **Mike Smart, Senior Analyst and Operations Officer, NelsonHall**

Nurturing talent

Cyber security technologies are, of course, rapidly developing to incorporate machine learning and artificial intelligence (AI) to better detect and respond to threats. Yet as well as being a huge area of opportunity, we need to recognise that AI also poses new risks. Mass attacks are ever more automated; adversaries are using AI to finetune malware and learn about different methods of attack. So, while the benefits of AI are clear, we need to better understand its challenges, including how attacks are perpetrated and how organisations can keep one step ahead.

More widely, it is vital that Government continues to work with private sector partners to build capacity and protect the public sector. Within the current strategy, the UK's growing cyber security capabilities have yielded results; this should continue with further investment.

If we look to countries like Israel, significant support and research data is provided to the cyber security community. In the UK, there will be opportunities to scale up the same kind of support through any future strategy: to retain intellectual property, nurture cyber security talent, and build capabilities to stem the threat here in the UK. This will make a significant contribution towards global collaboration, underpinning our position as a world leader in cyber security while keeping our nation, our economy and our citizens secure.

About techUK

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. Around 850 companies are members of techUK. Collectively they employ approximately 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium-sized businesses.

Mandy Haeburn-Little, CEO BRIM, former Chief Executive, Scottish Business Resilience Centre

Is the UK ready for the businesses of the future?

Recently I met a young tech entrepreneur who, having been through three successful rounds of investor funding, is attracting a lot of attention. His question to me was, 'why is it that all business networks aren't yet secure?'. In other words, while he is developing ever smarter ways to collect and use data, his frustration is, in effect, 'why didn't your generation sort this for us at the outset?'.

Changing business expectations

It's a fair cop. My answer is that we were too busy innovating and running to keep up with the pace of business and technological change and customer demand.

At the Scottish Business Resilience Centre, our purpose is to create a secure environment where business can trade securely, regardless of size and sector. Through my work with smaller businesses, it's clear that today's upcoming business owners and leaders have very different ideas to previous generations of what being in business is all about. And they have different expectations of cyber security and their challenges in relation to business resilience.

Larger companies are likely to continue with a strong risk-based approach to cyber security; this involves rigorous and innovative interrogation of systems and data, with preventative security controls and a culture of cyber security awareness. But what about smaller businesses - the young entrepreneurs and the pop-up visionaries? What cyber security support and services are they looking for?

Hyper-connectivity and integral security

As far as millennials and younger digital natives are concerned, online is their resource for anything and everything. They represent a global community for whom the concept of email and, increasingly, texting are ponderous and largely unnecessary. These are the generations who hold up a very timely mirror to the rest of us and ask, 'why do you do that?'.

Before they even begin trading, they are data-rich and have information (right and wrong) at their fingertips. Many work anywhere and at hours that suit them and their markets. And they are clear about what they want from the wider business and technical community: hyper-connectivity, absolute and integral security, volumes of data and analytics, speed of access, high performance and flexible digital workplace solutions.

New cyber security challenges

What is more, consider how cyber security must evolve in the age of increasing volumes of data and artificial intelligence. Who looks out for unknown threats? Where are they likely to come from and how do businesses monitor their own perimeters? Where does lost data go and where could it go? The implications of this are momentous – not least, the growing volumes of stolen credentials and other security information now available to cyber criminals and hackers on the dark web.

> There are many things organisations can do to protect themselves against cyber crime. Most employ a Chief Information Security Officer and all need to use the technical support available to them. Yet what remains most critical is the people component: every attack has an element of human error or threat. Therefore, we must focus on maintaining the cyber security conversation outside the IT department and at Board level.
>
> **Maxine De Brunner QPM, former Deputy Assistant Commissioner, Metropolitan Police Service**

58% of consumers weren't sure they would trust an organisation after an attack

82% expect an organisation to inform its customers in the wake of an attack

Trust and integrity

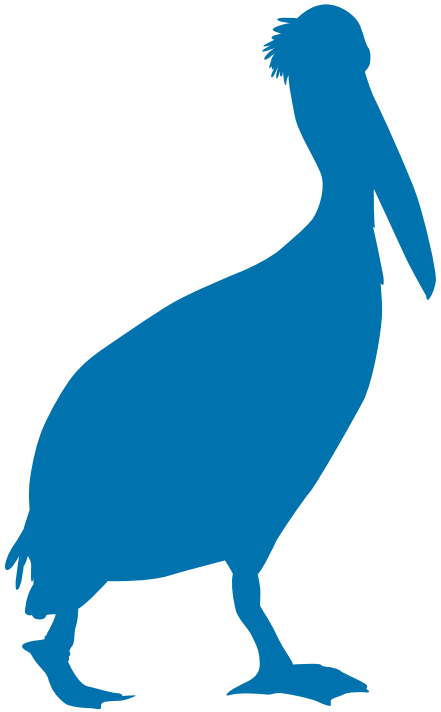
The solution for every organisation must be a rigorous assessment of specific cyber security risks and risk profile; resilience in this context will require an individual approach and bespoke planning. Yet whatever your business, having an up-to-date risk register and advanced mitigation of risk is essential. And of course, risks will change. Communication with customers and others about cyber security is just as important for building trust. Atos's recent consumer survey about cyber security underlined what I see in my own work with businesses, with 58% of consumers saying they weren't sure they would trust an organisation after an attack and 82% saying they expect an organisation to inform its customers in the wake of an attack.

At the Scottish Business Resilience Centre, we work with organisations of all sizes to develop affordable and innovative cyber security and business resilience solutions and services. Now, as never before, we all need to select business relationships of trust and partners with integrity in cyber security. This is vital if we are to be mutually ready for the speed of change in the fast-expanding business world.

About Scottish Business Resilience Centre (SBRC)

The Scottish Business Resilience Centre (SBRC) is a non-profit organisation which exists to support and help protect Scottish businesses.

Recently Mandy Haeburn-Little officially stepped down from her role as Chief Executive of the Scottish Business Resilience Centre after nine years to set up Business Resilience International Management (BRIM), a new company which looks to set up new business resilience and cyber centre's globally.



Kevin Cooke, Head of Cyber Security Delivery, Atos UK & Ireland

Why do we need prescriptive security?

In 2018, the total volume of all electronic data ever created reached 18 billion terabytes. By the end of 2020, that will have more than doubled. The data generated through security monitoring, while smaller in volume, has been growing at a similar pace.

As we enter the fourth industrial revolution, the transformational power of technology lies in how human beings can maximise value from what is sometimes called the data overload. Equally, turning the growing volumes of security-related data into actionable insight is vital for effective cyber security.

Cyber security: a brief history

So firstly, how has cyber security evolved over time? For many years, cyber security analysts inspected and assessed data about a myriad of cyber threats using a mix of standalone solutions. Security tooling was dotted around the network, with each tool generating its own volumes of data about threats relevant to its specific function.

