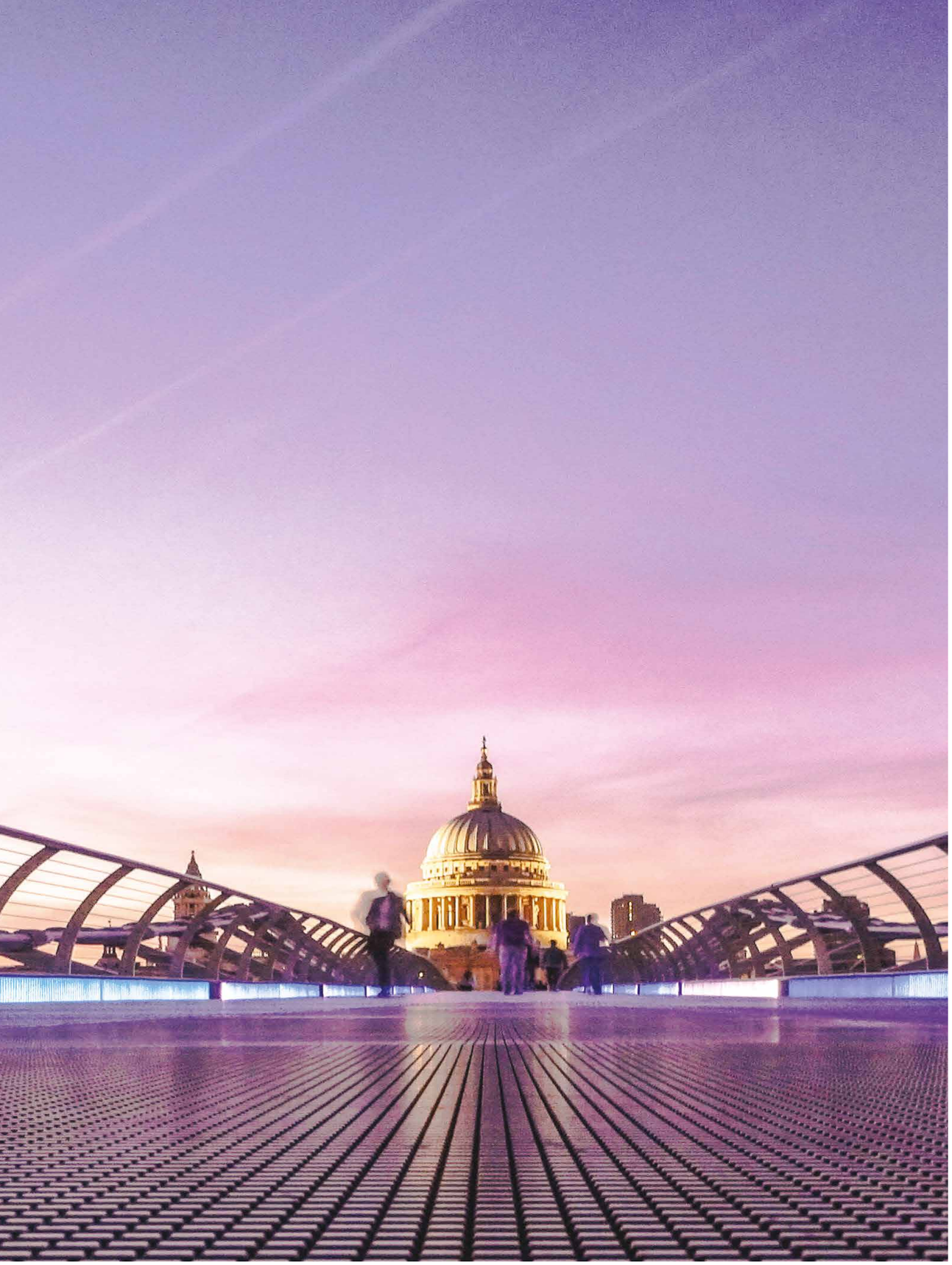

SECURITY
THROUGH
INNOVATION
Secgate

# CONTENTS

# SETTING THE SCENE



# CURRENT SITUATION AND PERSPECTIVES

## Take Leadership In A Digital World

The global digital landscape is constantly evolving. Global digitisation brings opportunities for organisations to grow. As network infrastructures and IT systems develop to meet the increased reliance on digitisation, cyber opportunists look to benefit.

No matter who you are, information is collected, stored and utilised about you and your organisation in data servers across the world. The incentives to compromise this information differ from financial gain, to politically motivated disruption, to abject anarchy. In the midst of ever changing uncertainties, one thing is certain: If you haven't already been affected by this – you, and your organisation, will be.

Tackling cyber crime might not be your primary business concern: However, the ability to securely access your own digital infrastructure and for your customers to securely digitally interact with you is, critical to your commercial success.

Today, we see the frequency and severity of cyber attacks on the rise. High profile hacks at some of the world's largest companies make it onto the front pages of our newspapers on an almost weekly basis. It is imperative for the sustainability of all of our industries that we are prepared for - and protected against - cyber crime.

This is where we come in; our end-to-end cyber security programmes are driven by world class cyber security experts and are supported by unsurpassed technology solutions.

- Our Cyber Security Consultancy services provide expert advice on the best strategies to combat cyber crime
- Our Cyber Security Technology solutions monitor and remediate threats, utilising cutting edge machine learning algorithms to detect anomalous behaviour on your network
- Our Threat Intelligence solutions draw intelligence from the full spectrum of available data feeds and will put you one step ahead of the wide range of threats that exist
- Our Security Lab staffed by inhouse experts can train your staff to become leaders in the fight against cyber crime
- Our Cyber World platform offers a unique stage where you can share knowledge with other organisations and learn what is happening in the cyber security marketplace

Secgate cannot combat cyber criminals alone and you shouldn't have to try either. Do not leave yourself isolated in the event of a cyber attack - let us work together to combat this growing threat and to build a safe and successful working environment.

Yours,

**Laith Gharib**
Managing Director, Secgate

# RAPID ADVANCEMENT OF TECHNOLOGY

## Global Technology Trends

As nations grow, so does consumer pressure on organisations to provide faster, more advanced and intelligent network infrastructures. This pressure drives investment into increasingly complex technologies that deliver the solutions that consumers require. This includes increasing utilisation of Artificial Intelligence, Machine Learning and emerging technologies such as Blockchain. The timeline on the right demonstrates the speed at which cutting edge technologies have developed over the past decade.



## Technology Breakthroughs & Trends

**2007**

Emergence of web-oriented architectures, possibilities of unified communication platforms and capacity for virtualisation

**2012**

Development of cloud computing, utilisation of big data, usage of media devices and mobile applications

**2017**

Development of AI, machine learning and conversational systems that can develop into entirely ‘intelligent systems’

**2022**

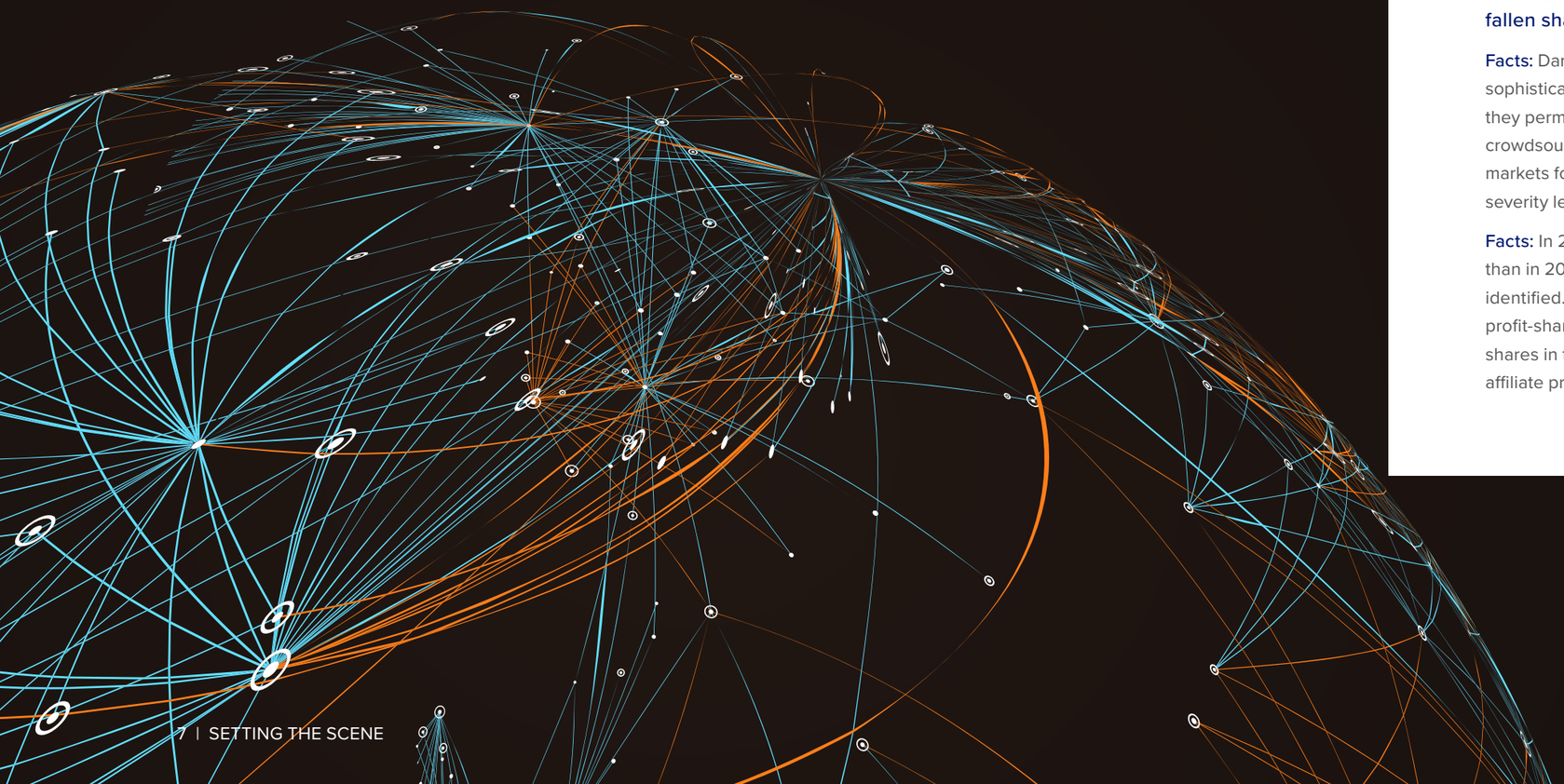
Projected Trend: Intelligence at the edge of the Internet of Things (IoT), voice as the dominant user interface, advances in DNA and microbiome applications; organisations will employ mass AI adoption

