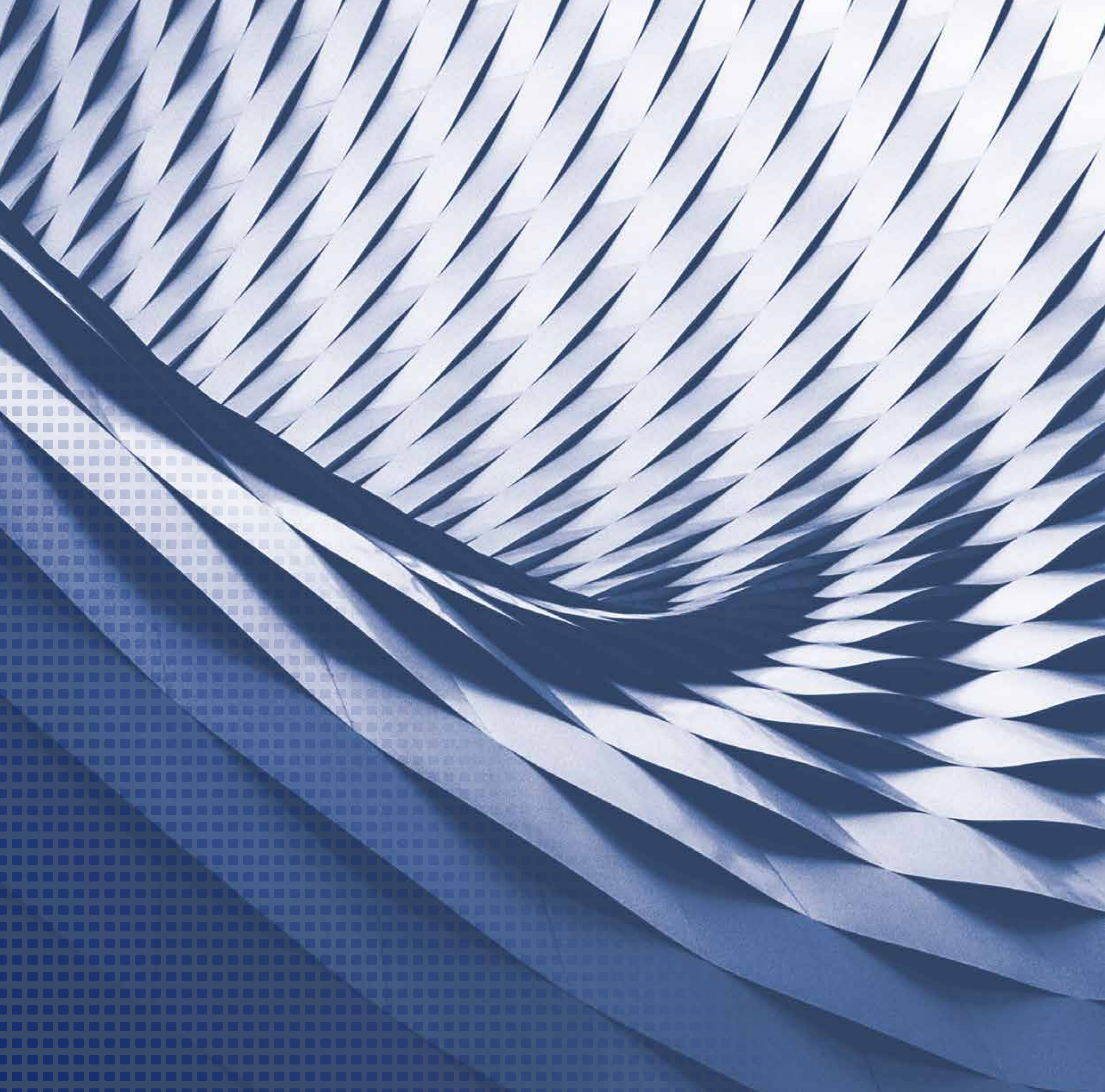
