



## Cyber Security & Data Privacy Consulting

# How should CxO address Cyber Security & Data Privacy to build digital trust and resilience?

DRIVE – EMBED – DESIGN – IMPLEMENT – ASSESS



We support and secure your digital journey with consistent services to assess your posture, embed security and privacy, design platforms and implement best practices to protect sensitive data, critical infrastructures and digital services. This enables you to drive a consistent digital security strategy and roadmap focusing on risks, data and people.

### Drive, Embed, Design, Implement and Assess

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 challenges and endangering the success of digital journeys. In this landscape, while cyber criminals have matured and professionalized, Cloud, Internet of Things and connected objects, Big Data and AI technologies and services make today's digital enterprise increasingly vulnerable. The criminals are quick to exploit this.

The cost – both financially and in reputational damage – is huge. The annual cost of security incidents and data breaches is anything from \$400 billion to \$600 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. It's clear why embedding security & privacy are key to mitigate the threat of cyber-attack is a strategic priority.

Indeed, cyber security and data privacy are a board concern strongly linked to trust and resilience, innovation, competitiveness and business growth. Safeguarding personal data, research and development findings, intellectual property, business development documentation, and other critical information assets must be addressed in the context of Digital Transformation. It's key to design Security & Privacy platforms for Cloud and Mobile computing, as well as Big Data and AI, Operational Technologies (OT) and Internet of Things (IoT).

Business leaders in both strategic and operational roles must answer vital questions.

With the growth in cyber-attacks and data breaches costing business and the public sector millions every year, cybersecurity is high on the strategic agenda. Business leaders in both strategic and operational roles must answer vital questions to ensure their business is resilient. Cyber Security & Data Privacy Consulting provides key answers enabling strategy alignment, competitiveness and performance.

Globally, organizations are facing 3 big challenges to manage digital risks

#### #1 Challenge: Disrupt digitally



- How to embed cyber security and data privacy in your Cloud strategy enabling your digital enterprise?
- How to ensure secure digital transformation with limited constraints for users?
- How to transform your current practices to manage increasing threats and ensure your business is resilient?
- How to transform your Governance and Risk Management processes?
- Can you trust new digital opportunities & transform without compromising your critical assets?
- Can you trust partners / third parties / new acquisitions or will their lack of security have an impact on your reputation?

#### #2 Challenge: Protect and Comply



- How to manage and control cyber-threats efficiently?
- Are you compliant with security and privacy regulations and corporate policies as well?
- How do you transform the CISO function to deal with business and legal requirements efficiently?
- How to control security & privacy operations across digital services, apps, data, infrastructures and endpoints?
- How your clients trust your services or products in terms of how you use and secure their data?
- How to manage the impacts of any security incident or data breach?

### #3 Challenge: Reduce (optimize) costs

- What are the most efficient governance models?
- What are relevant human resources and skills to rely on?
- What are the technologies to be implemented at best cost?
- What balance in terms of in sourcing and out sourcing?
- What balance in terms of Prevention/Protection vs Detection/Response?
- How to include cyber insurance in your Risk Management practices?

### Some examples: 2012 - 2018

ME: Stuxnet malware is the first public attack on industrial systems that reduced Iran nuclear industry capacity.

NA: Based on a phishing attack, criminals accessed data for 40 million credit cards. The retail company cost for credit card replacement estimated at \$200 million.

