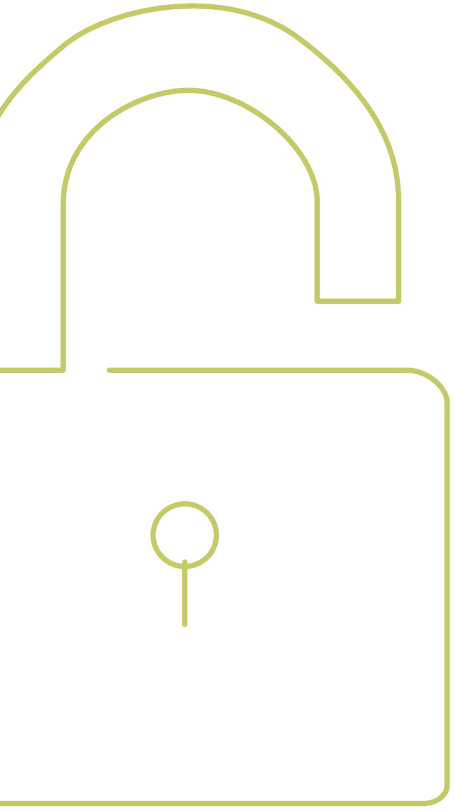
Capgemini Consulting

Address C-level Cybersecurity issues to enable and secure Digital transformation

We support cybersecurity transformations with assessments, diagnosis and audits of your organization, the protection mechanisms you have implemented and your security supervision capabilities related to sensitive data, critical infrastructures and digital transformation. This enables you to define your cyber security strategy and transformation roadmap.

Understand your position and **increase your AWARENESS** of **CYBERSECURITY**



Understand your position and increase your awareness of cybersecurity

As Digital Transformation initiatives gain pace across the world, the threat of cyber attack grows in tandem. Further risks stem from the evolving business and regulatory requirements and technology trends that are posing new cybersecurity challenges and endangering the success of digital programs.

In this landscape, while cyber criminals have matured and professionalized, Social, Mobility, Analytics, Cloud and Internet of Things (SMACT) technologies make today's digital enterprise increasingly vulnerable. The criminals are quick to exploit this.

The cost – both financially and in reputational damage – is huge. Estimates suggest the annual cost of cybersecurity attacks is anything from $375 billion to $575 billion. Add to this the once loyal customers who take their business elsewhere following a security breach, reduced competitive advantage, fines, and loss of business due to system downtime, and it's clear why mitigating the threat of cyber attack is a strategic priority.

Indeed, cybersecurity is a broad concern strongly linked to trust, innovation, competitiveness and business growth. Safeguarding customer data, research and development findings, intellectual property, business development documentation, and other critical information assets must be addressed in the context of Digital Transformation. For example it should embrace Cloud and Mobile computing, as well as Big Data, IT, Operational Technology (OT) and Internet of Things (IoT).

Business leaders in both strategic and operational roles must answer vital questions. How do you know if your business is resilient enough? Are you compliant with privacy and security regulations and corporate policy? Is it possible to combine digital transformation with acceptable risks, and how secure are your websites, IT infrastructures, applications and data?

Capgemini Consulting help to answer these questions with insight into enterprise security positions. This informs strategies for successful cybersecurity. The more you know about your real situation (vulnerabilities and security controls), the more you can strengthen your organization with effective solutions and procedures for governance, risk and compliance (GRC).