As a result, the number of security controls grew significantly, making it harder for organisations to detect and respond to threats in reasonable timeframes. Analysts were flooded with alerts, many of which were 'false positives'; this hid genuine attack data and, most importantly, hampered effective decision-making.

At the same time, ongoing digitalisation exacerbated data volumes, with increasing convergence of information technology and operational technology (OT), the growth of the Internet of Things (IoT), and vast infrastructures linking together multiple systems and networks. As businesses strive to integrate plant equipment and new IoT devices into their networks, this broadens the attack surface. Given the increasing connectivity of such devices, securing these systems and networks requires visibility across the connected whole.

From reactive to prescriptive

Dealing with the ever-expanding data volumes and ever more complex cyber threats clearly places an increasingly heavy burden on the skills and knowledge of cyber security analysts. Advanced computing power, automation, machine-learning and artificial intelligence (AI) have catalysed a revolution in cyber security.

By harnessing these capabilities over time, cyber security has moved from reactive analysis – which tells you what has just happened, through proactive analysis – which extrapolates what may commonly happen next, to prescriptive analysis – which uses machine learning to identify patterns in the data that might indicate a zero-day threat or attack in progress.

To compare this to the aerospace industry, proactive maintenance might suggest that an aircraft part requires inspection; in contrast, prescriptive maintenance would use data from an aircraft fleet to identify points of failure before they occur, resulting in higher safety and lower costs.

Human and machine

In a Prescriptive Security Operations Centre, more automation is deployed and can analyse the bulk data gathered over long timeframes; this enhances the analysts' ability to spot patterns and trends, identifying common types of attack or specific targeted industry sectors.

Uses of advanced analytics include: pattern recognition to identify malware and other threats; anomaly detection to find unusual activity, data or processes; natural language processing to convert unstructured text into structured intelligence; and predictive analytics to process data and identifying patterns. From there, the response to any detected threats can be seamlessly orchestrated.

Responses to known threats are automated based on a high level of confidence using pre-configured scenarios. In other cases, multiple data points are collated and enriched with contextual threat intelligence to help the analyst make evidence-based decisions, including whether to trigger automated 'playbooks'. Crucially, prescriptive security frees up cyber security experts and analysts to focus on advanced detection, in-depth analysis and threat hunting tasks.

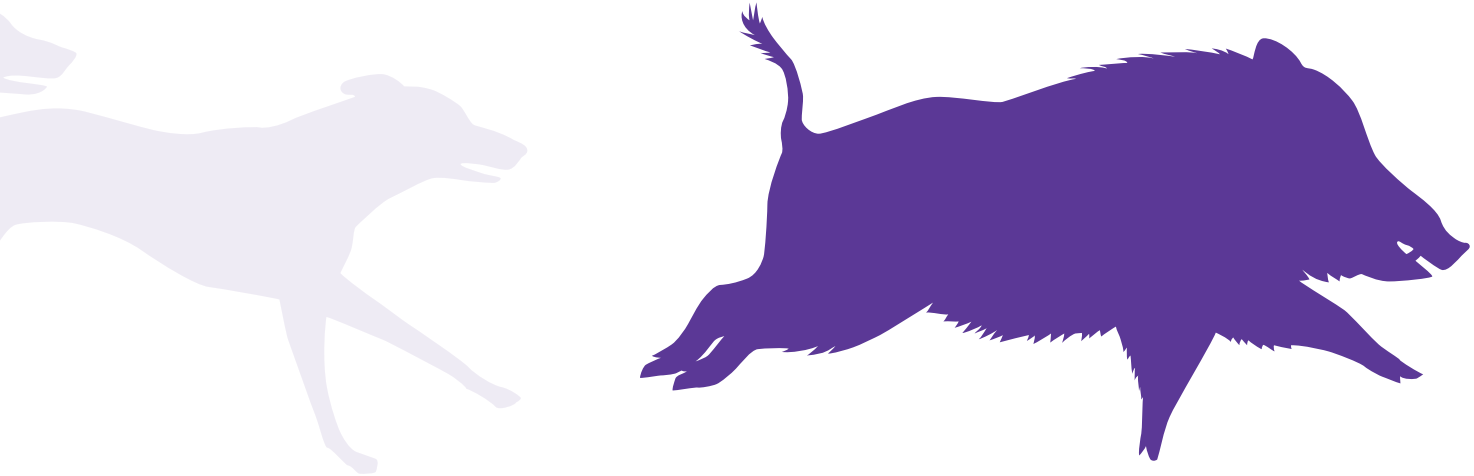
Cyber security ecosystem

To implement an effective prescriptive security strategy requires organisations to consider cyber security as an ecosystem, with all available data brought together into a single repository where it can be effectively analysed. The AI-driven insight into this 'data lake' enables organisations to take an evidence-based, risk-driven approach to managing their security posture.

Without this, an organisation's cyber security approach can become a game of chance, with obvious implications ranging from potential loss of service to negative impact on share price, regulatory compliance and reputation; trust is central to every business's success.

Prescriptive security is both the solution to, and the opportunity created by the huge volumes of data being generated. While computing power is critical, so too are the skills, insight and talents of human cyber security experts who enable organisations to navigate the best and worst of the data overload.

> The growing trend towards incorporating machine learning and rapid application development methods as part of a digital transformation strategy is driving a fundamental change in the office of the CISO. Increasingly, this will result in a greater influence on the decisions relating to how data is used, and the incorporation of security controls directly into the product/app development process.
>
> **Andy Kennedy, EMEA Security Specialist, Google Cloud**



Osian ap Glyn, Director of Cyber Security Engineering, Atos UK & Ireland

What is prescriptive security from a technical perspective?

Prescriptive security is, at its heart, a fusion of technologies and processes designed to reduce the time and effort needed to detect and respond effectively to cyber security threats and incidents.

A critical aspect of prescriptive security is its use of automation and artificial intelligence technologies. It is vital that the exact combination of technologies and processes – including where and at what level automation is used – is based on a thorough understanding of the organisation's specific risk profile and level of risk appetite. Usually, prescriptive security solutions are based on selected types of security 'use case': a use case is a repeatable way of applying the technologies and processes; these evolve as new threats and challenges emerge.

Prescriptive security phases

Data collection

As with any analytical process, the relevance and quality of raw data is critical to success. For example, user entity behavioural analytics identify and analyse the actions taken by a user or an asset; the more diverse and relevant its sources of data, the richer the story it can create about a user's behaviour.

Based on each use case, it is possible to identify which types of data and logs must be collected and what additional controls need to be implemented.

Processing and fusion

Once all relevant data logs have been collected, they need to be stored centrally in as simple a format as possible ready for processing and additional data fusion. This is where a big data capability is important because it enables very fast processing of data models as well as rapid scalability if needed.