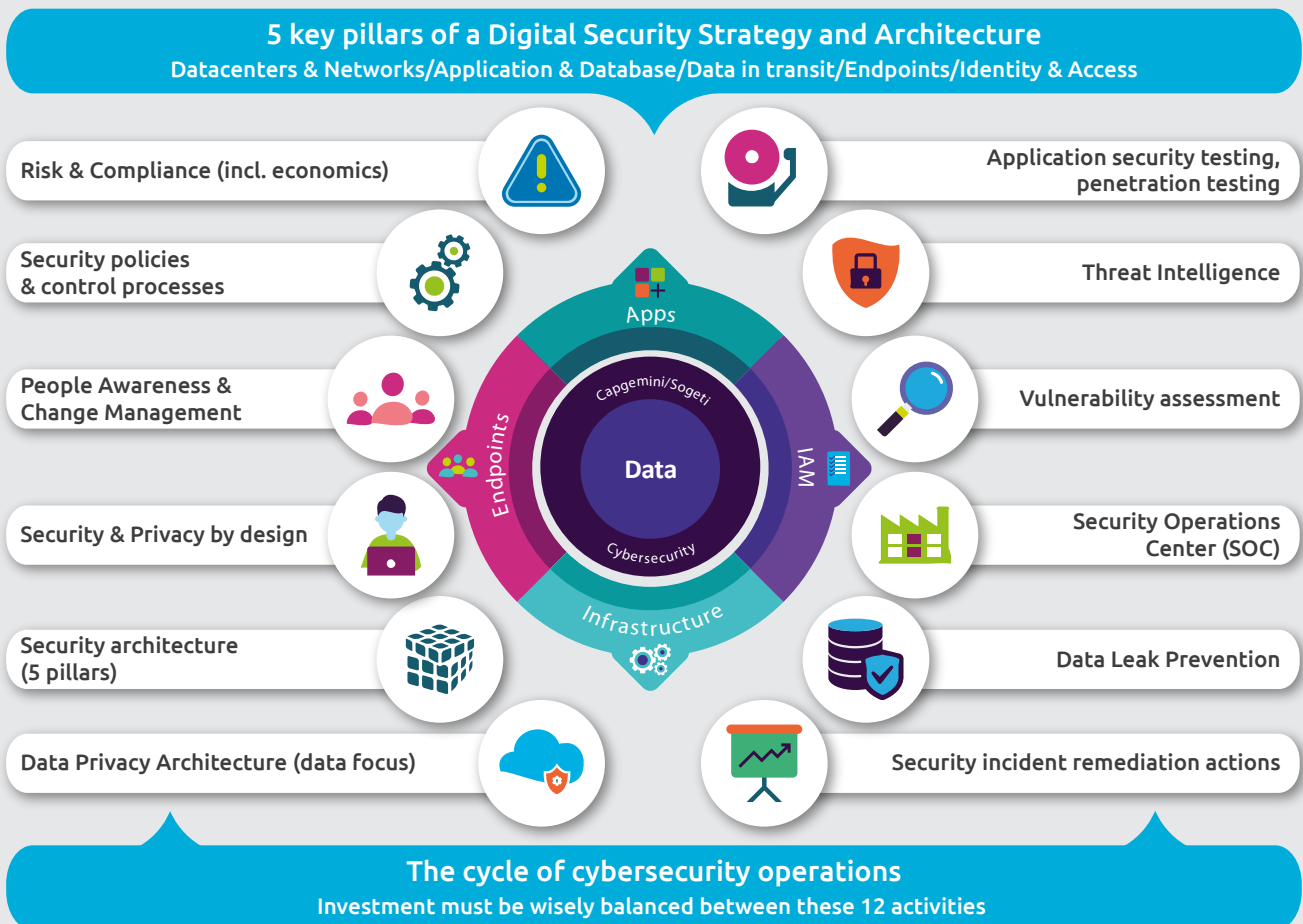
FR: Cyber attack on international TV by State sponsored or Hacktivists. Huge sabotage of operational systems using social media credential.

UK: A telco has been fined a record £400,000 fine for security failings which led to the theft of personal data of almost 157,000 customers.

WW: The largest RansomWare attack in history hit over 200,000 computers in at least 150 countries on 13th May 2017.

WW: Cambridge Analytica harvested the data of 87 millions of Facebook profiles, taking advantage of a loophole in Facebook API.