# GLOBAL CYBER SECURITY SITUATION

## Understanding The Scale Of The Issue

Technology is advancing exponentially both in terms of its complexity and its adoption to support our critical systems of interaction. A decade ago the possibilities of web–oriented architecture and unified communication were only first being explored; in the next five years, we can expect to see interaction with AI utilised at almost every single end point. The ability for digital devices to communicate, both with us and with themselves, has proliferated cyber attacks for organisations across the world to a mind–boggling complex level.

The true cost of cyber crime is unknown. However the global cost is estimated to reach **$6 trillion** by 2021 from **$3 trillion** in 2015.



**Globally, we are seeing major shifts in the aggression and scale of cyber attacks:**

### The scale for citizens to be exposed to cyber attacks has risen dramatically

**Facts:** The interconnectivity of systems has led to cyber attacks that can span multiple continents at once, causing disruption to citizens worldwide. The May 2017 Wannacry ransomware attack affected 200,000 people in 150 countries, taking advantage of a security exploit on a global scale. Research shows that one in every 131 emails now contains malicious source code attachments.

### Attacks go beyond economic espionage and into the realms of internationally politically motivated sabotage and subversion

**Facts:** Governments are bolstering their cyber security offensive and defensive capabilities as other states fund and provide amnesty for their hackers' activities domestically. Well publicised hacks conducted by nation states are on the rise, with alleged attacks on the American democratic processes, Ukraine's energy grid, Iran's nuclear centrifuges and various activities from Chinese and Russian affiliated groups. The cyber arms race looks set to continue as geopolitical conflicts continue to rage.

### The barrier to accessing advanced cyber security weaponry has fallen sharply

**Facts:** Dark web channels allow unskilled hackers to purchase and deploy sophisticated attack techniques with limited technical capability. Plus, they permit highly skilled hackers across the world to collaborate and crowdsource the development of malware. The development of established markets for Hacking as a Service (HaaS) has amplified this threat at all severity levels.

**Facts:** In 2016, there were 167 times the number of ransomware attacks than in 2015, with a 752% increase in the amount of ransomware families identified. This has been largely attributed to the development of a free, profit-sharing Ransomware-as-a-Service (RaaS) model in which the author shares in the affiliates' earnings, similar to a legitimate software affiliate programme.

## Cyber Threats Affect All Countries And Regions

Despite these trends, organisations across the globe continue to be both unaware and unprepared to deal with a cyber threat.

### United States (US):

A survey of 509 North American companies across various industries, revealed that 79% of IT professionals do not have the appropriate infrastructure to identify and defend against cyber attacks. 38% stated that their cyber security controls were non-existent despite the average cost of a cyber attack to each of the companies surveyed totalling $3.5 million a year.

### United Kingdom (UK):

In 2017, two thirds of the boards of Britain's 350 biggest companies had not received any training to deal with a cyber incident. This was in spite of more than half of the businesses stating that cyber threats were a 'top risk' to their organisation. Only 53% of company boards have set out their approach to cyber risks, compared to 33% a year ago.

### Africa:

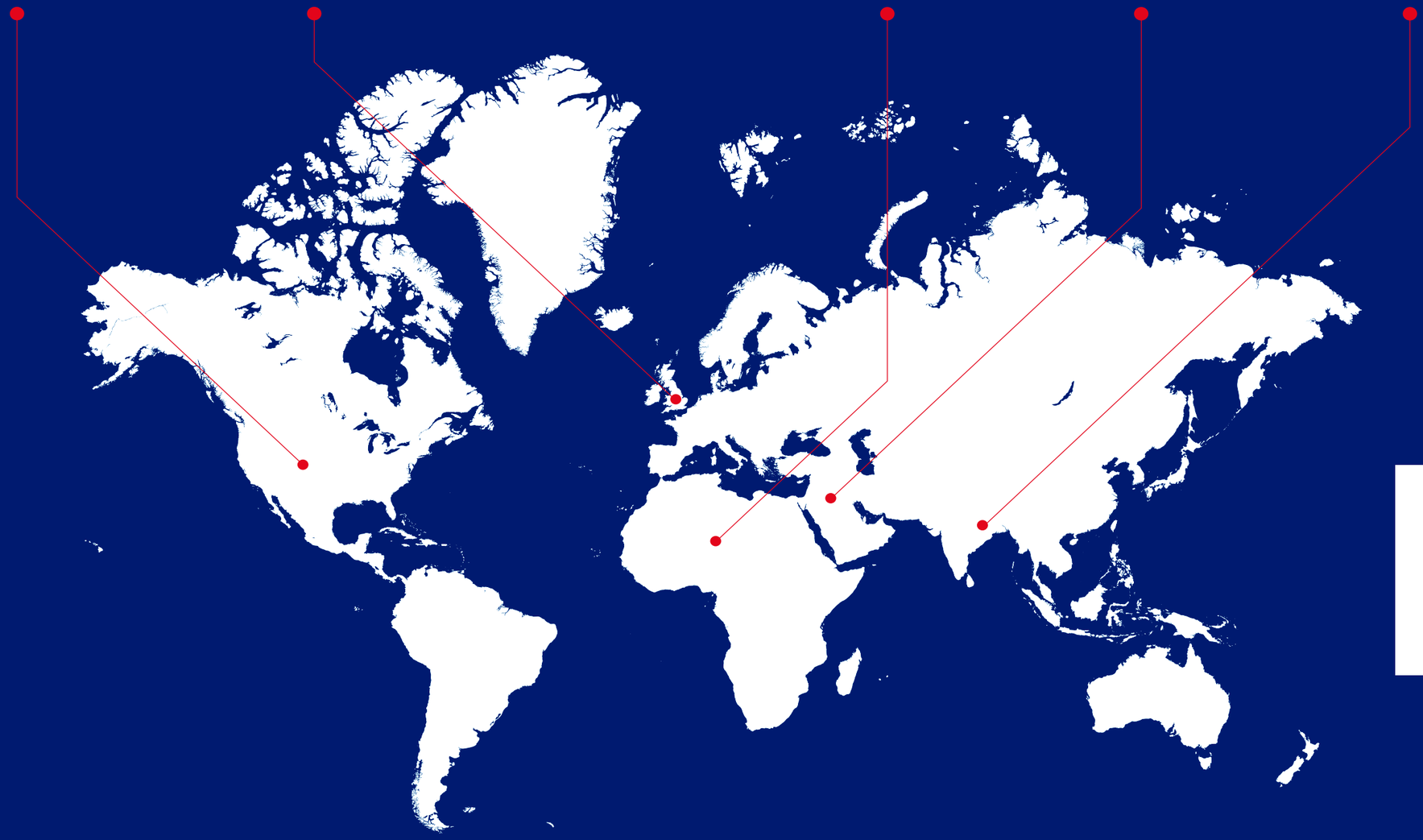
Internet users almost tripled from 167.3m people in 2012 to 448m as of June 2016. Despite the estimated cost of cyber crime totalling $2bn in Africa there were only 6,892 certified cyber security professionals reportedly working in the continent during the same period.

