CORPORATES

VALUABLE. INSPIRED. CONNECTED

+44 (0) 2081 239 463 | hello@cybersecuritycapital | cybersecuritycapital.com

Proud to serve the industry

+44 (0) 2081 239 463 | hello@cybersecuritycapital | cybersecuritycapital.com

People, process and technology are the foundations for all cyber security initiatives.

We live in an age where organisations are locked in an arms race with professional cybercrime gangs and state sponsored attackers. Being intent on fraud, extortion or theft of your information assets, each operates as ruthless and efficient entrepreneurs with business plans, extensive resources and the support of a highly developed and rapidly evolving black market.

However, the ability to counter attacks and protect an organisation successfully remains with organisations, providing they can integrate three critical elements - people, processes and technology into their strategy and wrap vision, resources, culture, incentives and action plans around them. If any one is missing confusion, anxiety, frustration, or slow or little progress will prevail.

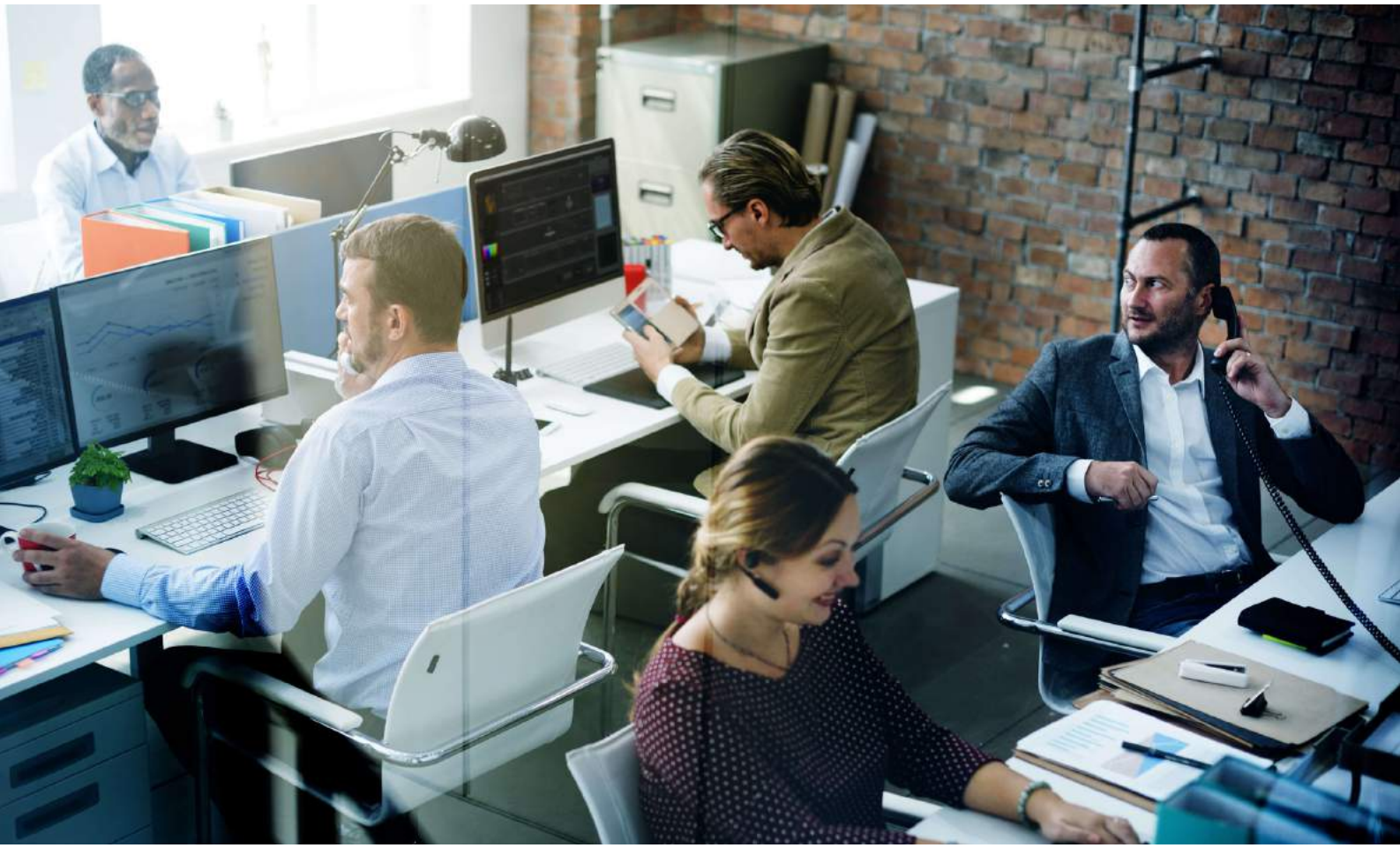
Take people. When assets were physical things, shareholders owned them, but nowadays the vital assets are people and they cannot be owned. To protect its assets, the best an organisation can do is to create an environment that makes its people want to stay and perform to the best of their ability. As a cyber security leader, a strong people strategy is, therefore, vital. You need to ensure that each team member has the appropriate knowledge, skills and competencies so they can communicate with all of the stakeholders and achieve win-win scenarios.