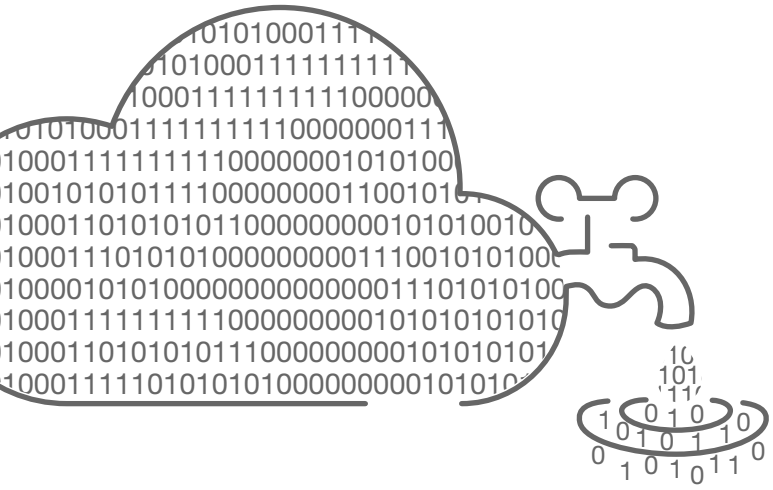
The **CYBERSECURITY** challenges

The cybersecurity challenges

Cyber threats (sabotage, fraud, theft, etc.) and regulatory requirements (personal data protection, critical infrastructures resilience, breach / leak notification, etc.) are an escalating global concern. This raises a number of issues for the modern digital enterprise, including the following four challenges:

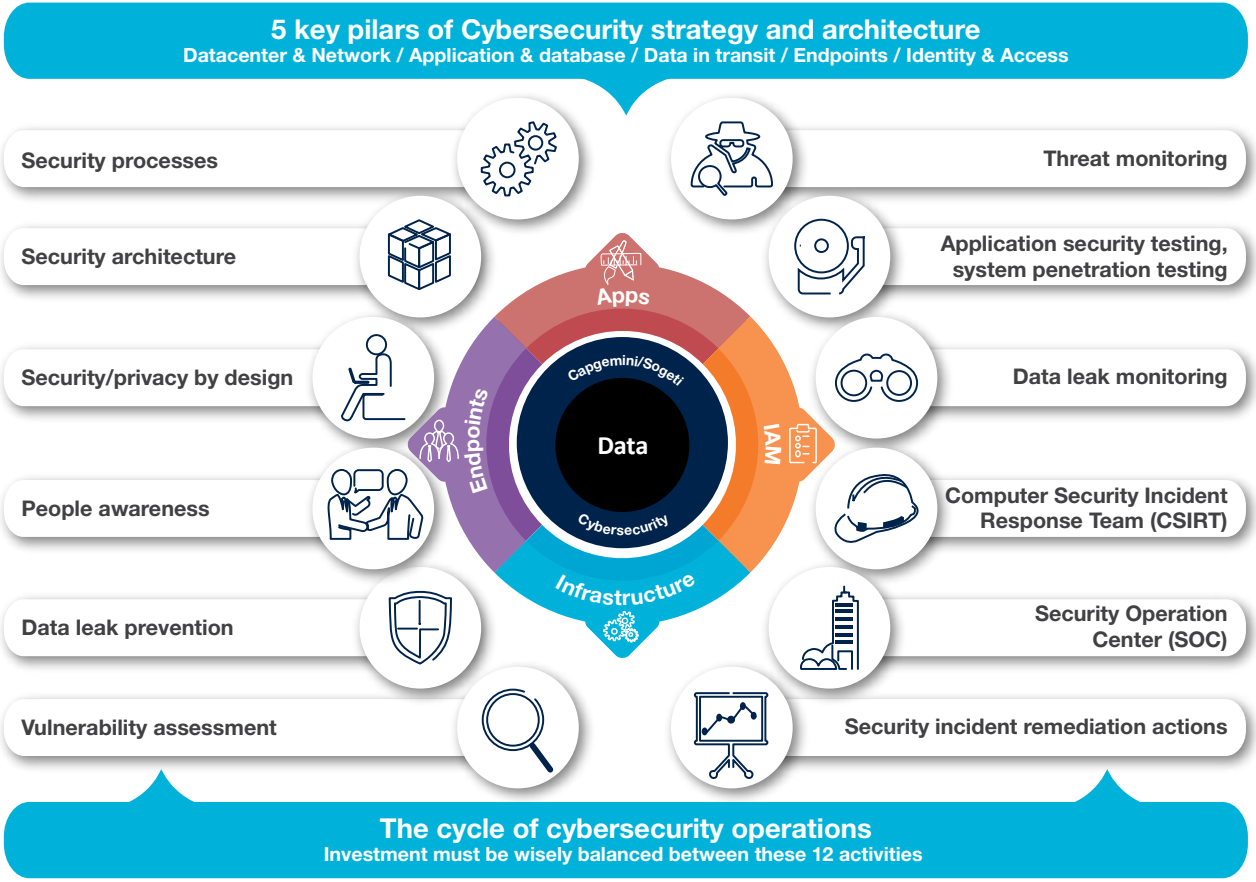
- **How to evolve the traditional security model so that there is a focus on data, people and risks.** This demands a rebalancing of security protection from 'network centric' to 'data centric' in the fight against data leaks linked to digitization, as well as solutions adapted to anticipate unknown risks.
- **Where best to invest now that security operations no longer rely solely on IT protection.** Investment must be balanced between a cycle of cybersecurity activities comprising: anticipation > prevention > protection > detection > reaction (as depicted here).
- **How to align the new cybersecurity vision with business as part of the transformation journey to deliver deep changes in the security function.** Protection should be based on the 5 pillars of: data center security; applications & database security; endpoints security; identity & access management (IAM); and data security.
- **How to evolve the security function towards a people-centric approach in order to avoid employees being the weak link.** This can be achieved by developing a cybersecurity culture and by strengthening professionalization of security people (including crisis management exercise).