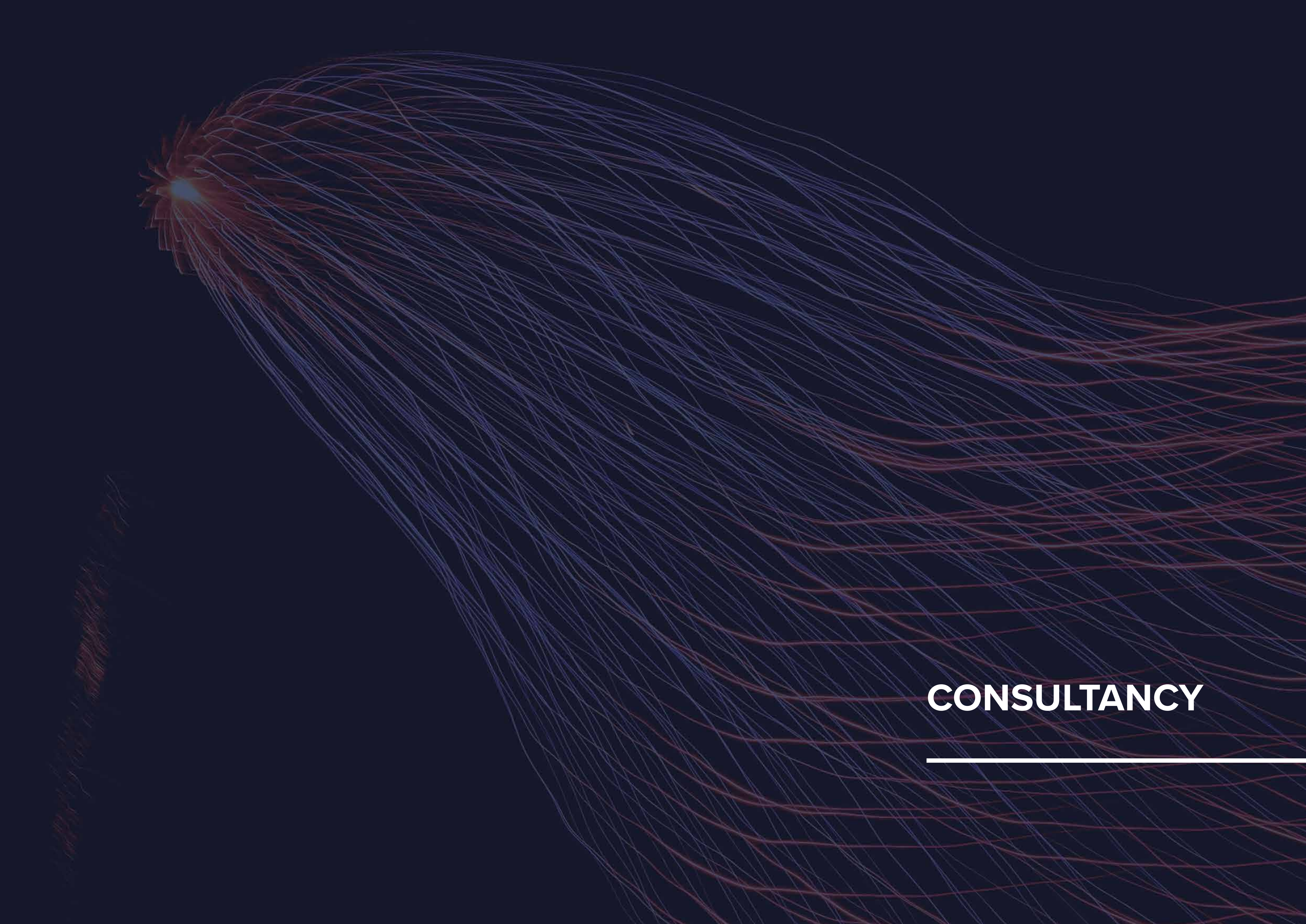