### Middle East:

A regional survey reported that despite most firms considering reputation as their single most important asset, 42% of respondents said that their organisation had suffered high or medium level damage to their status as a result of cyber attacks. This compares to 30% globally.

### Asia-Pacific (APAC):

In 2016, 90% of APAC companies surveyed reported a cyber attack of some form. This was an increase from 76% in 2015 and 66% reported incidents by the same companies in 2014.



It is clear there is a dissonance between understanding the global cyber threat and a nation's or organisation's ability to protect themselves from one.

# THE COMPANY

# WHO WE ARE

## Security Through Innovation

Secgate is a cyber security innovation group revolutionizing the method of delivering solutions. Our team of experienced professionals have been handpicked to deliver intelligent protection solutions that strengthen and empower clients' IT security and resilience. Combining security consultants, threat intelligence agents and technologists allows us to deliver next generation solutions to our customers and partners. This ensures tangible value is provided to each engagement we take part in.

### Our Mission

Driven by our relentless desire to succeed and our passion for innovation, Secgate aims to be the pre-eminent cyber security company. We aspire to be recognised across the globe for our innovative security solutions which are clearly differentiated in terms of delivering tangible results, quality of service and generating premium rate return for our customers.

### Our Values

At Secgate we are united by a collective passion for our craft and a communal ambition to provide cutting-edge solutions. At the heart of our approach is innovation, that drives us to push the boundaries of what is considered best practice within our industry. We value proactivity and inclusiveness in all areas of our business, from the people that we hire to the clients we engage with. Our global team has a culture and environment that recognises and supports diversity through inclusion and development of each individual.

### Our Ethics

We deliver with integrity and aim to innovate with every engagement. Each client is given a personalised and tailored solution to fit their own business needs. We provide this through services and technology, or a combination of both. We build loyal, trusted partnerships that enable our clients to grow through resilient IT security.

# A TEAM OF GLOBAL SECURITY EXPERTS

## Focused On Protecting Your Business

Secgate is a dynamic and diverse company with a passion for security. Our team is focused on delivering effective, viable and innovative solutions to our customers. We aim to prepare for, overcome, and further prevent, the world's most complex cyber problems.

As a group of accomplished global security experts, we are passionate about our craft. The products and services we develop are market-leading, delivered with integrity and trusted by our customers worldwide. In the marketplace, we are renowned for our honesty, know-how and ability to swiftly act and engineer the right solutions at the right time.

**Laith Gharib**
Managing Director

Laith leads Secgate's mission to combating cyber security throughout the world. With over 15 years international business experience, ranging from software development to physical and cyber security, Laith has protected some of the largest organisations in the world. Holder of the Ovum Industry Award for innovation, Laith continues to challenge himself and his team to design revolutionary technology innovations. Prior to founding Secgate, he held positions at Deloitte and KPMG.

**Chris Gould**
Head of Consulting

Former Partner for Cyber Security and Cyber Crime at EY and PwC, Chris is Head of Consulting at Secgate. He specialises in information risk and has over 25 years experience in assisting organisations throughout the world to assess and manage technology related threats, specifically in information security, business continuity and crisis management. His pragmatic approach enables him to get to core issues quickly and provide value.

**Iván Blesa**
Head of Technology

Specialising in business model and strategy definition, Ivan is responsible for Secgate's technical team to continually create effective cyber security solutions through innovating technology. Previously, he globally led a high-profile data loss prevention company where he defined product strategy and successfully launched business solutions. His experience includes analysing safety critical applications for satellite navigation systems in space.

**George Thompson**
COO, Head of Enterprise Solutions

Former Director at KPMG and Chief Information Security Officer (CISO) to a major communication company, George heads Enterprise Solutions at Secgate. He specialises in helping business leaders focus on the development of their operations and exploring opportunities to integrate their enterprise security requirements into Secgate solutions. George is highly experienced in the international cyber arena helping businesses across various sectors.

**Steven Hutt**
Head of Machine Learning

Former Managing Director at UBS and Executive Director at Morgan Stanley, Steven leads the machine learning team at Secgate. He specialises in the design and implementation of scalable learning algorithms for the analysis of network flows. Steven's in-depth knowledge of machine and deep learning includes financial data analysis, automating market strategies, building intelligent network intrusion detection applications and order flow analysis solutions.

**Mak Chishty**
Head of Government Solutions

Former Commander at the Metropolitan Police Service, Mak was responsible for overseeing the development of community relations in London and working with international partners on public policy and reform. He was awarded the Queen's Police Medal for Distinguished Service with 30 years of policing experience at the forefront of national and international policing. His experience is invaluable in leading Government Solutions at Secgate.

# ONE STEP AHEAD

## A Complete Cyber Security Solution For Your Full Protection

At Secgate, we are dedicated to protecting you and your organisation. As security experts we fully understand the cyber threats that you face and have strategic consultancy services and technologies to not only stop them, but reduce the risk of them happening again. Our approach to working with you is to provide a comprehensive cyber security solution from a health check of your network and systems, reviewing your internal IT security protocols, analysing internal and external security threats and devising a scalable risk management strategy.

We differ in our approach as our end goal is for you to own your security risk management strategy. For this to be effective, we will provide you with the necessary tools and training, plus continue to support you as and when needed. We are unique in that the technology we have designed allows us to have full visibility of anomalies in your network infrastructure and systems. We can then analyse in parallel to external open and closed source information. This approach enables us to have full intelligence of where threats are coming from and to anticipate where they are likely to derive from in the future.

We also understand the complexities of organisations and businesses across different sectors and countries and as such, our services and technologies are flexible to fit individual business requirements. Our passion is security and we feel strongly that all citizens should have the freedom to be able to go about their business and live freely. To this end, we have a unique offering, called White Wolf, to support governments in their fight against cyber crime and to protect their nation.

Our team prides itself on leading the world against cyber crime. As thought leaders and innovators we have devised a platform wherein security professionals and industry leaders can debate cyber threat issues and help educate others in a common language for the boardroom or in a laboratory. We call this Cyber World.

Cyber crime is here to stay as it is a profitable business for the criminals involved - whether monetary, politically or motivationally. Our experienced team - from security experts to technologists - coupled with our consultancy services and intelligent technology are ideally positioned to ensure that you protect your assets, people and future business success. We help you stay one step ahead from cyber crime.



# CONSULTANCY

# CYBER SECURITY CONSULTANCY

## Protecting And Empowering Your Business

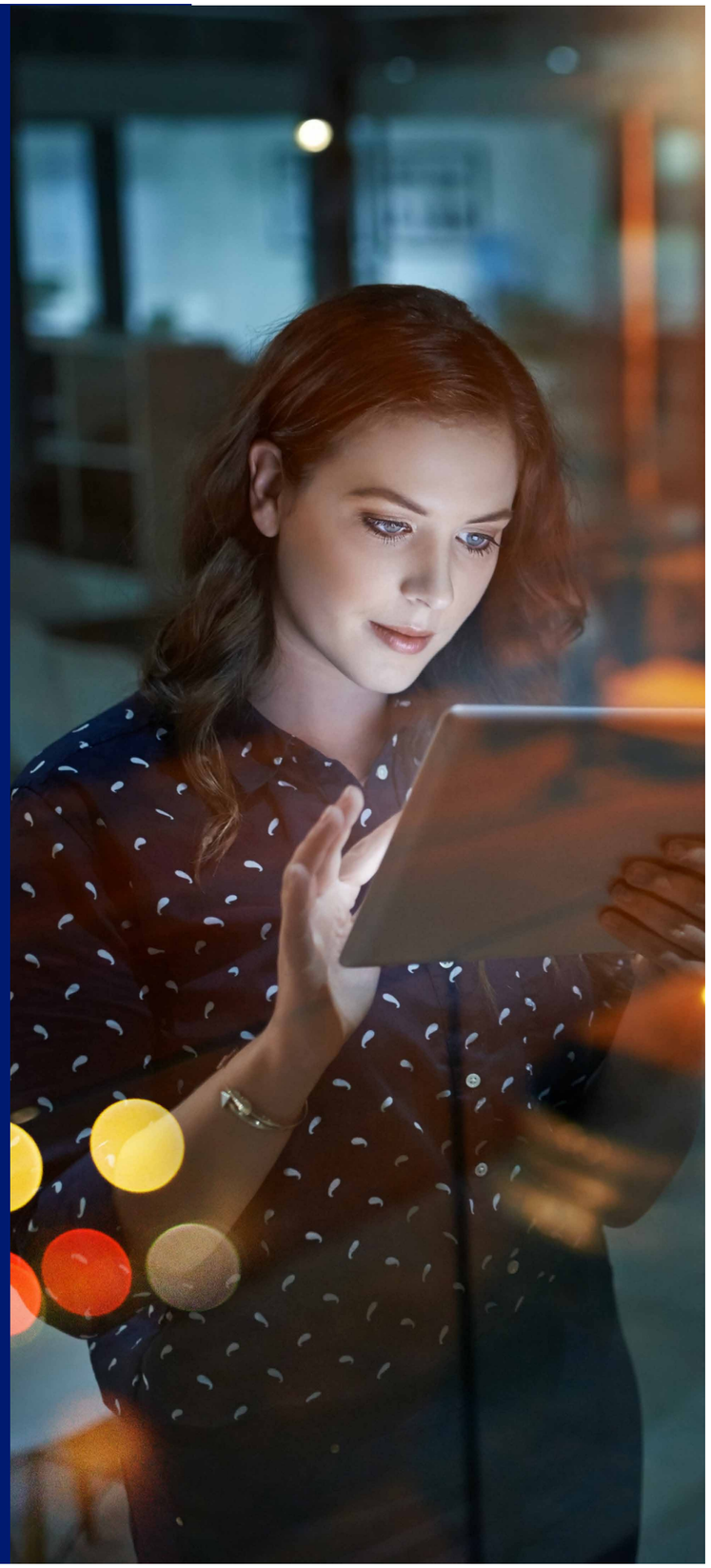
At Secgate, we care about protecting institutions, organisations and consumers from rapidly increasing cyber threats. We are united in our concern for the rising disparity between the capabilities of today's cyber attacks and organisations' cyber defence capabilities. This widening gap potentially exposes all citizens to damaging risks. With cyber criminals undeterred by the increased probability of being caught, it is critical that a sustainable solution is developed to enable your organisation to keep pace with changes in the threat landscape.