You also need to ensure that they can work together seamlessly, adapt to rapid changes in a technology environment and deal with pressure when stressful events occur.

Looking to process next, this can be defined as a series of actions or steps taken in order to achieve a particular end. By creating effective processes you can maximise efficiencies, create order, accountability and reduce risk. However, you must ensure that they're considered against shared organisational goals and your department's objectives. Furthermore, that they're viewed holistically so that one changed process doesn't create an issue for another area.

Finally, technology is all about deploying effective tools and systems that make the business secure and efficient. It's imperative that technology is only ever selected after the people and process issues have been solved, and that a comprehensive evaluation of the needs of all stakeholders involved has taken place. Only then can you be sure that the new technology is a good fit, has the scalability required to support the organisation's needs over the long-term and as it grows in complexity.

At Cyber Security Capital we can help you with all of these critical elements. We've a plethora of solutions for you to choose from and pride ourselves on being flexible, responsive and quality driven. What's important to us is that we're aligned in accordance with values and that we deliver beyond your expectations so we maintain an enjoyable long-term relationship and repeat business.



People are your greatest assets and when an organisation is at the top of its game you can be assured of one thing - it invests in its people.

Whilst others assume that good recruitment is sufficient for performance and business growth, savvy leaders know better. They know that if they're to succeed in building an optimal cyber security team then they've got to do more to attract, develop and retain the best talent.

They also understand that whilst experience, computer science degrees and certifications are useful gauges for new hires, they're not always necessary for all roles. At Cyber Security Capital we understand this and can help you find and retain your best talent, in line with your diversity goals.

People

In a job market where cyber security talent is in short supply, particularly women, and human capital is becoming an increasing focus for the Board of Directors, cyber security leaders know that they now need to pay close attention to their working environment, incentives and professional development.

They also know that the strength of a cyber security team comes from the diversity of its collective talents that originate from the unique experiences and technical expertise of its individuals spread across multiple demographic groups. The skills that are therefore required are aptitude, attitude and cultural fit, plus effective communication skills and business acumen.

At Cyber Security Capital, we understand this and that's why we focus on gender diversity, capability and engagement. This combination makes us unique in our market as we consider your cyber security team's journey holistically. We address the whole process from new recruits starting out to those in leadership positions. We believe this is essential for peak performance and to maintain a robust security posture.

With technology moving at speed we know the only way you can meet your objectives and outperform the competition is by staying abreast of human capital advancements and having regular access to a variety of learning programmes.

Our learning programmes are modern, diverse and flexible. They're available as classroom lead, or self-paced, online. They can be delivered as complete learning and development programmes or as individual components.