SECURITY THROUGH INNOVATION

Secgate



CONSULTANCY

CYBER SECURITY CONSULTANCY

Protecting And Empowering Your Business

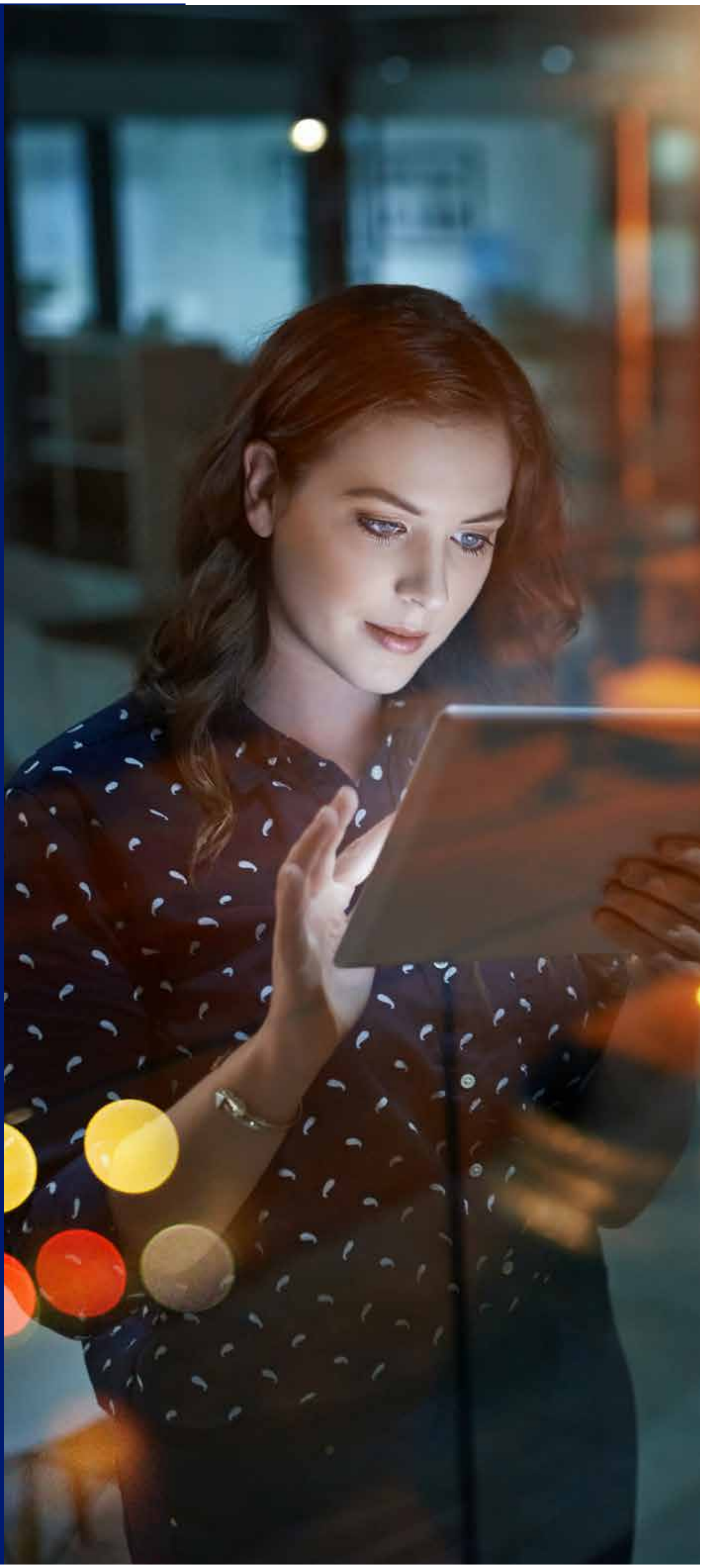
At Secgate, we care about protecting institutions, organisations and consumers from rapidly increasing cyber threats. We are united in our concern for the rising disparity between the capabilities of today's cyber attacks and organisations' cyber defence capabilities. This widening gap potentially exposes 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