In a cyber environment with ever-changing risks and threats, our Strategic Consulting services help clients to meet these challenges. How? By providing the insight needed to aggressively establish sound cybersecurity practices that do not hinder businesses performance. Based on a clear "Target and Roadmap", we define transformation programs enabling our Operational Consulting teams to implement standards (ISO 27xxx and others) and relevant solutions.

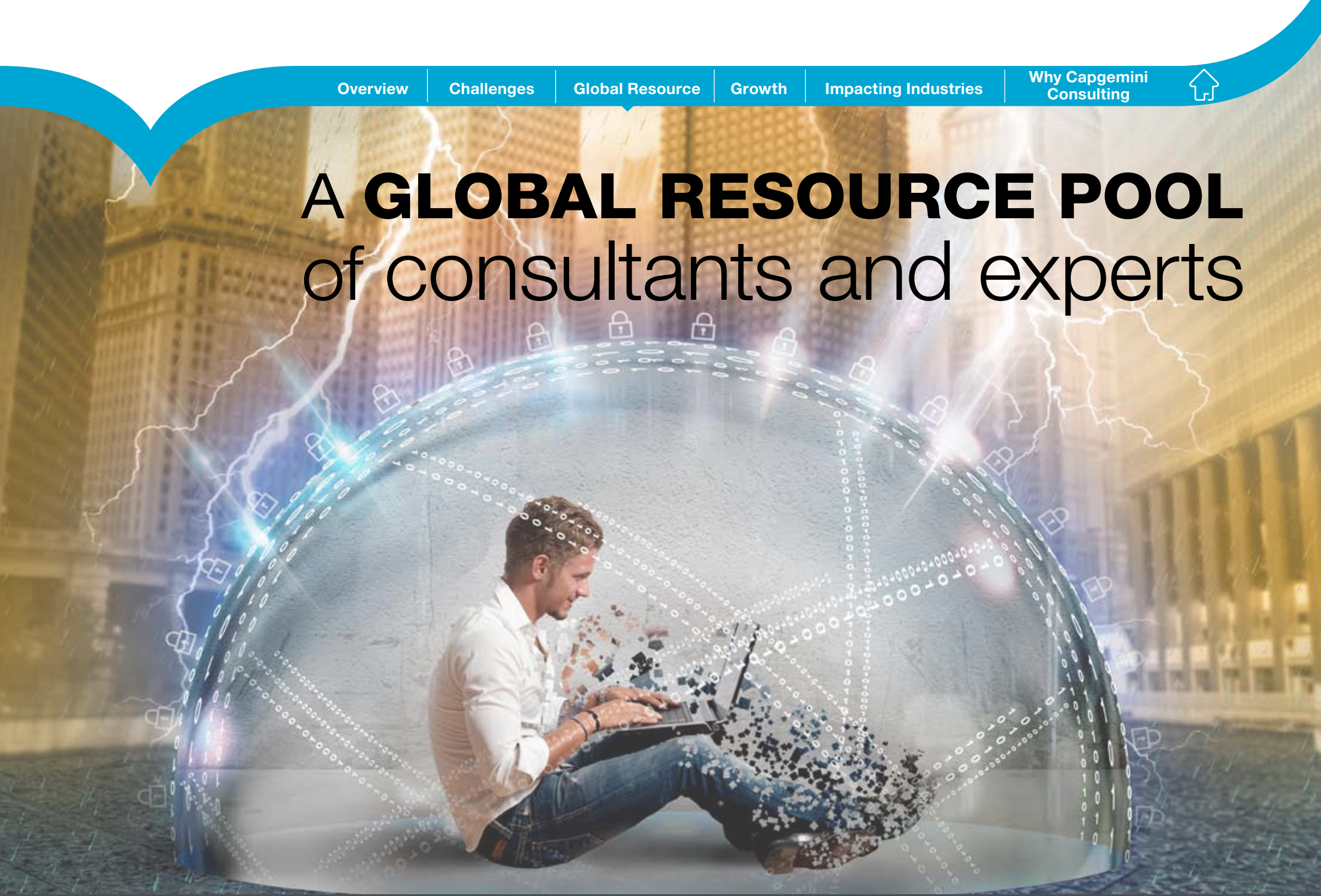


The World Economic Forum "Global Risks 2015" report highlights a number technological risks among the most important global macro risks. Data fraud or theft and cyber attacks are listed in the 10 most likely risks, while the breakdown of critical information infrastructure and networks is among the top 10 risks in terms of impact. The report also points to massive and widespread misuse of technologies as a global risk.

Partnerships with leading security vendors ensure our clients benefit from the latest tools and technologies to safeguard their enterprise assets. These include partners who are specialists in 50 different security product segments (identity access management (IAM), security information and event management (SIEM), etc.).



A **GLOBAL RESOURCE POOL** of consultants and experts



A global resource pool of consultants and experts

Capgemini Consulting's Strategic Consulting services are a key component of our broader Cybersecurity Global Practice. This comprises more than 2,500 specialists with cybersecurity skills and a deep knowledge of relevant standards, methodologies, tools and processes.

The complete portfolio of services and technologies is designed to help organizations defend themselves against cyber crime, while leveraging the power of SMACT technologies. It's a comprehensive cybersecurity transformation suite of methodologies and services giving clients proven practices, world-class consulting and technology, and leading edge managed security services. These are built on the five pillars of cybersecurity defense: Users, Applications, End-points, Infrastructure and data security

Our Cybersecurity Strategic Consulting professionals have proven experience of defining and implementing the right strategy, target operating model and GRC structure to help clients ensure their security design and operations support strategic objectives and business continuity. We accompany our clients throughout their digital and cybersecurity transformations with services integrated into the cybersecurity strategy, along with protection and monitoring capability.

Securing your Digital Transformation

By planning ahead with a cybersecurity strategy as part of your Digital Transformation journey, you will be in a more confident position to stay compliant and achieve cost savings. Your organization will derive a range of benefits around the three key themes of enabling growth, improving resilience and reducing cost.