Figure 1: 5 key pillars of Digital Security Strategy and Architecture



The World Economic Forum “Global risk report 2018” highlights four technological risks among the 30 most important macro risks:

- Cyber attacks
- Data fraud / theft
- Critical infrastructure breakdowns
- Adverse consequences of technological advances

Cyber attacks are in the top 10 risks, both in “Likelihood” and “Impact”

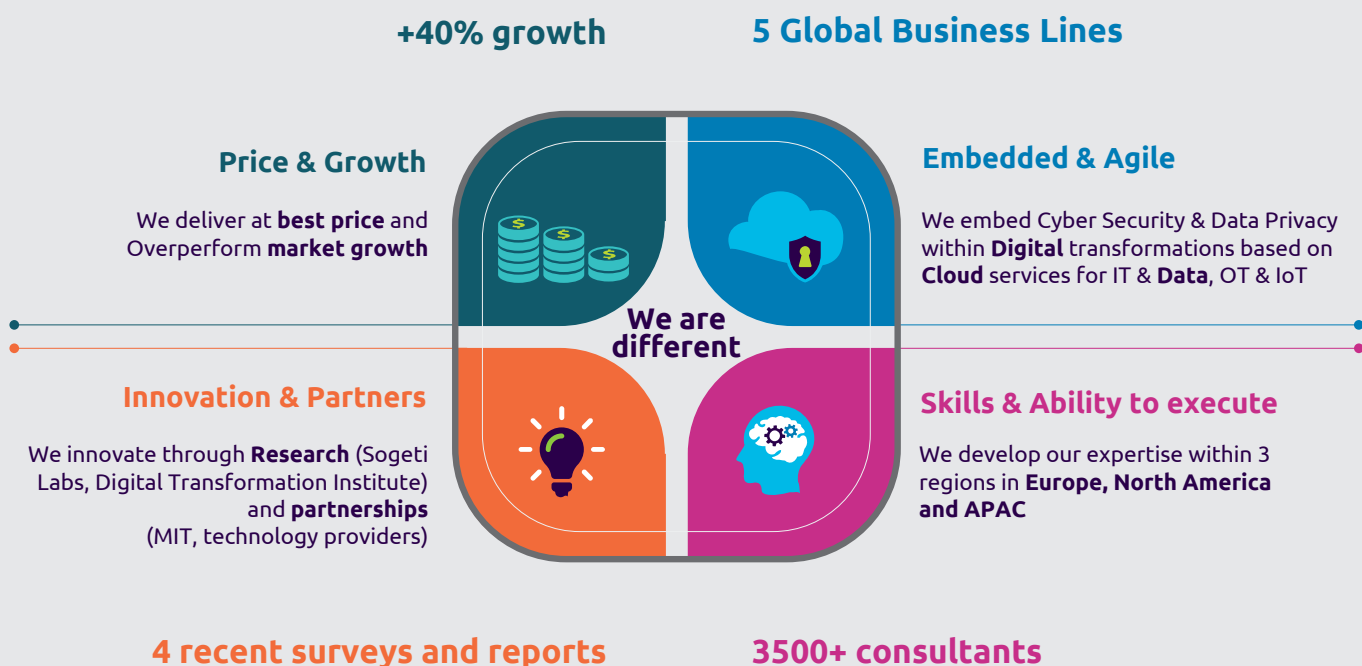
## A coordinated resource pool of consultants and experts

### Joining forces and skills

Our consulting services are a key component of our broader Cybersecurity Global Practice. This comprises more than

3,500 specialists with cyber security and data privacy skills and a deep knowledge of relevant regulations, standards, methodologies, tools and processes. The complete portfolio of services and technologies delivered by our teams, is designed to help organizations defend themselves against cybercrime and demonstrate proper compliance, while leveraging the power of Digital and Cloud technologies. It’s

Figure 2: Why are we different



a comprehensive suite of skills, methodologies and tools giving clients proven practices, world-class consulting and technology, and leading edge managed services. These are built on expertise covering the five pillars of our cybersecurity models: Users, Applications, End-points, Infrastructure and data.

Our Cyber Security & Data Privacy Consulting professionals have proven experience of defining and implementing the right strategy, target operating models and GRC structure to help clients embed security and privacy as a business enabler and design adequate platforms with people, process and technology. We accompany our clients throughout their digital journey to implement relevant standards and comply with regulations along with protection and monitoring capability.

### Developing trust and resilience

By planning ahead with a cybersecurity strategy as part of your Digital Transformation, you will be in a more confident position to develop trust and resilience, 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, innovation and competitiveness, 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 data breaches and cyber-attacks and ensure efficient compliance with regulations, such as those relating to personal data protection.