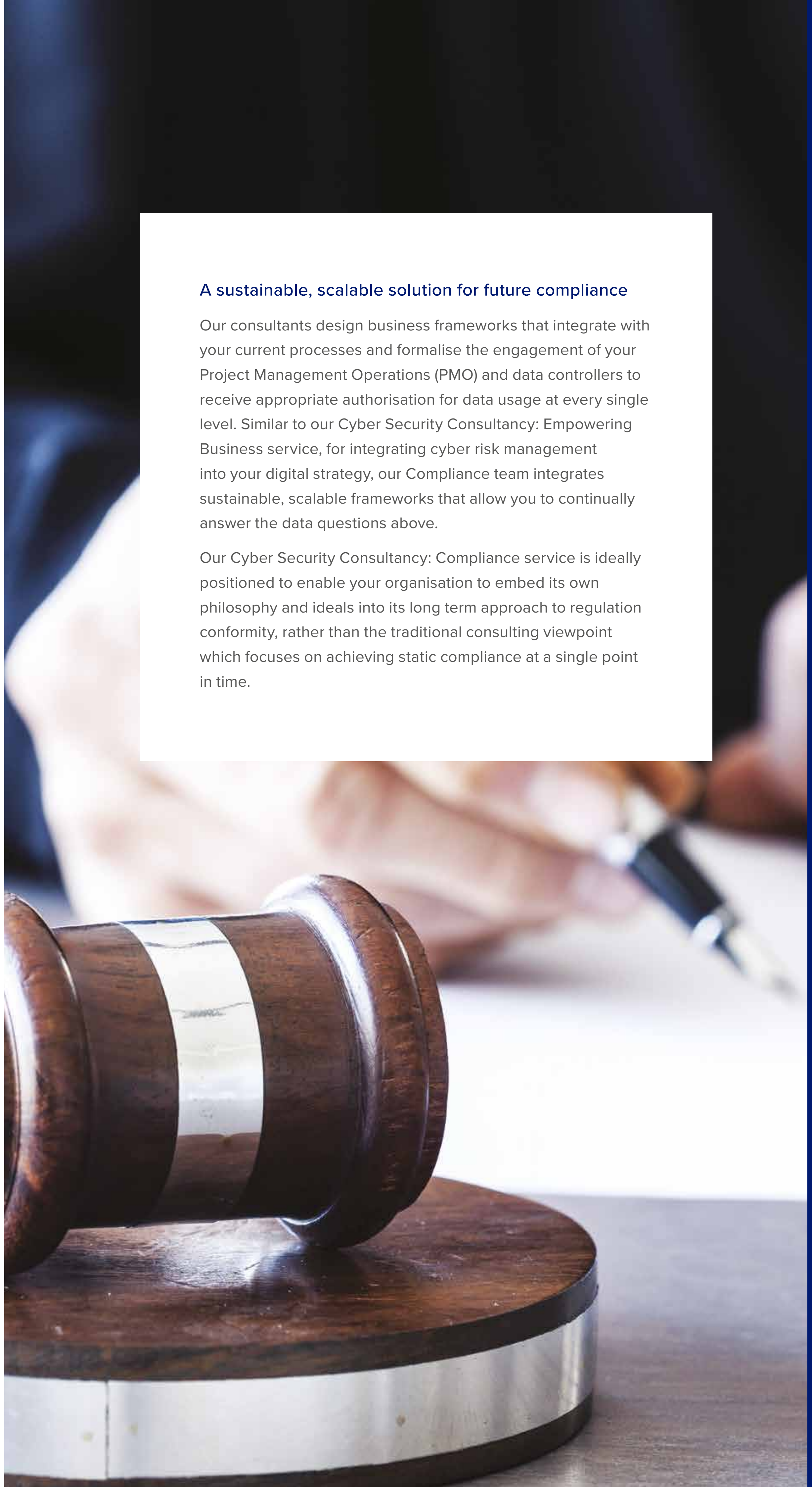
Organisations need to have an accurate, real time understanding of exactly what types of data they process, where they are stored, who is responsible for them and how each piece of data is collected and utilised, at every single point in time. Once the baseline question of, 'What are we doing with data?' 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.