Secgate was founded to think differently about this problem. From the outset, we gathered the cyber security industry's leading problem solvers, strategists and forward thinkers together to design far-reaching cyber security consultancy solutions that went beyond traditional services.

At its heart, our solutions revolve around two key principles:

**Threats are a collective action problem. Solutions cannot be solved in isolation.**

**Utilise the opportunity to empower your business by delivering additional value to customers and achieve your long term digital goals.**



Our Cyber Security Consultancy team has international experience at the world's top consulting firms. Building on these foundations, they joined Secgate to design and deliver solutions that are proactive rather than reactive, flexible enough to be tailored to a client's individual problems and to empower organisations to own their long term cyber risk management strategy.

### Partnering with the best people, technologies and clients

Whilst having the best team is critical to solving the problem, we understand that unsurpassed cyber security is enabled by smart technology. At Secgate, we align with the cyber industry's best thinkers and connect them to our core technologies developed by world leading experts, to create robust cyber security solutions. Our flagship technology products are powered by our core intelligence solutions to monitor, analyse and secure an entire organisation's digital infrastructure in real time. We work in partnership with clients throughout the globe to develop security solutions specifically to solve their current cyber problems and counter future issues.

### Our primary goal

To give you confidence about your cyber security capabilities so that your organisation can understand the implications of changes in the cyber threat landscape and the long term impact.

# COLLECTIVE ACTION PROBLEM

Robust cyber security, like good national security, is most effective when people within an organisation understand, communicate and implement sound cyber security practices as a collective. It is here, that we perceive cyber security consulting differently.

We believe:

**Cyber security is a collective action problem and is everyone's responsibility**

**Cyber security is a critical enabler for businesses in the digital age and not a bottom line cost**

These two principles are the starting point for our Cyber Security Consultancy as they push us to discover a deeper and broader insight into the root causes of cyber risk. This enables us to develop security strategies that permeate across your entire organisation, thereby empowering people to be proactively cyber secure over a long period.

Because of this, our Consultancy approach, unlike traditional consulting, is not grouped into security solutions that focus on mitigating specific risks. Instead, we consider the results of four key questions that organisations are, and should be, discussing internally around cyber security:

**How can we deploy cyber security to enable our business and our digital strategy?**

**How can we manage the cyber risk that we as people bring to our organisation?**

**How can we ensure that we are acting in a responsible and lawful manner?**

**How can we prepare for a crisis?**

Framing the solution in this manner is important because we fully understand that organisations, like countries, have different philosophies and priorities that need to be candidly addressed before discussions can begin about what the right cyber solution is. As such, we preface all our engagements with the four questions above as part of the Secgate triage discussion. This enables us to understand your priorities and tailor our Cyber Security Consultancy services to your specific requirements.

# EMPOWERING BUSINESS

## Enabling Your Business And Digital Strategy

To understand why cyber security is important and how it enables us all to achieve our business goals, we also need to consider why we value national security. When citizens are safe, so is their ability to freely pursue their goals and express their ideas to the rest of society. The safer the space, the greater the scope for the mass exchange of ideas and information.

At an organisational level, business enablement works much the same way: ensuring your employees are free to do their job or Business-As-Usual (BAU). This encompasses a lot of the provision of traditional cyber consulting services, for instance: providing network security so your employees can communicate and securely transfer data on mass or providing good governance, policies and standards so individuals understand what is - and isn't - responsible behaviour. Business enablement centres on providing robust cyber security controls to create an environment where employees can work efficiently whilst protecting your organisation from risk.

### Traditional consultancy shortfalls

We feel that this is where traditional cyber consultancy gives its focus, and in a lot of cases where it ends. The problem with this model is that grouping and procuring cyber services in this way leads to individuals requesting specific services for individual systems or processes that they are responsible for within your business, rather than providing services that protect your business as a whole.

For us, this is the equivalent of giving weapons to soldiers based on how loudly they shout for them, rather than how much danger they are in. This is a problem when it comes to thinking long term about your cyber security; it is a lot more expensive as a strategy to continually put out the fires that you can see, and are behind you, rather than dousing the ground ahead of you to prevent future breakouts.

### Cyber security goals

Long term, our aim is for your organisation to proactively own your cyber risk management and for good cyber practice to be integrated and aligned with your digital strategy. At its simplest, a digital strategy is a collection of technology focused projects which introduce a host of new technologies into the digital infrastructure of an organisation. However, all technology comes with cyber risk therefore integrating security at the outset of new IT projects will significantly reduce your organisation's accumulation of short and long term threats and associated costs. With the increasing complexity of technological networks, the earlier this process is established the better equipped your organisation will be to survive the future decades of unknowable cyber security advancements.

### Our approach

Our Cyber Security Consultancy: Empowering Business service starts with the implementation of IT security controls across an organisation that provides the base level protection needed for employees to do their jobs. These activities are prioritised through our triage approach: understanding where the most critical risks currently are within your organisation combined with a base alignment to international cyber security standards for example, ISO27001/NIST to secure employees in their BAU activities. This base level of security acts as a platform to start thinking strategically about how cyber security can enable your future business goals.

### Sustainable strategies

Our experienced consultants customise frameworks that align with specific project development life cycles to ensure that cyber security guidance is provided at the technical, operational and executive level, enabling a secure and sustainable digital strategy. When this framework is successfully incorporated into BAU, your reliance on external consultants and sources of information for cyber risk management will be heavily reduced long term, allowing you to own your cyber risk management.

### Proactive integration

There are many benefits for you to act proactively to integrate a cyber risk management strategy specific to your business requirements. You will reduce the risk of cyber attacks, enhance governance and be more attractive for others to trade with you. Our proactive integration approach ensures that your critical assets are protected from cyber risk – so you can focus on your core business.

SOLUTIONS

- Secure Software Development Lifecycle
- Third Party Security
- Cyber Security Strategy & Budget Planning
- Security Architecture
- Security by Design Principals

# COMPLIANCE

## Preparing Your Organisation To Act Lawfully And Responsibly

Our Cyber Security Consultancy: Compliance service considers current legislation responsibilities and focuses on the likelihood of future compliance requirements given the trends in the evolution of regulations surrounding privacy and cyber security governance. This context is important because legislation, at its core, is a documented aggregation of the moral preferences of citizens within a society and those preferences continually evolve.

We analyse the current trends and activist movements to prepare your organisation for future regulatory changes thereby avoiding unnecessary investment into static cyber security solutions that may become irrelevant. For example, in 2015 the US Safe Harbour agreement, the framework that legislated how data should be transferred between North America and the European Union (EU), was nullified. This was replaced by the US-EU Privacy Shield, which is aligned to General Data Protection Regulation (GDPR), however this also looks likely to be quashed. This is due to increasing vocal movements across continents that are fighting for more consumer rights in a world of data. These movements are transient however, so should your organisation's strategy in ensuring sustainable, long term compliance.