It is at this point that the data can be enriched with any other relevant threat intelligence, indicators of compromise, and any other data on the organisation's security posture that has been gathered by scanning the estate.

Using this fused and enriched data, machine learning will identify patterns of behaviour against learned norms or known adversarial fingerprints so that any threats can be identified.

Analysis and resolution

At this point, alerts will be automatically generated and presented to human analysts for fast evidence-based corroboration and action.

This is where playbooks and application programming interfaces (APIs) are used.

A playbook is a self-contained set of processes on how to deal with the most common incident types; they include procedures, advice, further enrichment tools and rapid access to the relevant toolsets for remediation. Playbooks can be created and expanded as the maturity of the security operation grows.

APIs enable end-to-end automation; each playbook calls on automated APIs to implement actions and changes with no human interaction required.

Critical resources

By implementing prescriptive security, the ever more precious human resource of analysts is freed up to focus on higher-priority, actionable scenarios. At the same time, the organisation gets better not only at detecting and responding to security incidents but also at predicting, preventing and pre-empting risks and incidents.

Against a backdrop of increasingly sophisticated and diverse cyber security threats, prescriptive security is becoming business-critical for public and private sector organisations to protect their people, customers, systems, networks and data from any kind of harmful breach or attack.

Example: a new virus on a corporate network

Here is an example of how a full prescriptive security incident might emerge and be dealt with.

A '0 day' polymorphic virus is found on a corporate network; this malware has never been seen before as it has chameleon properties and traditional anti-virus software has not detected its activity.

The presence of the malware is detected by its behaviour; machine learning tracks anomalous behaviour and alerts an analyst.

The data is enriched so that the analyst can see that the affected endpoint is in fact the CEO's executive assistant who has been the victim of a targeted phishing attack.

A playbook for malware infection is activated as the alert comes in; the analyst immediately decides to isolate the endpoint now that they know the business risk is low (the CEO's assistant is not considered business critical). The analyst can initiate the action with just a button press because the playbook is integrated via an API into the relevant endpoint detection and remediation product.

In addition, critical indicators of compromise have been discovered, for example the web address of the command and control servers used by the adversaries to coordinate this malware attack. This information is used to automatically update any 'blacklists' of activity and actors on boundary security so that even if there is another instance of the malware, it cannot make contact with its controlling infrastructure; this renders it useless to the adversary.

A ticket is automatically raised to have the assistant's laptop disinfected; this can be done slightly later as the problem has been isolated from the network and no longer poses an immediate threat.

From this incident, a maturity review can be done to decide whether, if this use case happens again, this playbook can be fully automated.

Stephen Wing, Security Consulting Practice Lead, Atos UK & Ireland

What is prescriptive security from a process perspective?

The processes around prescriptive security are distinct from those around traditional cyber security in a number of ways. To examine the differences, let us take the example on page 19 of the device belonging to the executive assistant to the CEO having been subject to a phishing attack, resulting in a virus. As every cyber security expert knows, phishing email campaigns are increasingly targeting smaller, more focussed groups and becoming more sophisticated and therefore more likely to succeed and business email comprise (BEC) has taken over as one of the major challenges.

Traditional security processes

In a traditional security environment, the analyst must first log into multiple tools to work out what is happening. The analyst uses each tool to view the necessary logs and data to understand the incident. Whilst the analyst might quickly establish that there is a '0 day' polymorphic virus, the tools may not link the endpoint with the user in order to easily trace the phishing attack. Without this link, actions to update security at the boundary may not happen quickly, if at all; as a result, more users could be affected.

The analyst also needs multiple security systems and applications to co-ordinate the right response. This will take time, especially if these security tools aren't in daily use – again increasing the risks to other users. There may also be risks associated with the order in which remediation steps are configured into the various systems. Even worse, where devices are offline or not connected back into the corporate network, the design of the virus keeps them vulnerable to attack for some time.

If the analyst is not sufficiently trained, or has no access to a particular tool, they may need to raise service tickets to action a response, further lengthening the time to respond, especially if those processes take time or the tool is not managed 24x7.

Each of these steps must be fully documented, with processes for logging into the various toolsets such as anti-virus management, network access control management, endpoint detection and response, in order to manually trigger actions.

Prescriptive security processes

With prescriptive security, the time it takes to identify a problem shrinks to milliseconds. Information about multiple events is collated into one place and enriched with threat intelligence ready as a single 'ticket' for the analyst to analyse and make decisions.

Straightaway, the analyst has better visibility of the incident using advanced data processing, analytics and security event management systems so they can quickly link the virus to the phishing attack and to the CEO's executive assistant. Given that this is a new problem, human intervention is needed and yet still minimal: the analyst selects the most effective playbook of automated actions to protect the whole estate.

This ultimately removes the risk of errors and not only improves the time to respond to the initial incident, but also helps to reduce or even eradicate the time to detect any similar subsequent incidents.

> Prescriptive security is a game changer: it transforms the way security analysts work so that teams can keep ahead of bad actors – even as they grow in number and get ever more sophisticated in their attack strategies.