Through our value added support forum, we're available to answers questions long after your training has finished, which improves success rates as the team is fully supported. We offer consulting, coaching and an extensive range of soft skills training programmes:

- Defining, identifying & developing cyber security talent
- Talent mapping & management
- Individual team assessments
- Coaching for professionals with a military background
- Leadership
- Communication
- Team building & performance
- Time management
- Change management
- Conflict resolution
- Resilience
- Emotional intelligence
- Selling to stakeholders
- Negotiation
- Influence
- Personal branding

Strategy requires effective processes. Without them it's little more than a wish list.

As a cyber security leader you're responsible for securing your organisation's assets. Your team is also responsible for they need to know what the assets are, where they reside, how they rest and move, who has access and why. In order to do this they need processes to follow and the ability to create new procedures and policies, as the environment changes and the threat landscape evolves.

At Cyber Security Capital we can help you address these challenges. We can assess existing processes and policies, making recommendations, or creating new ones.

Processes

Processes underpin good management. When managed effectively they ensure that the cyber security team follows an informed and consistent approach that's in line with the organisation's operations. When not followed the results can be catastrophic.

Many top cyber security teams are busy working their way through major changes to their ingrained processes so they can keep abreast of the ever-changing threat environment and technology-driven business initiatives. They're developing a deep understanding of business processes too and working much more closely with the business units.

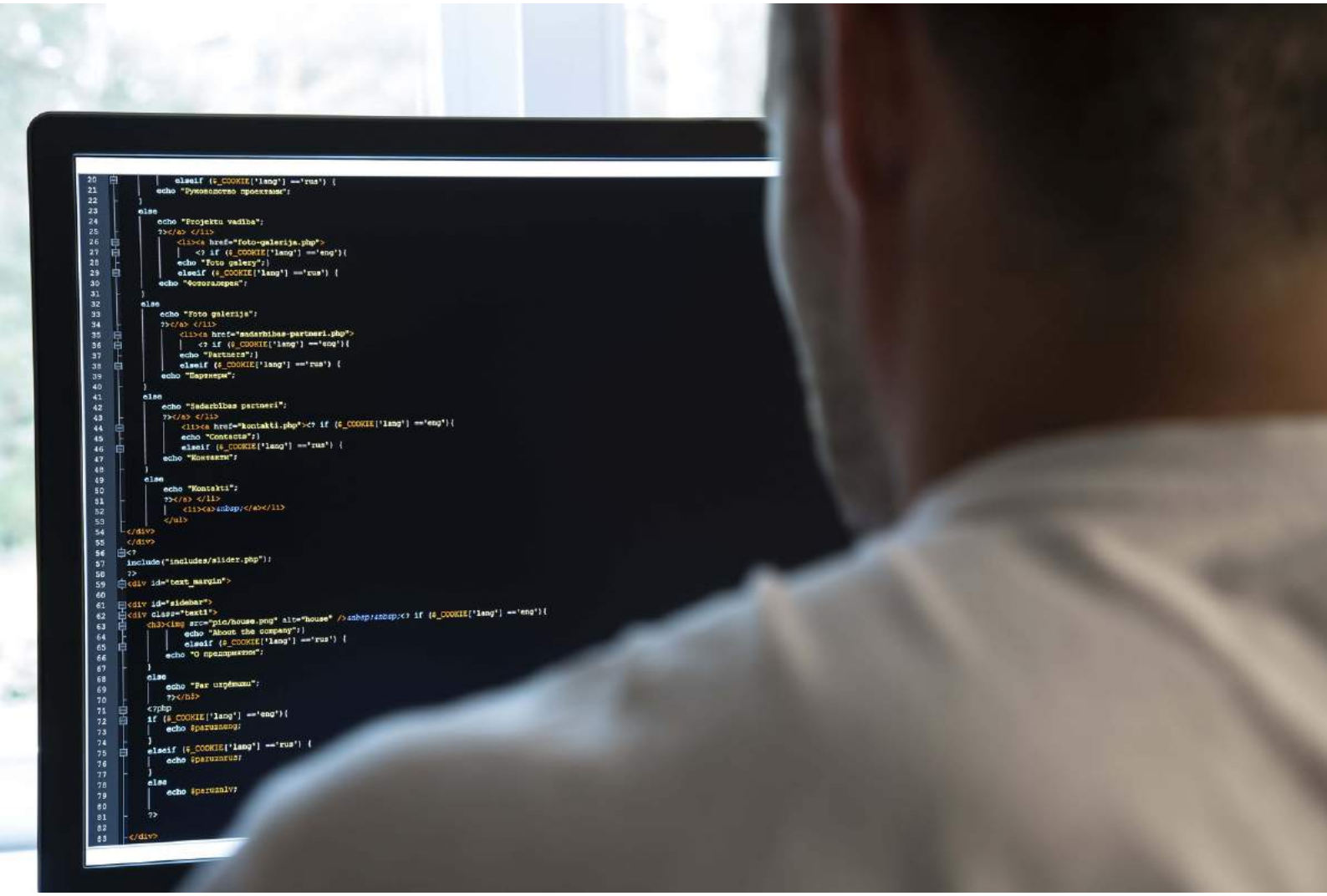
As cyber security risks are now one of the Boards main priorities, many business units and stakeholders are willing to play ball with the cyber security department and release budget in order to secure their systems and mitigate their liabilities. They're interested in understanding their risks and with such collaboration, cyber security processes are finally becoming integral throughout the organisation.