### Understanding your data with Secgate VisDa technology

Organisations need to have an accurate, real time understanding of exactly what types of data they process, where they are stored, who is responsible for them and how each piece of data is collected and utilised, at every single point in time. Once the baseline question of, 'What are we doing with data?' is answered, organisations can proactively answer the question 'What should we be doing with data?' Once you are empowered to continually answer the latter question, you can ensure compliance, regardless of changes in legislation.

Our flagship technology VisDa, provides the answer to the first question. Its' core technology maps out data flows across an organisation and provides, at a glance, a real time overview of what data is being utilised and where.

### Strategy creation

Our Cyber Security Consultancy: Compliance service then formalises the gap analysis and creates a strategy to achieve your desired level of compliance. We help you assign and train data controllers across your organisation how to answer these questions:

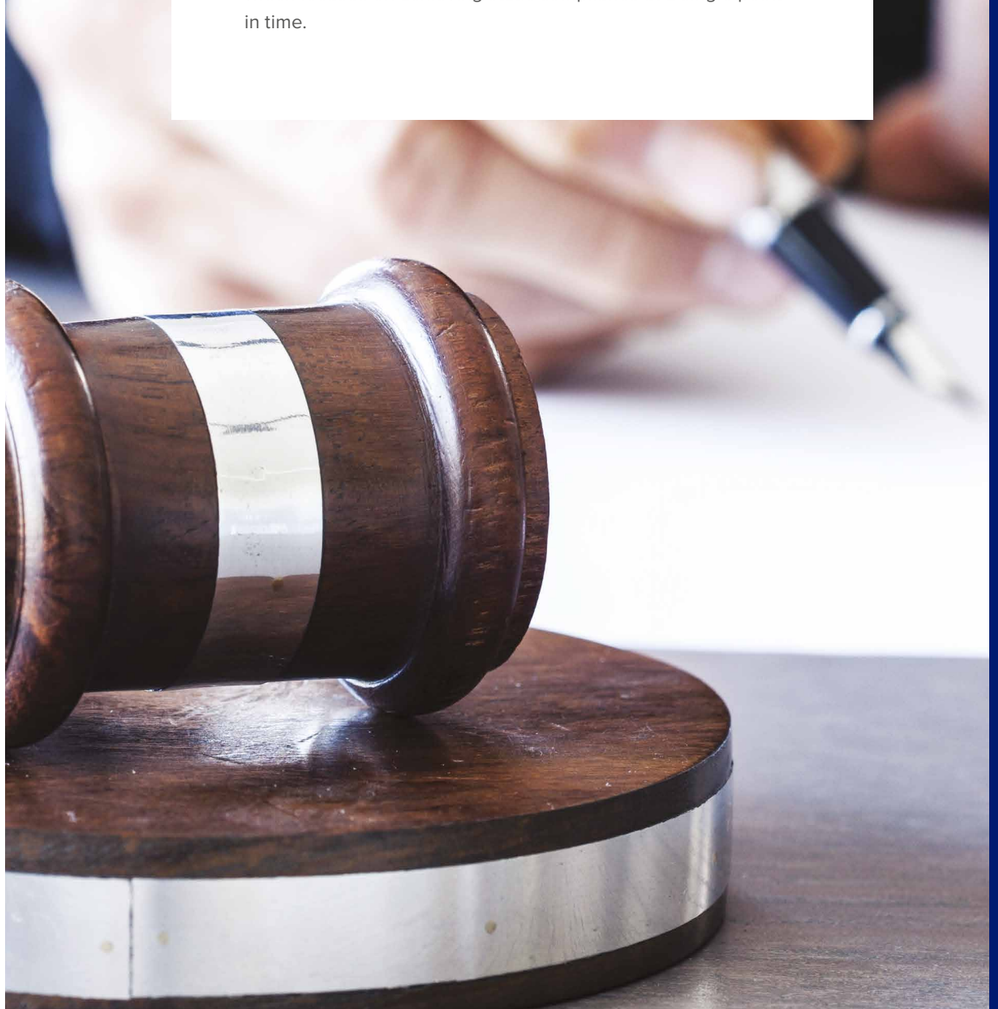
- Q. What data should we be collecting?
- Q. How should we be collecting it?
- Q. What purpose should we be using it?
- Q. How should we be protecting it?
- Q. How long should we be keeping it for?



### A sustainable, scalable solution for future compliance

Our consultants design business frameworks that integrate with your current processes and formalise the engagement of your Project Management Operations (PMO) and data controllers to receive appropriate authorisation for data usage at every single level. Similar to our Cyber Security Consultancy: Empowering Business service, for integrating cyber risk management into your digital strategy, our Compliance team integrates sustainable, scalable frameworks that allow you to continually answer the data questions above.

Our Cyber Security Consultancy: Compliance service is ideally positioned to enable your organisation to embed its own philosophy and ideals into its long term approach to regulation conformity, rather than the traditional consulting viewpoint which focuses on achieving static compliance at a single point in time.





General Data Protection Regulation (GDPR) Solutions

Payment Card Industry Data Security Standard (PCI DSS)

Data Classification & Governance

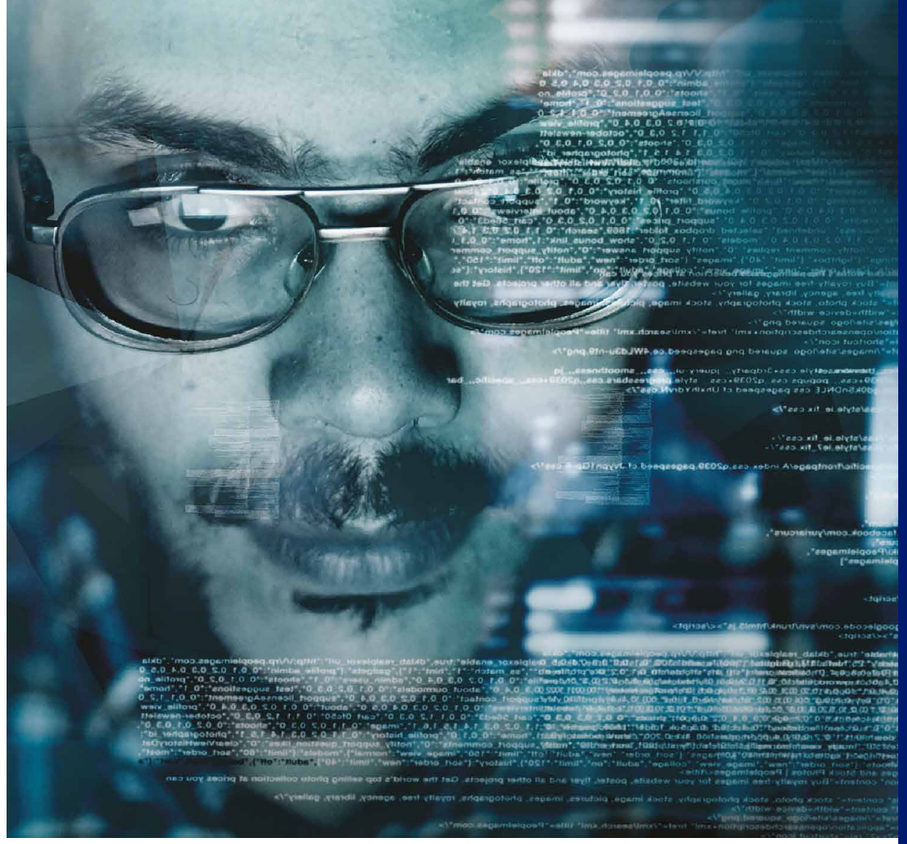
Information Security Management System ISO27001 Implementation & Audit

# FIRST RESPONDER

## Managing How To Effectively Deal With A Cyber Security Crisis

There is no such thing as being 100% secure therefore, in the case of a breach, it is paramount to have a streamlined and effective response mechanism that can limit the damage done to the organisation. Once again, this is a collective action problem and cannot just be left as the sole responsibility of your incident response team.

The best analogy here is to envisage your organisation like the British Isles in 1066 with the armada heading your way across the channel. There are three key parts to the defence:



### Detection

How far out do you see the attack coming and how quickly can the people who are manning the lighthouse understand the severity of the attack?

Similar to a cyber attack you need to possess the intelligence to understand the nature and severity of the breach that has occurred. This is what our technology Forest Tree provides.

In 2016, the median time taken to recognise that a cyber attack was occurring, or had happened, within an organisation was 200 days. Forest Tree's purpose is to drastically shorten that time so your resources can be mobilised as quickly as possible thereby mitigating the impact of the attack.

### Escalation

How quickly can you organise an effective response to the incoming attack?

In 1066, the speed with which information could travel from the coast to London and into the hands of war generals was critical to organising an effective response before an attack took place. This required a seamless understanding between the person in the lighthouse, who first discovered the attack, all operators of the 100 beacons and the people responsible for organising a response.