Ongoing service management

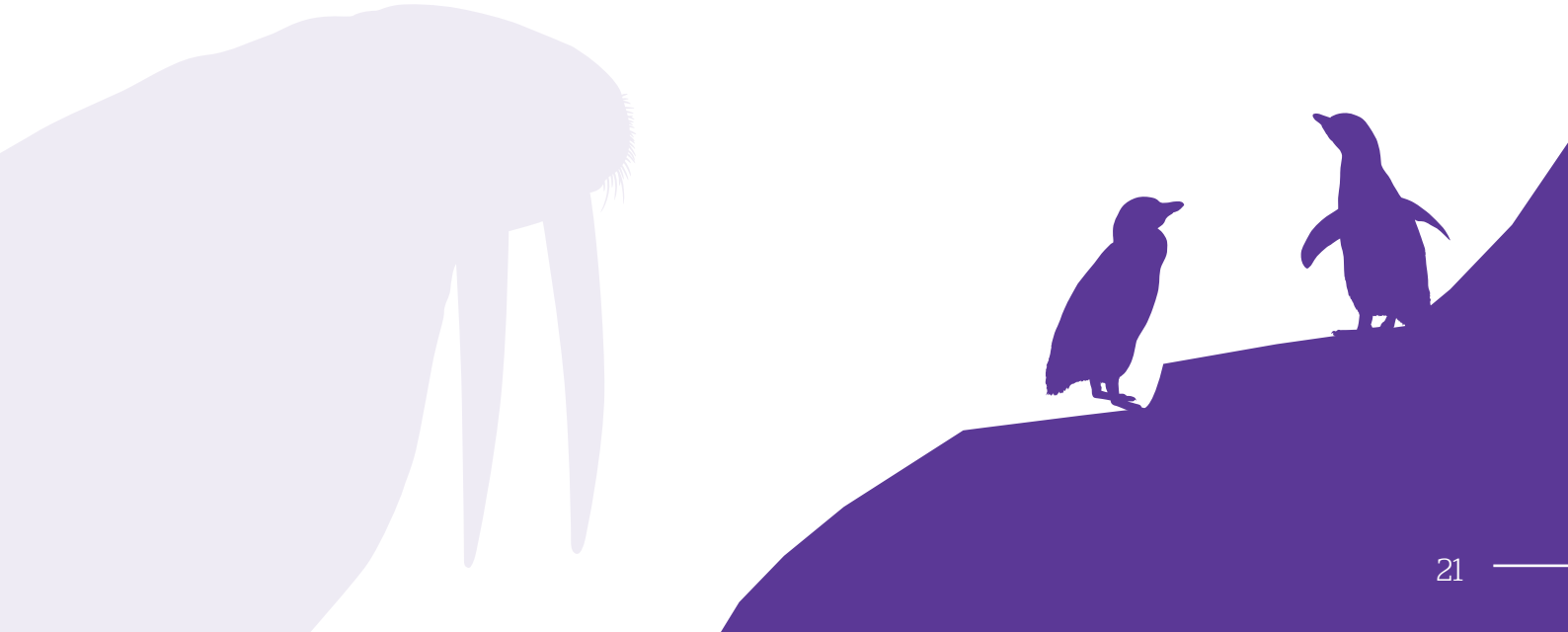
All security incidents are monitored, identified, prioritised and managed at the Security Operations Centre and a key part of security operations is integration with the rest of service management, for example, to ensure that every change to an IT estate is documented and audited.

If all details and current remediation tasks are held purely within traditional security tools, this is likely to lengthen the time to respond, and create extra change management tasks for the service management team. In contrast, with prescriptive security, everyone involved can easily be kept informed of the situation. So, for example, when the CEO's assistant rings the service desk the following morning because the device cannot connect to the network, the service desk can instantly see how and why the device has been isolated and explain this.

Forensic investigation

Following any serious incident, thoughts will turn to reviewing how the incident occurred, and how to predict and prevent similar attacks in future.

Just as having data spread across disparate systems makes analysing and responding to an incident slower, it also makes it harder to fathom details of the attack path in retrospect. In contrast, with prescriptive security, there is full auditability and continuous learning, working in harmony to bolster the defences against cyber threats. Prescriptive security is a game changer: it transforms the way security analysts work so that teams can keep ahead of bad actors – even as they grow in number and get ever more sophisticated in their attack strategies.



Life as a Security Operations Centre analyst

Meet Andreas Giorgakis, Security Analyst at Atos's Security Operations Centre (SOC)

What is your role as a SOC analyst?

My role is to work as part of a team to safeguard our customers' digital 'crown jewels'. Working in cyber security right now is fascinating and exciting because new threats are emerging all the time. Our greatest challenge is to keep pace with them, or even get ahead of them. The stakes are high: the costs and consequences of an attack can be serious – not just in terms of business continuity, but financially and reputationally, both for our customers and for Atos. I am totally focussed on preventing that happening by identifying, analysing and responding to security incidents.

A welcome change for me is the shift from repetitive work and alert management to automated threat analysis, called prescriptive security. With sophisticated and rapid analysis of complex and random data, this uses machine learning to identify and assess threats, and even remediate them. Far from replacing analysts, by eliminating repetitive tasks this intelligent automation frees up our time for more valuable work.

What kind of work does the technology free you to do?

We can focus on using our passion, skills and tools to unlock all the intelligence we have at our fingertips for more accurate detection and decision-making. For example, we reverse-engineer malware – which means working back from what the virus does, to understand the code that makes it function and block its effectiveness – or 'detonate' it in a controlled environment called a sandbox so that we can tune our systems to automatically detect and neutralise future attacks using these types of malware.

We can also develop our threat intelligence, for instance by setting up 'honeypots' – which are intentionally vulnerable servers – that lure in adversaries who attempt to break into them. From this, we can identify new sophisticated attacks, advise our customers about common passwords that adversaries use, or trace where an attack might be coming from. We can also focus on researching and identifying our customers' digital footprints, which is information that a person or entity leaves behind as a result of their online activity; we find sensitive customer data that has been leaked onto the web or dark web.

> Advanced technologies enable organisations to redirect resources to fine-grained and proactive threat detection. From identifying and processing known threats, in a monitored environment cyber experts can focus on hunting new and unique ones. This turns the most mature organisations from threat intelligence consumers to threat intelligence producers.
>
> **Lukasz Olszewski, Computer Security Incident Response Team and Threat Intelligence Lead, Atos**

How do you develop your skills?

Life in the SOC is a continuous learning curve; as an analyst I must have up-to-date knowledge on attacks, vulnerabilities and data leaks. I continually learn by practising my skills through my work and using free time to stay informed of new developments. More formally, there are also certification qualifications, defence security skills development and ethical hacking training to understand how hackers behave and react.

A challenging, but at the same time stimulating feature, is that as our defences become ever more effective, so too do attackers become more sophisticated in their strategies. Getting into the mindset of a threat actor is therefore essential. This is where 'gamification' training comes into play: undertaking training as a digital game experience, where analysts learn through simulated scenarios how to keep one step ahead of our adversaries. One useful training scenario is called 'Capture The Flag', a hacking simulation in which we race to break into systems to capture the 'flag', which is a unique text in a special file on the target system. As well as being a memorable and exciting way to learn, it puts us into the adversaries' shoes in order to understand their ways of thinking and acting.

Overall, I see my role as a huge responsibility as well as being very rewarding. We are contributing to society by helping to protect critical assets for and on behalf of citizens, governments and businesses. While our work is all behind the scenes, we're fighting on the cyber security frontline.

Did you know?

10 CYBER THREATS & ATTACKS EXPLAINED

1 Lone hacker website attack

In July 2019, an attack targeting vulnerabilities within part of a large financial organisation's website resulted in a data breach that affected around 100 million credit card customers in the US and six million in Canada. While it's unlikely that the data was used for fraud, the cost to the company was around $150 million.

2 Magecart

Originally thought to be one group, Magecart is now considered to be a number of cybercriminal organisations, some in competition with each other. They are commonly engaged in card-skimming and formjacking, using malicious code to steal credit card details and other information from payment forms on e-commerce sites. Two recent Magecart attacks hit the ticketing and airline industries in the UK in 2018.

3 Largest Denial of Service attack

A Denial of Service (DoS) attack in February 2018 rendered an online code management service used by millions of developers temporarily unavailable. DoS attacks often flood the targeted machine or resource with superfluous requests in an attempt to overload systems. The organisation called in assistance to reroute the traffic to its site while removing and blocking malicious data.