Within these themes, we help our clients to enable Digital Transformation and innovation, while protecting their assets and reputation so that they sustain business growth. We help to extend security from deterrence and protection to prevention and full resilience. And we minimize the impact of breaches and attacks and ensure efficient compliance with regulations, such as those relating to personal data protection.

CYBERSECURITY

enabling **business growth** through **digital innovation**

Cybersecurity enabling business growth through digital innovation

Cybersecurity is a business enabler for building trust in the digital world. We have deep experience in cybersecurity transformation across Financial Services, Utilities, IT Services, Manufacturing, Government, and other sectors.

With a strong focus on data / information protection and IT / OT resilience our Cybersecurity Strategic Consulting services comprise:

- **Cybersecurity & Information Protection Maturity Assessment –** we elaborate a transformation program (quick wins, hot topics and mid-term roadmap) based on a 360° approach (technology, people, process, regulation) leveraging international standards and our own referential;
- **Cybersecurity Organization Transformation and Professionalization –** we take a global approach to cybersecurity management, encompassing both IT, OT and Data Protection, throughout a qualitative and quantitative assessment of resources (internal and outsourced), organization and governance. We aim to enhance the professionalization of enterprise cybersecurity based on a clear target organization chart, job descriptions (CISO, DPO, analyst, architect, etc.), RACI matrix, governance scheme, sourcing strategy and training / certification programs.
- **Cybersecurity Acculturation & Change Management –** we put people at the heart of cybersecurity by helping to deploy a relevant cybersecurity cultural change plan (communication, awareness and training) according to profiles, topics, resources and timing. The change management approach depends on a client's maturity and is a central tenet of successful transformation program implementation;
- **Data Classification/Protection/Privacy –** based on a maturity assessment, we focus cybersecurity programs on critical data protection across the end-to-end process. We help to identify critical data assets and build a data management roadmap including data governance, data classification, identity and access management, storage and destruction, encryption and data leak;

- **Economics and Cyber Insurance –** for our more mature and biggest clients, our service includes an assessment of cybersecurity budget and its split between organization, protection and supervision. We analyze OpEx and CapEx, people and tools. We also enable our client to review their cyber insurance policy.
- **Crisis Management for C-levels –** cyber attacks are commonplace and our task is to help our clients to be ready to manage cybersecurity crisis (by elaborating and testing concrete scenarios in their business and operational context). A cyberdefense training platform will be provided in 2016.

Our consultants will help you to increase risk control (security and privacy) throughout an effective change management process that balances the risks and opportunities of your digital journey.

From Strategic to Operational Consulting

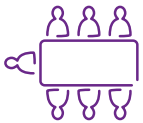
Cybersecurity & Information Protection Maturity Assessment
Elaborate a strategy and roadmap based on Capgemini framework and standards and a 360° approach (technology, people, process, regulation)

Cybersecurity Organization Transformation and Professionalization
Reposition cybersecurity as a Risk & Compliance and Competitiveness subject separating strategy, operations and controls

Cybersecurity Acculturation & Change Management
Deploy relevant communication, awareness and training actions according to profiles (individuals or communities), topics, resources and timing

Data Classification, Protection & Privacy
Ensure critical / personal data protection through proper classification and end-to-end process (prevention/protection + detection/reaction)

Cybersecurity Economics & Cyber Insurance
Optimize and adjust budgets (incl. cyber-insurance) by developing a lean management process for cybersecurity and information protection



Crisis Management for C-Level
Help clients to be ready to manage cybersecurity crisis, by elaborating and testing concrete scenarios in their business and operational context.