Our Cyber Security Consultancy: First Responder team designs incident response playbooks and trains individuals throughout your organisation to report and respond to indicators of cyber attacks in multiple scenarios. Once again, your employees are the best collective form of defence.

### Response

What are the generals' strategies when attacked by an enemy and what conditions trigger which options?

Good generals are pre-prepared with solid strategies. Our goal is to empower you as a leader to mitigate the impact a cyber breach has on your organisation as quickly and effectively as possible. The Cyber Security Consultancy: First Responder service provides unique strategies for you to be ready should a security breach occur. These are supported by incident response playbooks and simulation exercises providing real-life scenarios for decision makers and incident response teams to rehearse their response.

# EMPOWERING PEOPLE

## Equipping Your Employees To Defend Your Organisation

Our approach to human risk consultancy differs to traditional approaches. We believe that accidental and malicious employee cyber breaches such as the deliberate exfiltration of sensitive data, the accidental data loss from a wayward email, a lost laptop or a misunderstanding of confidentiality, are not individual risks. They do not warrant separate solutions; instead, they are symptoms of a corporate culture unaware of what constitutes very best cyber security practice.

Cyber security needs to be addressed as a collective action problem; it is the responsibility of every individual within your organisation. A typical organisation can have as few as 10 or as many as 100,000 employees all processing an exponentially increasing amount of sensitive data.

### First line of defence

So, similar to the fight against terrorism whilst it is important to have a strong first line of defence in the technical solutions used to prevent individual incidents occurring, good national defence is enabled by its citizens. It is vital that individuals remain vigilant within their organisation and corporate communities, and inform their cyber security teams when they feel that there are risks arising. Why is this important? The way a government thinks that a community operates and how it works are often two separate things. It is only when citizens are empowered to act, seek out and report malpractice that communities become safer places to live.

### Mobilising your employees

Our Cyber Security Consultancy: Empowering People service provides a focus on redesigning the cyber roles and responsibilities for all individuals within your organisation. Our aim is to create a culture that better enables you to carry out cyber risk mitigation and provides those individuals with the training and intelligence required to do so confidently. Giving your citizens the intelligence and resources to root out cyber risk can turn your employees into your most effective form of defence.



SOLUTIONS

- Strategy, Governance & Policy
- Reporting & Metrics Frameworks
- Education & Training
- Insider Threat Programmes
- Identity & Access Management
- Removable Media
- Data Loss Prevention

# TRAINING

# CYBER SECURITY TRAINING PROGRAMMES

## Enhancing Employee Knowledge And Skills

People are the biggest weakness to an organisation's security in the modern day; we have the training facilities and skills to change this.

Our training room has the technology to provide individuals with a laboratory environment to test their skills without working on live systems. Learning through diverse media types and hands-on practise is the best way to learn.

The Secgate cyber security team has created a leading-edge centre for cyber learning where analysts and engineers can improve their knowledge, hone their existing skills and develop new competencies. We offer a blended framework of e-learning, virtual classrooms and workshop based face-to-face training. Training is categorised into general security awareness, technical and advanced cyber security programmes.

Before starting, our team assesses your business security needs and then advises how you can maximise employee and department performance. We offer set and customised cyber security training programmes.

## Set Security Programmes

### Introduction to Information Security

Obtain essential knowledge about the risks, threats and vulnerabilities your organisation and specific industry will potentially occur.

### Staff Awareness Training

Defend against phishing, social engineering, weak passwords and other day-to-day IT security issues.

### Introduction to Penetration Testing

Learn the five phases of a penetration test and the methods an attacker will use to gain access to your network, assets and Intellectual Property Rights. This course is good for reviewing external testing companies and their methods.

### Penetration Testing - Module 1

Discover how to perform an end-to-end penetration test with the various tools available. This is a theory and practical hands-on course in a laboratory environment.

### Advanced Penetration Testing - Module 2

Gain advanced techniques to accessing a target network, maintaining entry and clearing tracks. This is a practical hands-on course.

### Social Engineering

Learn how the various types of social engineering are a huge threat to your organisation including targeting individuals via telephone, face-to-face and through social media channels. Are you aware that dumpster diving, eavesdropping and shoulder surfing still exist?

### ISO 27001

Obtain expert training in how to comply with the International Organisation for Standardisation (ISO) certification in information security management systems. Find out how this ISO standard can elevate your business above your competitors and demonstrate to your customers how seriously you take security.

### Secgate Phishing Platform

Learn how to educate and test your employees on identifying dangerous email attachments spoof emails. Use this platform to test and review the performance and focus on the areas and departments that require more training.

## Customised Cyber Security Training

We design training courses to meet specific business and industry needs. Our customised courses can cover phishing, vulnerability scanning, insider threat, forensics, threat intelligence, endpoint security, physical security  and much more.

## Regulatory Compliance Training

Learn all you need to know about the latest certifications and how to gain accreditation. Courses include:

### GDPR

Be prepared for the introduction of the EU General Data Protection Regulation in May 2018. This course applies to all businesses that hold EU citizens' personal and identifiable data.

### CEH

Our team will help you plan for the International Council of E-Commerce Consultants, known as the EC-Council, Certified Ethical Hacker examination. You will achieve an understanding and the knowledge in how to identify potential weaknesses in target systems thereby assessing any security vulnerabilities.

### Introduction to Penetration Testing

Learn how to achieve CREST membership, a not-for-profit organisation that validates cyber security companies' ability to provide a consistent standard of technical services including penetration testing.

# TECHNOLOGY

# COMPLETE PROTECTION

## Understanding The Engine Room

Whether you represent a business or government your network infrastructure, stored data, employees and customers are at risk from a cyber threat and as such, your future success relies on you being able to safely protect your assets. Cyber security threats are constantly evolving, increasing in number and becoming more sophisticated. It is therefore paramount that you have a strong, scalable risk management strategy in place supported by the top cyber crime identification, protection and mitigating technologies available. Cyber security consultancy services and technologies are business enablers. However it is when they are combined that you can achieve complete protection. Our technology solutions provide your organisation with all the information you need to manage your comprehensive cyber risk management strategy.

## Next Generation Technology

Our combined team of scientists and global specialists create technology solutions focused on providing innovative cyber security solutions for tomorrow's enterprises. Our research and development department works hand in hand with our engineering and development departments pushing the boundaries of science, technology and business to make the world a safer place.

Our mathematicians are pioneering and testing the most advanced machine learning algorithms that act as the nucleus to our next generation technology solutions. This will enable organisations to identify anomalies in their systems, and in doing so, businesses will be able to assess the risk within their organisation to cyber attacks and implement cyber security strategies and preventative measures accordingly. Our solutions give you full insight to your organisation and provides business leaders the transparency they need across your network, multiple departments and teams to be able to make informed security decisions.

# FOREST TREE

## Be Ready For The Inevitable

Have certainty over your digital infrastructure with Forest tree, a holistic, modern cyber security solution. Our unique approach enables a complete view over your organisation's behaviour, empowering you to make informed decisions and investigate even the most sophisticated threats.

### CAPTURE

Our core engine is highly scalable, reading network traffic from every device. It captures and decomposes the packets, analysing the contents for the most valuable information to store in real time. Unlike other solutions, Forest Tree can see inbound, outbound and cross-network traffic; it can even capture the VPN traffic of remote users. While firewalls might protect your endpoints, FT ensures you can see what is really happening inside the network, see if devices are scanning each other, thwart man-in-the middle attacks and understand how an infection might spread through the network.

### DISCOVERY

Forest Tree has a comprehensive set of filters and visualisation tools to let analysts get to the information they need, fast. It makes it easy to integrate and drill-down a large volume of traffic, see the connections over time and over geography, as well as a list of all the events.
You can also go back in time, see what happened last Tuesday or investigate a specific breach after the event.

### COLLABORATIVE INVESTIGATION

Forest Tree lets you collaborate on an investigation using Cases. A case is a place to store all of your notes and evidence around an existing investigation, operational issue or interesting events in the network. Everyone with a FT account can contribute to the case, adding evidence or notes. It can be assigned to a particular account to take ownership of any actions and be closed when the case is considered resolved. All of your sensitive network information stays inside the secure environment, limiting the opportunities for screenshots or copy-paste.

### API

It's your data, so it's yours to use. Our comprehensive API (Application Program Interface) is yours to use for integration into any number of existing solutions you might be using. So if you find you need something else, it's easy to build more of your applications on top. With built-in documentation and a sandbox environment, it's so easy for developers to learn. Best of all, Forest Tree uses GraphQL, a new type of API language. This means that you can be confident it will be compatible with past and future software.