4 & 5 Meltdown & Spectre

These are two related examples of vulnerabilities within modern central processing units (CPUs) that stem from code designed to accelerate processing, but which can be maliciously exploited for unauthorised access to data. In 2018, researchers found over 130 samples of malware that tried to exploit Meltdown and Spectre vulnerabilities, although most appeared to be tests rather than live attacks. Since Meltdown and Spectre, new sets of vulnerabilities like 'Zombieload', 'fallout' and 'RIDL' have emerged which steal sensitive data from CPUs and cloud environments.

6 NotPetya

NotPetya started in June 2017 and targeted machines initially through updates to popular financial software after its source code was compromised. It affected companies in Ukraine and global companies with subsidiaries there, with costs totalling hundreds of millions of pounds; one company alone reported £100 million lost revenue.

7 Large scale unpatched software attack

In an attack on unpatched software, a global information solutions company that enables access to credit suffered a data breach in May 2017 that affected over 145 million US customers and over 15 million UK customers. Costs totalled $1.4 billion by May 2019, including legal and investigative costs, costs to improve security and shield customers from fraud, and a $700 million settlement with the US Government agencies.

8 WannaCry

WannaCry was a high-profile example of attacks that exploit vulnerabilities in software. Normally, when vulnerabilities come to light, software vendors write additional code called 'patches' to cover up the security 'holes'. WannaCry was a self-replicating ransomware attack that started in May 2017 and targeted unpatched Microsoft Windows environments. It affected over 200,000 machines in 150 countries, with collateral damage to public and private sector organisations and potentially hundreds of millions of pounds in operational losses.

9

Cloud Hopper

Cloud Hopper attacks infiltrate managed service providers, usually via a spear phishing email to trick employees into downloading malware or giving away their passwords. Attackers then use the cloud infrastructure to 'hop' from one target to another, gaining access to sensitive data. The original Operation Cloud Hopper, which started back in 2014, or possibly even earlier, hit a wide range of government and industrial entities in healthcare, manufacturing, finance and biotech in at least 12 countries; its costs are unknown.

10

Shamoon

Shamoon is an example of wiper malware, which is designed first to exfiltrate data and then to cover its own tracks and wipe the data from the machine, either by deleting it or overwriting it with garbage data. Shamoon specifically deletes the master boot records of a PC and renders it unable to start. While Shamoon dates back to a 2012 attack on national oil companies of Saudi Arabia, more recently it has affected other oil and gas organisations.

context

Dave Spence, Response Director, Context IS

Resilience in supply chains: a view from the cyber security frontline

As cyber threats grow and diversify, many organisations have been raising their own bar in terms of cyber security – but increasingly, they are being targeted via their supply chains.

Threat actors have always exploited the weakest links they can find and often these are human rather than technological. Adversaries leverage existing relationships of trust because, of course, people are less guarded with individuals or organisations they feel they know. Here in the UK, public and private sector organisations have diverse supplier bases; larger enterprises may have tens of thousands of companies in their extended supply chains. While relationships of trust exist between these entities, the reality is that many do not share a common understanding of the threats they face as a result of those relationships.

Through our work at Context IS, we know that adversaries are being successful at targeting organisations by exploiting vulnerabilities in relation to their suppliers, partners and subcontractors. One of the original major supply chain attacks of note was the Target breach in 2013-2014, which affected 70 million records, and we have investigated increasing numbers of ever more complex supply chain attacks over the last five years.

Growing risks

Providing remote access to critical systems for third parties, for instance, can significantly increase a company's 'attack surface' and makes the third parties attractive targets for attackers.

At the same time, within organisations, cyber security risks are growing as a result of so-called 'shadow IT': the software and apps that individual users acquire and maintain themselves – including automated software updates – from unverified and potentially dangerous sources. This was the source of the devastating NotPetya cyber attack in 2017, as well as a number of targeted attacks since. These include a massive malware attack in 2017 during which hackers replaced a technology company's original software with a malicious version that affected 2.3 million users and another in 2018, which sent malicious software updates from another technology company to half a million users.

Robust core processes

If an organisation has a connection with a third party, it needs to ensure that there are sufficient controls in place to manage the associated risks. For example, one key control for any kind of remote access would be multi-factor authentication to validate the individual.

It is important also for organisations to continuously manage who has access into their environments and systems and remove any unnecessary access, both for staff and external suppliers. In addition, robust processes and controls are needed, for example to prevent amended payments without additional authentication. Most importantly, staff need to be educated on how to spot suspicious activity so that they become a vital human firewall.

Additional security layers

Yet despite all these measures, we find that more advanced threat actors can circumvent key controls such as multi-factor authentication, where a user must enter at least two pieces of evidence before being able to access an account or machine. The answer, therefore, is to implement layers of prescriptive security controls – automated where possible – that not only limit initial access, but restrict ongoing activity, monitoring behaviours of third parties and identifying and investigating any anomalies.

In addition, companies need to define and implement effective responses in the event of an attack or systems failure. If we assume that breaches will happen, it is vital to have an effective incident response plan in place. The challenge is not only to detect and shut down incidents, but also to communicate with the relevant partners, organisations and customers. The General Data Protection Regulation makes this even more important given the financial and reputational implications.

Partner assurance

It is increasingly important for suppliers to understand that through a new business relationship they also inherit their customer's threat profile. They should therefore assess their level of cyber resilience against a combined threat landscape and not just their own.

More widely, supply chain and partner assurance models have tended to be paper-based, involving a process of answering questions about cyber security policies and procedures. In reality, this doesn't necessarily produce an accurate or up-to-date view of how effective the company is at mitigating risk against an evolving threat landscape.

Proxy measures

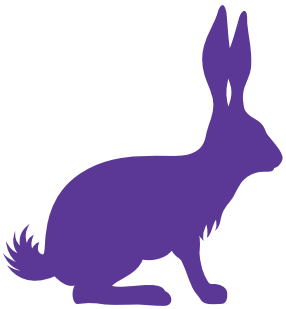
To more accurately assess and validate a company's cyber security posture, there are ways to take proxy measures of effectiveness, such as public domain intelligence or whether it has suffered an attack or a breach. However, while this kind of intelligence can be used to gauge how well suppliers might be managing their risks, it should not be used as a standalone measure.

We are currently seeing larger organisations and regulators wanting more proactive and comprehensive assurance of suppliers – especially in relation to business-critical systems and information. This could involve bringing the supplier into wider supply chain incident simulations and exercises, or contractually enforcing technical reviews by independent third parties if they are found to have a breach.

Remember, nothing and no-one is infallible and determined attackers will not give up easily. Companies under the impression that they have nothing worth taking need to understand that they might be a stepping stone to a more lucrative target. Ultimately, we are all part of someone's supply chain.