As cyber security processes are re-engineered, optimisation is a key success factor – and an on-going endeavour. As a result cyber security processes are having to be continually re-evaluated to ensure the effective use of resources and the effective mitigation of the risk to the business.

As the cyber security team considers how to renew these processes they're also having to keep up with shifts in technology for new technologies – particularly cloud or those analysing big data – are driving some key process changes.

Cyber Security Capital can help review, revise or write processes for the following areas:

- Risk measurement
- Business engagements
- Controls assessment
- Application assessment
- Third party assessment
- Secure development
- Threat intelligence & detection
- Incident response
- Crisis management



The growing engine of change is technology.

As a senior leader in cyber security it's your job to support the technology and either mitigate the risks that arise from implementation or ensure that the business stakeholders understand the consequences. To do this you need to be able to rely on trusted consultants, who can advise you independently.

At Cyber Security Capital, we provide this facility. Our world-class consultants are highly certified and have spent a lifetime in the industry working for corporations and major consultancies. They are readily accessible for all of your needs.

Technology

In today's global economy, organisations are hugely dependent on technology to build their products and services. Whilst rapidly changing, highly competitive, and in some cases volatile, technology can help increase an organisation's business performance by enhancing the delivery of products or services, at cost-effective prices, and in line with the organisation's agreed timescales and quality strategy.

As a cyber security leader your challenge is to ensure that you can secure the organisation, as threats increase daily and adversaries become more proficient. To do this you need assurance that technologies, processes and even the people who work for your organisation are not leaving you unduly exposed and vulnerable to attack.

With a multitude of cyber security vendors available selection is tough. However, when you understand your organisation's business motives, and where the security gaps are in your environment, you can determine which technologies may be suitable, whether they fit within your budget and the time-scales for implementation.

Cyber Security Capital can help you with all of this. For example, we can compile or review your use cases and success criteria, choose your vendor short list, support you during the proof of concept implementation and negotiate on pricing and Service Level Agreements.

We're passionate about cyber security technologies but only when they're innovative, scalable, easy to use and drive down costs. With an extensive global network that attracts many internationals, we're meticulous when we select our vendor partners. We assess not only the technology but the leadership team for competency, viability and culture fit.

Our vendor partners are hugely valued and our highly certified and experienced consultants can offer independent advice on the following technologies:

- Cloud
- Mobile
- End point
- Identity
- Infrastructure
- Application
- Data

How are we different?