## Forest Tree Capabilities

Forest Tree is designed to enable people to understand and explore their network traffic, enabling them to make informed decisions and investigate cyber security threats.

### Use it anywhere

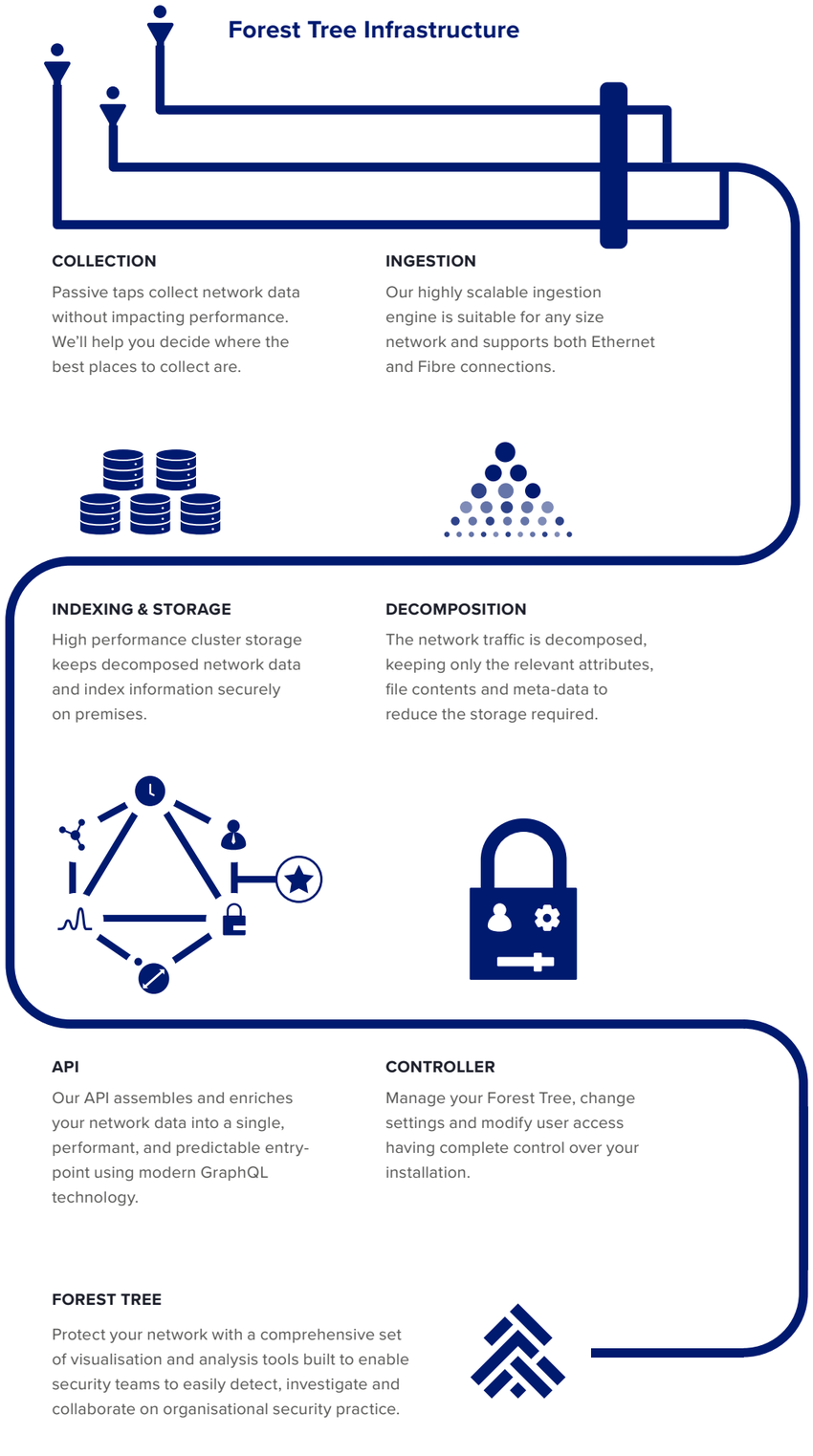
FT has been designed with the future of work in mind. We collaborated closely with industry to with industry, addressing the growing need  to be able to perform security operations from outside the SOC. FT works over your company's VPN. You can even run our capture appliance across multiple networks, offices or countries and access the information from the same client application. What's more, it is even available for your favourite operating system, whether you prefer Windows, Mac OS and Linux.

### Intuitive UI

We wanted to create something that would appeal to everyone, not just security analysts. Every element has a dedicated purpose and sports an aesthetic that helps communicate and simplify the often complex data. Our interface is optimised for a quality user experience. From an obsydian theme that is not only visually stunning on a HiDPI display but also helps reduce eyestrain, to carefully selected mono-space fonts avoiding aliasing for superior legibility of IP data.

### Performance

The entire architecture has been built around optimising the performance of analysing large data sets. We use comprehensive indexing to filter down millions of records in a matter of milliseconds, and only request the data that can fit in the application view. The Forest Tree API uses GraphQL to transport data between the server an application. It's incredibly efficient, only fetching the information it actually needs and caching queries for later. Most queries take under 1 second to analyse a dataset of millions of records.



## Forest Tree Use Cases

### Incident Response

Forest Tree is a perfect companion to assist in investigating an incident. With access to the historical network trafic, it's easy for an analyst to find the events they're looking for, inspect the traffic and re-create the series of events that unfolded, by creating a case. Collaborate and share across the whole team before taking action to prevent any furthur threat.

### Compliance & Governance

Whether you need  to meet GDPR or have your own internal governance, Forest Tree provides a quick way to really understand where your information is travelling. You can filter by country, IP addresses or services to quickly show where data is travelling in, out, and across your organisation's network. You can even look for particular types of traffic, including specific files sent or domains visited for an incredibly qualified and quantified view over the current and historical behavior.

### Network Operations

With a comprehensive set of network auditing tools, Forest Tree provides an in-depth analysis of network operations. You can find traffic patterns, unusual activity by users or even troubleshoot server connectivity.  Our solution enables organisations to optimise their network operations by having real insight into the activities and behaviours of users and devices.

### Threat Hunting

For any security operation it's essential to discover potential threats; Forest Tree provides numerous ways to discover potential vulnerabilities for exploit. Discover servers using older encryption, see client operating system versions and even find leaked credentials. Our intuitive application makes it easy to find connections that may be high risk to your organisation.

# THREAT INTELLIGENCE

# THREAT INTELLIGENCE

## Enhancing Employee Knowledge And Skills

### Our threat intelligence services cover both open and dark web channels to help you monitor threat within society and across the globe

Cyber security, as a risk management exercise, does not deal in absolutes. Effective risk management relies on a communal understanding of what is a reasonable, proportionate and/or legitimate course of action in a threat that an organisation faces.

By its nature, this process is highly contextual and subjective. A cyber security professional who is immersed in daily news reports of cyber breaches around the world, will have a different prioritisation of a cyber threat than a business executive whose role is far removed from the subject matter. When there is a conflict in the understanding of the risk of a cyber threat, it is difficult to effectively manage this as often a consensus on what is an appropriate response cannot be reached.

Threat Intelligence provides the context to a cyber risk and the potential impact your organisation faces if a threat manifests itself.

We present an objective overview of the information to all parties involved in your organisation to be used as a common platform for cyber risk management discussions. Good threat intelligence allows your business executives and technical leads to draw conclusions from the same set of information, discussed in a language that both parties can understand.

## Services include:

### Comprehensive threat intelligence helps you prioritise cyber security activities

Our Threat Intelligence technology searches open source information feeds which are publically available sources, as well as dark channels across the Internet. We monitor media at a global level in different markets and industries, plus investor relations, easily finding data which provides supporting evidence to anticipate a crisis. The information assists you to make the best choices and implement tangible changes while saving time and money. This service is underpinned by these core capabilities:

### Open Source Speech To Text Capability

Our Automatic Speech Recognition (ASR) technology converts spoken words into a sequence of written words across 80,000 media channels in 17 different languages. The advanced language model toolkit allows you to extend the vocabulary of the ASR system to not only recognise new words but to also catch words in specified pronunciations.

### Profiles And Ontology

Once large amounts of data are gathered, our intelligence agents are able to analyse and extract the useful information relating to your organisation. Our profiling and ontology feature enables you to do just that: extract hidden information from unstructured data, discover and understand relationships between diverse data and, subsequently, conduct complex analysis.

### Media Mining System

This is the core of our Threat Intelligence service. Our technology trawls the Internet and other information platforms to provide an analysis of current trends in the media and track changes in social opinion. The technology is fully customisable and can focus on areas most relevant to your business. At its base, it is an extensive, multi-lingual search across the Internet, TV, radio stations and other media platforms providing sentiment analysis and data projection across geographies and timescales. It also ranks the importance of influencers, such as journalists and social media bloggers, according to parameters including number of followers, depth of content and importance of channel.