About Context IS

Context IS is a certified cyber security consultancy helping businesses to manage their cyber risk and detect and respond to sophisticated cyber attacks. The company provides specialist cyber security services, including penetration testing and red teaming, cyber incident response and threat hunting, and product security testing.



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

Security by design: the new cyber security paradigm

We are living in remarkable times as ongoing digitalisation transforms the world in which we live. It is estimated that by 2025, an average person will interact with connected devices around 4,800 times per day – that's one interaction every 18 seconds.

This speed of innovation is, however, also expanding the 'attack surface' and creating opportunities for threat actors to reach what is one of organisations' most valuable assets: their data. Cyber security must therefore be integrated into the fabric of organisations: in other words, organisations must be secure by design.

Security by design introduces agile security controls that can adapt to changing digital environments and is based on the following four elements: an understanding of the threat landscape; people; scalability; and speed. In addition, security by design must be underpinned by a robust ethics framework.

Understanding the threat landscape

Cyber criminals and state-sponsored actors are using innovative techniques to steal data, commit fraud, extort money and paralyse critical national infrastructures.

2017 was the year of ransomware. 2018 was the year of cryptojacking, as well as hardware flaws such as Spectre and Meltdown. In 2019, these cyber threats are still going strong: malware used to process cryptocurrency transactions using other people's computing power remains popular and variants in ransomware have increased nearly 50% since 2018. In addition, we are still facing vulnerabilities that are 'wormable', which means, for example, that patches issued for existing vulnerabilities may still be leveraged by cyber criminals to create the next Wannacry or NotPetya. Hardware flaws spawned more attacks and 2019 brought new cyber threats into the spotlight, such as Domain Name Service hijacking campaigns (to steal data by diverting traffic to spoof websites), inter-cloud attacks and cross-platform malware that moves from IT environments to industrial platforms, or vice versa.

In future, we will see more threat actors harnessing AI to launch ever more sophisticated attacks. It is, therefore, undeniable that traditional cyber security methods will not be a match for attacks perpetrated by smart machines: the need for cyber security by design is urgent.

People

Security by design should focus on people as much as technologies, and organisations need to ensure that all their employees are cyber aware and cyber vigilant.

Organisations lacking the necessary human as well as technological cyber security resources struggle to keep their security teams updated on the latest threats and technologies. Organisations should therefore identify expert partners who can walk this journey with them.

With an undeniable shortage of cyber security skills, it is predicted that by 2022, around 1.8 million cyber security jobs will be unfilled. As Europe's number one cyber security provider, Atos is active in addressing this challenge. With over 5,000 cyber security professionals and 14 security centres, we operate dedicated cyber security skills recruitment and development programmes – including our Cyber Academy and Digital Growth Network in Cyber Security.

Scalability

With the move to cloud and the arrival of a hyper-connected world, organisations need flexible and scalable cyber security solutions and services. For example, the adoption of edge computing (whereby vast computing power is transferred out into the network) is accelerating; swarm computing will be yet another major transformation, bringing together edge, multi-cloud and Internet of Things devices into highly distributed, hyper-connected computing environments.

New cyber security solutions will be orientated towards data-centric security, whereby the data itself is secured. Even today, advances in the use of strong encryption to protect data is in turn used to encrypt malware to avoid detection. In advanced prescriptive security environments, security controls will self-adapt to the changing threat landscape, all interconnected by prescriptive Security Operations Centre and security analytics either at the edge or in the cloud.

Cyber security specialists are also preparing for the quantum revolution by adopting quantum-safe encryption and leveraging the vast power of quantum computing to improve cyber security analytics for detection and response.

Speed

Cyber security should never slow down or block digital transformation, with security by design empowering organisations on their digital journey.

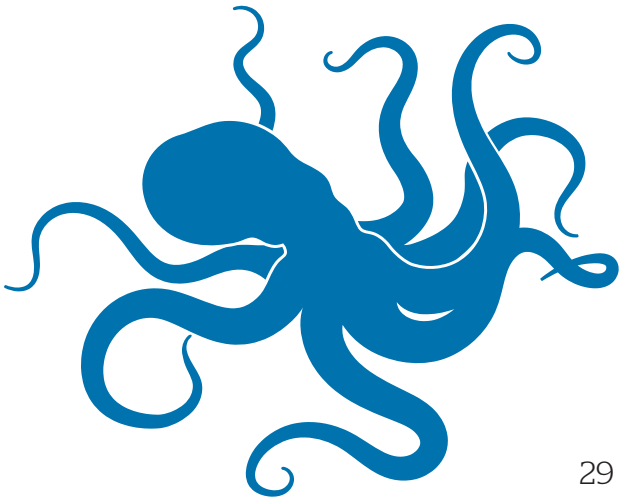
At the same time, the speed of cyber security innovation is so fast that organisations sometimes find themselves investing in a technology only to soon discover another that is more effective or efficient. Moving to procuring cyber security 'as a service'– instead of having to maintain their own cyber security infrastructures – will better enable organisations to adapt to changing challenges and threats and optimise the cost-efficiency of cyber security.

Instinct and intelligence

Security by design must be underpinned by a robust and evolving ethics framework. Data privacy and ethics are shaped by the changing regulatory landscape, with clear warnings from governments and others about the need for auditability and transparency in AI algorithms. Directing the power of AI is as much about what AI should do, as what it can do.

Organisations must therefore adopt an ethical framework that will guarantee that ethics and privacy controls are implemented throughout the data lifecycle, including the programming and adoption of AI and automation.

Given the pervasiveness and power of AI, the future of cyber security itself will be AI-powered, thwarting complex attacks and leveraging the best defence mechanisms to win the battle. Success will be thanks to the careful balance between instinct and intelligence and between human and machine – working together to protect people and infrastructures.



Sandy Forrest, Client Executive - Cyber Security, Atos UK & Ireland

How to create a protective cyber security ecosystem

In the physical world, the 'barbed wire and broken glass effect' has been used to describe a building that looks beautiful, but whose security is so lacking that barbed wire and broken glass must be retrofitted to keep intruders out. Similarly, in the digital world, ensuring that cyber security is proactively and fully integrated into business operations is vital.

Key to this is to create a cyber security ecosystem that is end to end – from cyber security strategy, through policy, design, delivery and incident resolution. This is commonly supported by a specialist cyber security consulting and managed service provider, whereby multi-disciplinary cyber security experts work with people in the business to develop and implement the right cyber security strategy and policies.

Identifying challenges and risks

To create a truly protective cyber security ecosystem, the starting point shouldn't be 'which solutions or equipment do we need?', but 'what business challenges do we have and what threats do we face – not just generic threats but those specific to our business?'. This includes looking at organisational governance, risk and compliance structures, including any specific legal and regulatory requirements.