SOLUTIONS

General Data Protection Regulation (GDPR) Solutions

Payment Card Industry Data Security Standard (PCI DSS)

Data Classification & Governance

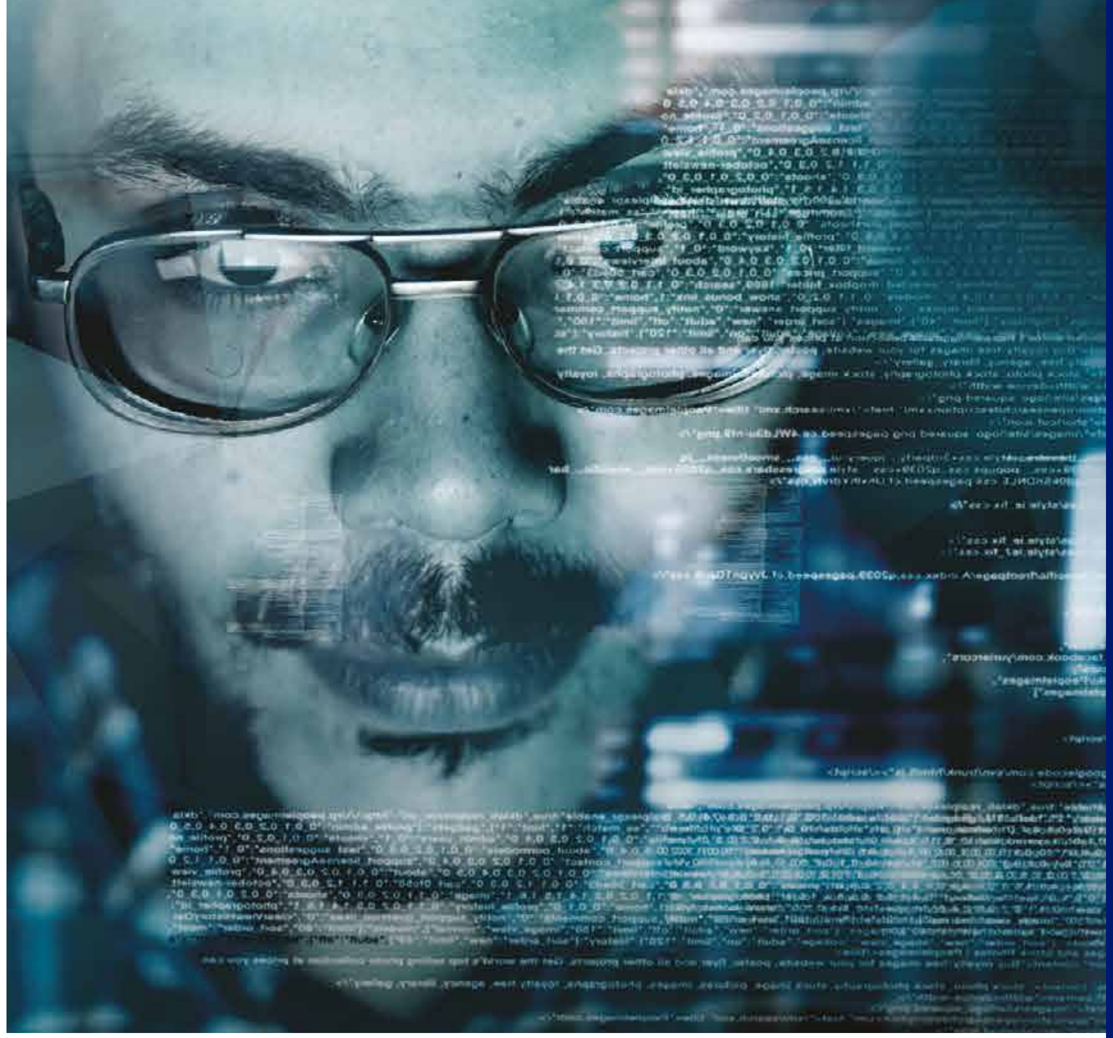
Information Security Management System ISO27001 Implementation & Audit

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.

SOLUTIONS

Incident Simulation Exercises

PR and Media Training

Cyber Incident Response

Business Continuity Planning

Penetration Testing

Network Scanning

Malware Detection

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

Secgate

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