Access world-class consultants and resources that support the global ecosystem

We offer a global community of like-minded, vetted cyber security consultants and partners, who are at the peak of their profession and readily accessible for all of your cyber security needs. Wherever you are in the cyber security ecosystem - a professional, a leader or an entrepreneur, we can help. You use our vault of resources or tap into our remarkable pool of expertise to build genuine connections so you can collaborate on projects, exchange thoughts and best practice learnings.

A partner who shares an aligned vision including giving back

We see a world where we are winning the war against cybercrime, where diversity is balanced within cyber security and where there is an abundance of top talent that is on-boarded through attitude and thinking capability. Our mission, therefore, is to empower and train you to thrive and solve meaningful problems so you become better, stronger and faster at thwarting every form of cyber attack and more resilient in the workplace.

In addition to speeding up learning, problem solving and accelerating success, we aim to inspire more of our clients and partners to support the UN Global Goals through giving and innovation. Our vision is that our clients measure their success based on their ability to positively impact the world.

Increase insight, knowledge and innovation so you remain ahead

We provide a range of services from securing systems to learning and development programmes, as part of our on-going commitment to supporting the success of cyber security professionals worldwide. Successful projects to us always mean accelerating learning, sparking creativity, inspiring performance and connecting you to new talent and collaborators who can help you achieve your career ambitions.

Responsive and flexible ways of working

Through our profound knowledge of the cyber security ecosystem we have devised effective strategic and tactical services, which help you to solve complex, diverse challenges quickly, to budget and around the clock. We pride ourselves on our ability to be responsive, flexible and to make every interaction a positive experience.

Consistent quality and long-term partners

You can be assured of consistent quality as we work to structured methodologies. Furthermore, each project we undertake undergoes a formal quality review, which maintains our reputation as outstanding, consistent and long-term cyber security service providers.

Our goal is to strengthen cyber space by empowering and mobilising a diverse, optimised cyber security workforce.

We see a world where we are winning the war against cybercrime, where diversity is balanced within cyber security and where there is an abundance of top talent. We want to empower and train more cyber security professionals and leaders to thrive and solve meaningful problems. We want to see better, stronger and faster solutions to cybercrime and other forms of attack. We believe that by having a diverse workforce we will benefit from diversity of thinking and that this will improve our ability to safeguard businesses, individuals and countries. Cyber security is a varied profession and there is a huge need for cyber security expertise. We want to lead the way for all diversity and be part of a movement that identifies, develops and retains talent regardless of biased discrimination.

Take the next step.

- Contact us.
- Meet to define the expectations and agree the scope.
- Receive a proposal and terms.
- Accept terms and agree start date.
- Commence project.
- Meet for project debrief.

Contact

To discuss our services, please email:
Jane Frankland at hello@jane-frankland.com
Cyber Security Capital (CS^)
http://cybersecuritycapital.com
Company Number: 7634264

Cyber Security Capital

Cyber Security Capital has a mission to help the cyber security industry to become better at fighting cybercrime and to empower, train and mobilise a gender diverse cyber security workforce. It was founded by Jane Frankland when she witnessed a changing workplace, a dire need for improved connection and access to resources, particularly amongst cyber security women, leaders and entrepreneurs. As a result, we offer a variety of solutions for cyber security entrepreneurs, leaders and professionals that are based around people, processes and technology.

We operate on a global basis and whilst most of our clients include some of the world's best-known brands, many of whom are listed on the global stock indices, we also have a selection of start-up and mid-range organisations. All of our clients, no matter their size share commonalities: they are aspirational, operate in a state of readiness and see opportunities when others don't. They take measured risks, act fast and want what's current. Their decisions are based on instinct, insight and what works. They tell us that the reason they choose us over others is because they know that in order to be ready, they need to rely on a team of experts who can demonstrate up-to-date subject matter knowledge, experience through implementation and foresight.

Service Divisions

- Individuals
- Corporates
- Entrepreneurs

+44 (0) 2081 239 463 | hello@cybersecuritycapital | cybersecuritycapital.com