Developing the strategy

The National Cyber Security Centre (NCSC) has published advice for organisations developing their cyber security strategies, including its 10 Steps to Cyber Security and Cyber Risk Toolkit. In addition, for organisations delivering essential services according to the NIS (Network and Information Systems) Regulations, the NCSC has published a Cyber Assessment Framework. All of these have a common theme around assessing an organisation's cyber security risk and the impact of this on its business, understanding the infrastructure, identifying any gaps in security, and making rational decisions on what controls are necessary and proportionate.

Devising the right security controls

Using a specialist security provider, security controls can be devised using an integrated suite of cyber security value propositions, which translate business challenges and cyber threats into a series of security controls that will work in harmony. Working with Cyber Security Specialists, a skilled Cyber Security Architect will have oversight and ensure that that there are no overlaps or gaps. This includes managing Operational Technology (OT) and Internet of Things (IoT) devices through IT/OT/IoT security management.

Building resilience into the supply chain

Given the risk of adversaries targeting organisations via others within their supply chains, implementing federated cyber security solutions and controls will ensure that these risks are assessed and managed. Through a federated approach, larger organisations can protect themselves by extending the cyber security services they use into other organisations in their supply chain. This requires rigorous cyber security assessments by suppliers and other partners to ensure sufficient and comparable levels of cyber security and cyber vigilance.

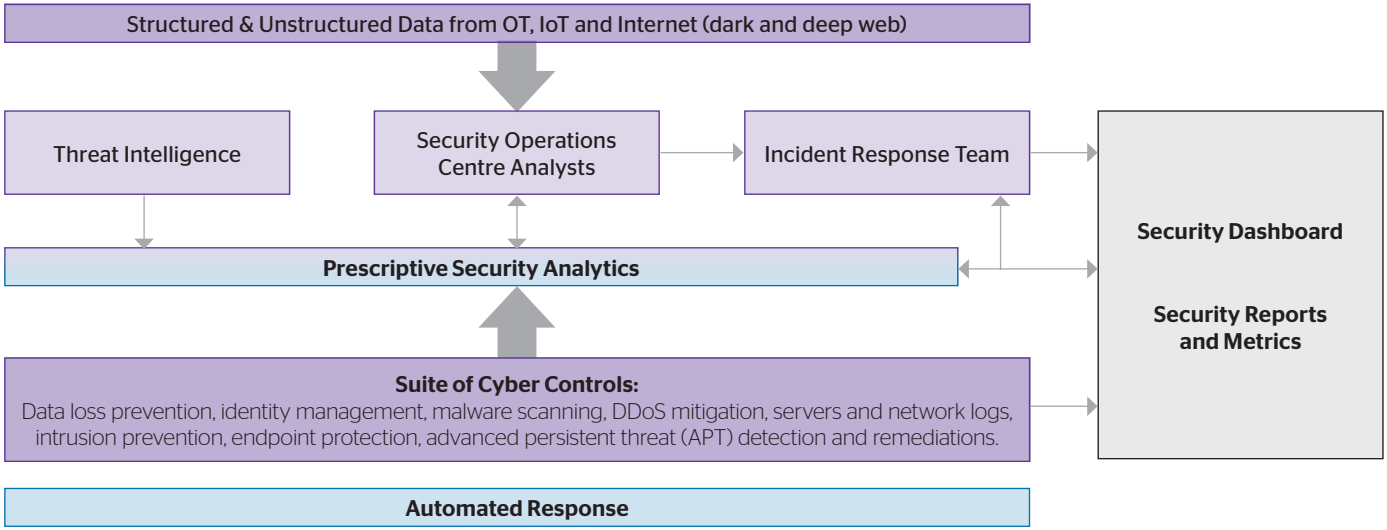
Securing a hybrid cloud

Some organisations can use a single commodity cloud provider to meet all their IT needs. However, the overwhelming majority need a hybrid cloud solution; this means they either procure services from multiple cloud providers, or they want to maintain part of their services on legacy equipment, either on-premises or in a data centre. Managing security, either cloud-to-cloud or cloud-to-legacy, or both, requires use of a Cloud Access Security Broker solution from a managed service provider.

Collecting the evidence

It is important that decisions on risk are evidence-based, with that evidence made available by establishing a single integrated view of what's happening in the network and out in the wider cyber world. This is achieved by deploying a modern Security Incident Event Management (SIEM) tool and monitoring at a Security Operations Centre. Here, specialist technicians and analysts, supported by prescriptive security capabilities, can identify and manage any incidents, dramatically reducing the time to identify and remediate threatening incidents.

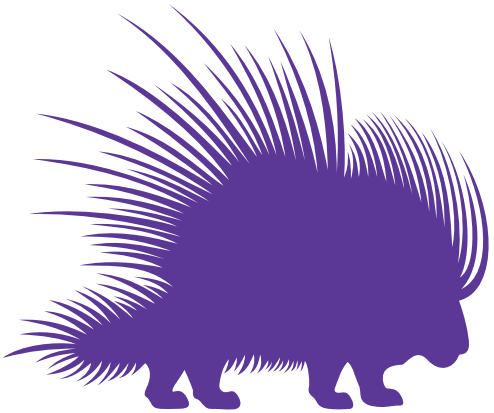
The Prescriptive Security Ecosystem



Critical enabler

Most organisations today need to implement digital transformation to optimise their efficiency and effectiveness and to deliver services and products in new ways. This must all be achieved securely right from the start to avoid infrastructures being damaged or exploited through cyber attack or unintentional misuse.

In all cases, creating a protective cyber security ecosystem requires an objective and comprehensive review and assessment of what is already in place. And whatever the partnership and supplier arrangements, cyber security must be built into the delivery of IT and business services and 'baked in' to technology solutions. Cyber security is not an add-on: in the digital world, it is a critical business enabler for any organisation to achieve its ambitions.



Lexicon

Application Programming Interface (API): a set of routines, protocols, and tools for building software applications. Basically, an API specifies how software components should interact.[1]

Behavioural analytics: looking for aberrant behaviour by an individual or a computer that may suggest there is a risk that needs to be addressed (e.g. that a user has become an insider threat or a computer may have been compromised).

Cross-platform malware: designed with payloads capable of running on multiple platforms e.g. Windows, Linux MacOS X. The implication is that the potential reach and impact of a single piece of such malware is significantly larger than for OS specific variants.

Cryptojacking: a malicious use of a person or persons' computing power to mine cryptocurrencies without consent. Often the victim has no idea their device is being used.[2]

Data exfiltration: the unauthorised copying, transfer or retrieval of data from a computer or server.

Data fusion: the process of integrating multiple data sources to produce more consistent, accurate, and useful information than that provided by any individual data source.[3]

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.