Operational Consulting

- CSO/CISO Assistance for Security Transformation and Compliance Program
- Risk analysis and Security objectives
- DPO Assistance for Data Privacy Transformation and Compliance Program
- Security training program and certification preparation
- ISO 27k implementation and certification preparation
- Control / Test / Audit of security measures

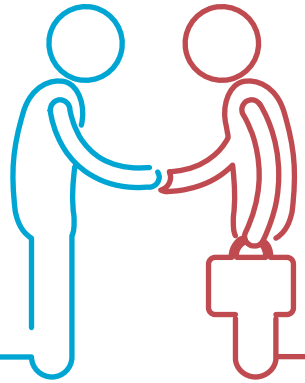
Impacting Industries

Impacting Industries

The impact of successful cybersecurity attacks is felt not just on corporate IT, but on the business and its executive too. Our insight, experience and cybersecurity capabilities will ensure your business is resilient against such attacks. Our Strategic Cybersecurity Consulting services have helped diverse organizations increase employees' awareness of the importance of cybersecurity and define their cyber defense strategies.

- Clients in Manufacturing, Industry, Utilities, Financial services and the Public Sector have drawn on our Cybersecurity & Information Protection Maturity Assessment service. This features maturity questionnaires (cybersecurity & information protection baseline, data protection, data privacy, critical infrastructures, human factor), as well as market standards (ISO, ISF, C2M2) and automated tools.
- Our Cybersecurity Organization Transformation and Professionalization service saw us drawing on knowledge of our clients' businesses and intimacy with their executives to support transformation initiatives of their security models (organization, key functions and roles, skills, RACI, training program,…) for organizations in Industry, Financial Services, High Tech and the Public Sector.
- We have provided Cybersecurity Acculturation & Change Management solutions for a large UK Public Agency and international groups (Banks, Insurance, Services), as well as a number of Oil and Gas companies. We adopt best practices and provide acceptable use policies, ready-to-use content and support for employees, IT staff, executives, etc., (on site, online/e-learning, use of different communication channels, and key performance indicators).
- Our Data Classification/Protection/Privacy/Leakage service has helped to protect data assets for a number of international groups (Banks, Insurance, Oil & Gas). We use assessment questionnaires and classification materials, and deploy best practices for information lifecycle protection.
- Our Economics & Cyber Insurance service has helped to review clients' strategy and funding to optimize their cyber security budget based on a deep maturity assessment (Telco, Utilities, High Tech).
- Our Crisis Management for C level service has helped a large European Administration to prepare itself in the event of a cyber attack through crisis management exercise.

Why Capgemini Consulting?



Why Capgemini Consulting?

Ongoing discussions at executive level on the risks and opportunities of Digital transformation

Significant investment to further develop our reputation as a global service provider enables us to address C-level cybersecurity concerns from a business risk perspective.

We work closely with Chief Information Officers, Chief Digital Officers and Chief (Information) Security Officers, Business leaders and Executives to ensure cybersecurity is an effective business enabler.

As you would expect from a global leader in cybersecurity consulting, we work with the highest industry standards to address:

- Sensitive data protection and data privacy including big data issues
- Critical IT and systems security
- Cloud and mobile computing security challenges
- Protection of Operation Technology and connected objects

Keep your organization ahead of current and emerging practices in a rapidly changing business and information technology landscape with Cybersecurity Strategic Consulting from Capgemini

Capgemini Consulting

For more details contact:

Pierre-Luc Réfalo
Global Head of Cybersecurity Strategic Consulting
pierre-luc.refalo@capgemini.com

Cyril François
Senior Vice President – Capgemini Consulting
cyril.francois@capgemini.com

About Capgemini

With more than 180,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2015 global revenues of EUR 11.9 billion.

Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

About Capgemini Consulting

Capgemini Consulting is the global strategy and transformation consulting organization of the Capgemini Group, specializing in advising and supporting enterprises in significant transformation, from innovative strategy to execution and with an unstinting focus on results. With the new digital economy creating significant disruptions and opportunities, our global team of over 3,600 talented individuals work with leading companies and governments to master Digital Transformation, drawing on our understanding of the digital economy and our leadership in business transformation and organizational change.

Find out more at:
www.capgemini.com/cybersecurity

MCOS_GI_AH_20160314