Analysis of the data allows you access to invaluable information about the threat landscape which can inform your business decisions.

### Dark Web Capabilities

Our Dark Web intelligence mining tool is capable of analysing activity relevant to your organisation across all open Dark Web forums. Our threat intelligence agents are trained to target activity that is specifically relevant to your organisation. For example, monitoring for the elicit release of employee credentials, following threads and forums connected to planned attacks and providing ongoing updates on wider criminal cyber activity relevant to your industry.

The profile manager is a powerful tool enabling the enrichment of profiles without limitation. We create a tailored portfolio of threat intelligence which is practical to use thereby helping you to make informed cyber security and business strategy decisions.

Our Threat Intelligence service benefits you by:

### Improving your understanding of your threat landscape

Threat intelligence is at its most beneficial when analysed within the context of your organisation. We will help you to understand the specific threats to each of your assets, whether that be monetary, data, physical or human - this will better enable you to quantify cyber risk. This acts as the platform for formulating what an appropriate response and/or mitigation activity might look like.

### Alerting you to real time cyber risks

Our Threat Intelligence technology monitors threat activity in real time and alerts your organisation on risks relevant to it. Our service is designed to cover the full scope of the threat spectrum from individual hackers on dark forums discussing known vulnerabilities within your organisation, to known advancements in nation state cyber offensive capabilities that could be utilised against you.

### Enabling the correct response and shaping your cyber risk strategy

We provide a tailored insight into threat activity in open source and dark channels that is either explicitly engineered to attack your organisation or poses an indirect threat if utilised by motivated attackers. Our Threat Intelligence service enables the timely response and mitigation of threats that arise against your organisation and provides credible intelligence that can inform proportionate cyber security defence strategies long term.

### Mitigating the impact of security breaches

The dark web capabilities of our Threat Intelligence technology are used to inform organisations when sensitive information about them is posted and circulated in hidden forums for example, leaked email addresses and passwords, technical blueprints and salary information. To protect your organisation, our technology alerts you to quickly mitigate the impact of these breaches including changing passwords and co-ordinating media responses.

### Preparing your organisation against future cyber risks

Our wider Threat Intelligence technology monitors ongoing activity from known threat actors and attacks against competitors, or similar industries, to anticipate and prepare you for comparable attacks against your organisation. The goal is to keep you informed and up-to-date on the threats facing your business in a world where the cyber challenges change daily.

# GOVERNMENT SOLUTIONS

# WHITE WOLF

## A Command & Control Centre To Arm Against Cyber Threats

In today's society, information is power. As such, cyber criminals are becoming increasingly sophisticated in extracting valuable data from government organisations and within public sector institutions. The true cost of a government cyber security breach is far greater than monetary loss: sensitive data has political ramifications, international legal implications and, could possibly lead to instigating a war.

Developed and developing nation governments need to be fully equipped to combat cyber crime. All countries need to have a cyber risk management strategy, effective law enforcement and technology resources in place. To facilitate this, our Government Solutions security team has developed an end-to-end cyber security programme called White Wolf.  Our solution is designed for nation states with one clear objective: to protect and defend countries from the threat of cyber damage.

White Wolf serves as a central location where a diverse set of capabilities and technologies come together to provide an ultimate cyber defence solution. We utilise the latest cyber defence technologies, processes, incident response, penetration testing, digital forensics and training coupled with some of the best minds in the fields of defence, monitoring, central intelligence and cyber security. This enables us to provide a comprehensive and unique service ensuring that you, as a leader in your nation, fully address the growing problems of cyber crime affecting your country.

White Wolf enables your government to prepare for the threat of cyber crimes by providing:

### A nucleus to capture and analyse all cyber activity

As a command and control unit, a SOC is the focal point for safeguarding against cyber related incidents, monitoring security and protecting government network assets and endpoints. The White Wolf Next Generation SOC provides situational awareness and continuous surveillance, including monitoring traffic, blocking unwanted traffic and detecting any type of attack.

### Fast, informed incident response

White Wolf's CERT strives to make the Internet a safer, stronger platform for all nation citizens. It achieves this by responding to major incidents, analysing threats and exchanging critical cyber security information with trusted partners around the world.

### Digital forensic experts

Governments need skilled personnel to perform media exploitation and recover key intelligence available on adversary systems. To help solve these challenges, we provide digital forensic professionals and work with cyber crime law enforcement agents to piece together a comprehensive account of what happened.

### Testing methods to identify and overcome security weaknesses

To test how secure your government systems are, our cyber security experts apply attack techniques to detect security vulnerabilities, analyse risk implication and write modern exploits. Following rigorous penetration testing, we then recommend mitigations before the system weaknesses are exploited by real world attackers.

### Advanced training to improve knowledge and skills

We have created a leading-edge training centre for customised cyber learning for your analysts and engineers to improve their cyber security knowledge and develop new skills. Our training programme provides a blended framework of e-learning, virtual classrooms and workshop based face-to-face training. We categorise training into general security awareness, technical and advanced cyber training programmes.

### Experienced strategic advice

The White Wolf SOC is the nucleus to your country's security. Our experts work closely together with you to advise how best to design, implement and execute your cyber security strategies and concerns. Our experience covers strategic cyber security advice across an entire nation, nationwide infrastructure, public utilities or more specific to a certain bank or government agency.

## BRITISH ENGINEERED

Science and technology in the UK has a long history: many important figures and developments in the field have produced life changing innovations. Major theorists from the UK include Isaac Newton, whose laws of motion and illumination of gravity have been a keystone of modern science, and Charles Darwin whose theory of evolution by natural selection was fundamental to the development of modern biology. Major scientific discoveries include hydrogen by Henry Cavendish, penicillin by Alexander Fleming, and the structure of DNA, by Francis Crick and others. Major engineering projects and applications pursued by people from the UK include the steam locomotive developed by Richard Trevithick and Andrew Vivian, the jet engine by Frank Whittle and the World Wide Web by Tim Berners-Lee.

Today, the UK continues to play a pivotal role in the development of science and technology within major industrial sectors including aerospace, motor, pharmaceutical and IT, plus cyber defence technology products.

Our solutions are drawn from specialists in the fields of defence, monitoring, central intelligence and the private sector. We have built strong links with British academia to harness the best minds in the country. We partner with the top universities in the country and work with Machine Learning and Cyber faculties to support the development of our unique technology.

White Wolf produces state-of-the-art cyber defence using British made technology and regional knowledge how to defend countries throughout the globe from cyber attacks.

# CYBER INTELLIGENCE COMMUNITY

# CYBER INTELLIGENCE COMMUNITY: CYBER WORLD

## Facilitating Cyber Security Debate

Cyber World is a digital media publishing and news platform, bringing our readers the latest news, analysis and insights from the world of cyber security. We publish Cyber World monthly in the United Kingdom with the aim of contributing thought leadership debate in rapidly changing IT and international security environments.

### A central platform for cyber security debate

To respond to challenges emanating from an escalating threat environment and to harness new opportunities provided by today's technological innovations, we recognise the need for closer cooperation between industry, academia and government. Bringing the three sectors closer together in our Cyber World magazine broadens and enhances the discussion on cyber security, making the subject more accessible to non-technical business and government audiences.

### Expert content for all business responsibilities and sectors

In Cyber World, you will find the latest cyber risk industry news, developments, trends, analyses and expert opinons from security professionals across the globe. No matter what role you fulfil in your organisation there is expert content tailored to you. Business leaders will benefit from learning about legislation changes, compliance requirements, technology solutions tailored to different industries and compliance considerations. For cyber security technologists, we provide technical articles and whitepapers discussing issues and trends including coding, algorithms, devices, frameworks and cryptography.

To support upcoming cyber security professionals, we include in-depth interviews with rising industry stars, competitions for graduate students plus winning submissions in the 'Future Leaders' section.

### Informed intelligence to your boardroom

The information can be used as a springboard in your organisation to bring a cyber security discussion to your boardroom and to a largely non-technical business and government audience. Our content covers cyber security issues which affect us all – across different industry sectors, job responsibilities and countries – and therefore can be used as a strong basis for an informed dialogue about your own cyber risk management strategy.



## A wide and strong voice

Cyber World's voice is heard by industry leaders and professionals across the globe whose lives may simply touch on or are submerged in cyber security. Individuals who participate in our Cyber World platform include:

- Government stakeholders
- The next generation of cyber security experts (graduate students)
- Academia
- 50,000+ professionals from the cyber security industry and other sectors including media, policy and international affairs
- 1,000+ CISOs, CSOs, directors and other industry leaders with a focus on board-level, business or those working in cyber security




E. info@secgate.com
W. secgate.com
A. 160 Fleet Street, London EC4A 2DQ