Digital forensic technologies: an area of forensic science that deals with the analysis of data retrieved from digital devices connected with investiga-tions into computer crime.

Domain Name Service (DNS): the way that internet domain names are located and trans-lated into internet protocol addresses. A domain name is a meaningful and easy-to-remember 'handle' for an internet address.

Edge & swarm computing: edge computing describes compute resources beyond the boundaries of data centres. Swarms are formed when these edge devices are able to interact and co-operate as self-organising intelligent groups.

Endpoint: an endpoint is a remote computing device that communicates back and forth with a network to which is it connected.[4]

Exploit: in the context of cyber security, a code that finds a vulnera-bility in a machine or network and exploits it.

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

Fourth industrial revolution: the current and developing environment in which disruptive technologies and trends such as the Internet of Things, ro-botics, virtual reality and artificial intelligence are changing the way we live and work.[5]

General Data Protection Regulation (GDPR): regulation that places obligations on organisations in relation to the protection of personal data and requirements to report data breaches.

Identity and Access Management (IAM): a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate ac-cess to technology resources.[6]

Incident management: manages the lifecycle of all incidents (unplanned interruptions or reductions in quality of IT services). The primary objective of this Information Technology Infrastructure Library (ITIL) process is to return the IT service to users as quickly as possible.[7]

Inter-cloud: a single common functionality combining many different individual clouds into one seamless mass in terms of on-demand operations.[8]

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

In association with SANS (unless otherwise stated as footnotes):
https://uk.sans.org/security-resources/glossary-of-terms

1 https://www.webopedia.com/TERM/A/API.html
2 https://www.forcepoint.com/cyber-edu/cryptojacking
3 https://en.wikipedia.org/wiki/Data_fusion
4 https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint
5 https://whatis.techtarget.com/definition/fourth-industrial-revolution
6 https://www.webopedia.com/TERM/I/iam-identity-and-access-management.html
7 https://wiki.en.it-processmaps.com/index.php/Incident_Management
8 https://www.techopedia.com/definition/7756/intercloud

National Cyber Security Centre (NCSC): the UK's independent authority on cyber security.

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

Payload: in computer security, the payload is the part of the private user text which could also contain malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.[9]

Phishing: A cyber crime in which individuals or companies are contacted by email, text or phone by someone posing as a trust-worthy 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.[10]

Playbook: a self-contained set of processes on how to deal with the most common incident types; they include procedures, advice, further enrichment tools and rapid access to the relevant toolsets for remediation.

Polymorphic virus: a complicated computer virus that affects data types and functions. It is a self-encrypted virus designed to avoid detection by a scanner. Upon infection, the polymorphic virus duplicates itself by creating usable, albeit slightly modified, copies of itself.[10]

Privilege Access Management (PAM): a class of solutions that help secure, control, manage and monitor users' privileged access to critical assets.[11]

Quantum encryption: quantum key distribution allows cryptographic (encryption) keys to be exchanged between two parties with guaranteed privacy — typically using photons transmitted through fibre-optic cable. Data transferred in this manner can't be intercepted or manipulated without leaving clear evidence.

Ransomware: a type of malware that is a form of extortion. It works by encrypting a victim's hard drive, denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.[xiii]

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

Security Operations Centre (SOC): 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.

Shadow IT: information technology (IT) applications and infrastructure that are managed and utilised without the knowledge of the enterprise's IT department.[12]

Terabyte (TB): a unit of information where a single terabyte is equal to one thousand gigabytes.

User and entity behaviour analytics (UEBA): a type of cyber security process that takes note of the normal conduct of users. In turn, they detect any anomalous behaviour or instances when there are deviations from these "normal" patterns.[14]

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 programmes and machines are compromised.

'0 day' attack: A '0 day' (or zero-hour or zero-day) attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software developer knows about the vulnerability.

[9] https://en.wikipedia.org/wiki/Payload_(computing)
[10] https://www.techopedia.com/definition/4055/polymorphic-virus
[11] https://doubleoctopus.com/security-wiki/authentication/privileged-access-management/
[12] https://www.webopedia.com/TERM/S/shadow-it.html
[13] https://techterms.com/definition/terabyte
[14] https://digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more

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	Senior Executive Vice President Chief Executive Officer, Atos UK & Ireland
Pierre Barnabé	Senior Executive Vice President Head of the Global Division Big Data & Security, Atos
Gavin Thomson	Senior Vice President, Private Sector and Big Data & Security, Atos UK & Ireland
Phil Aitchison	Chief Operating Officer, Big Data & Security, Atos UK & Ireland
Matt Warman MP	Parliamentary Under Secretary of State (Minister for Digital and Broadband), Department for Digital, Culture, Media and Sport
John Hall	Head of Portfolio, Atos UK&I and Scientific Community Expert
Thierry Breton	Former Chairman and CEO, Atos
Talal Rajab	Head of Programme, Cyber and National Security, techUK
Mike Smart	Senior Analyst and Operations Officer, NelsonHall
Mandy Haeburn-Little	CEO BRIM, former Chief Executive, Scottish Business Resilience Centre
Maxine de Brunner QPM	Former Deputy Assistant Commissioner, Metropolitan Police Service
Kevin Cooke	Head of Cyber Security Delivery, Atos UK & Ireland
Andy Kennedy	EMEA Security Specialist, Google Cloud
Osian ap Glyn	Director of Cyber Security Engineering, Atos UK & Ireland
Stephen Wing	Security Consulting Practice Lead, Atos UK & Ireland
Andreas Giorgakis	Security Analyst, Atos UK & Ireland
Lukasz Olszewski	Computer Security Incident Response Team and Threat Intelligence Lead, Atos
Dave Spence	Response Director, Context IS
Zeina Zakhour	Distinguished Expert, Global Chief Technical Officer, Cyber Security, Atos
Sandy Forrest	Client Executive - Cyber Security, Atos UK & Ireland

Production team

Editor: Kulveer Ranger
Production team: Heidi Idle, JooYun Jung, Sarah Waterman
Design team: Atos Marcom Agency
Consultation: Phil Aitchison, Sandy Forrest, Charlotte Januszewski, Felipe Hickmann, Adam Fisher

About Atos

Atos is a global leader in digital transformation with over 110,000 employees in 73 countries and annual revenue of over € 11 billion.

European number one in Cloud, Cyber Security and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information technology space. Its expertise and services support the development of knowledge, education as well as multicultural and pluralistic approaches to research that contribute to scientific and technological excellence. Across the world, the group enables its customers, employees and collaborators, and members of societies at large to live, work and develop sustainably and confidently in the information technology space.

Find out more about us
atos.net
atos.net/dvfcs

Let's start a discussion together

CT_190816_JM_DIGITAL-VISION-FOR-CYBER-SECURITY-2