### Delivering large projects

Our teams are used to work for national and international accounts in complex and multicultural environments. Our biggest teams are located in France, UK, North America, Germany and the Netherlands. They are complemented and supported by strong capabilities in Spain, Portugal, Italy, Nordics and India.

Figure 3: Cyber Security & Data Privacy Consulting Portfolio

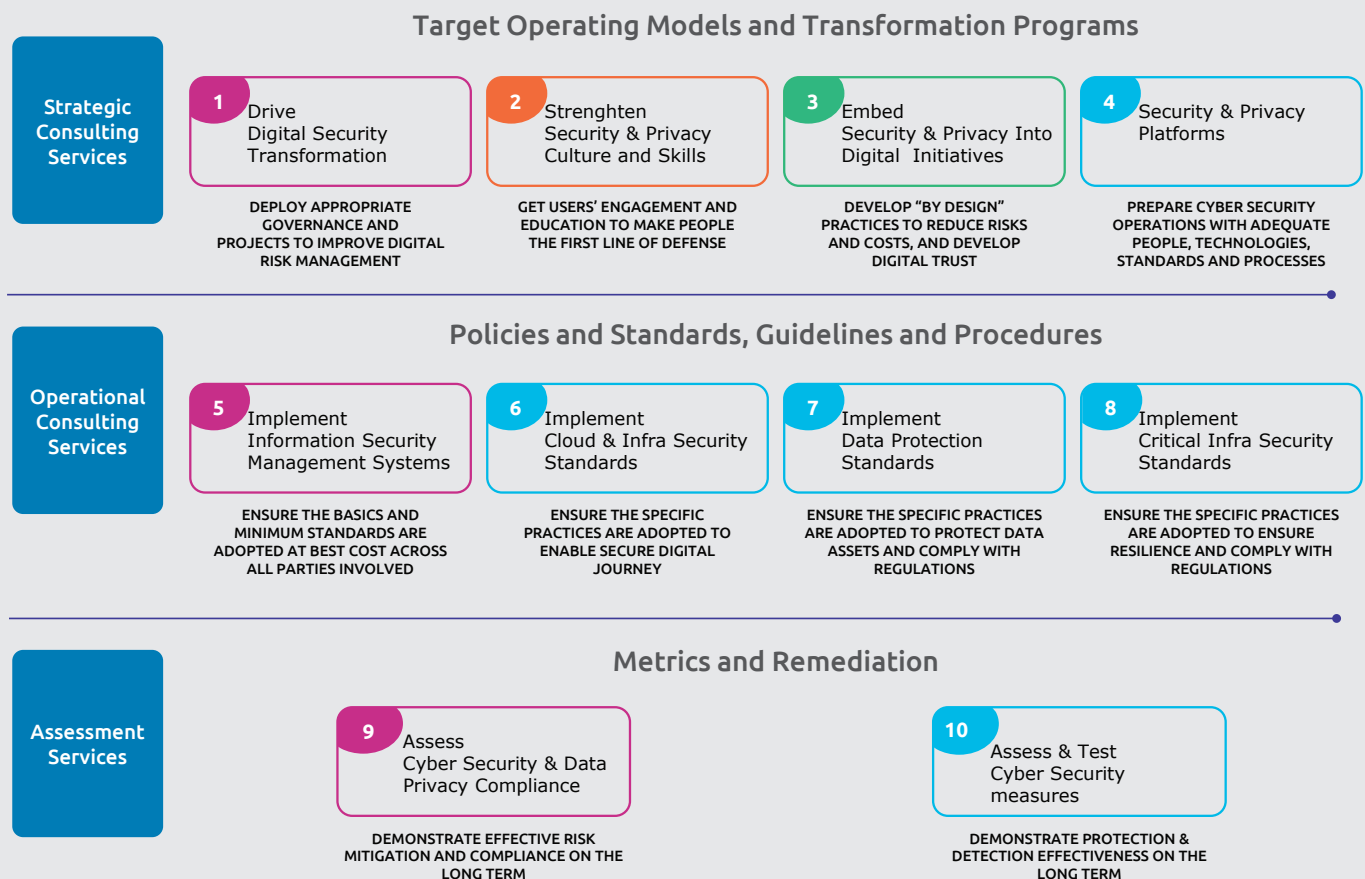
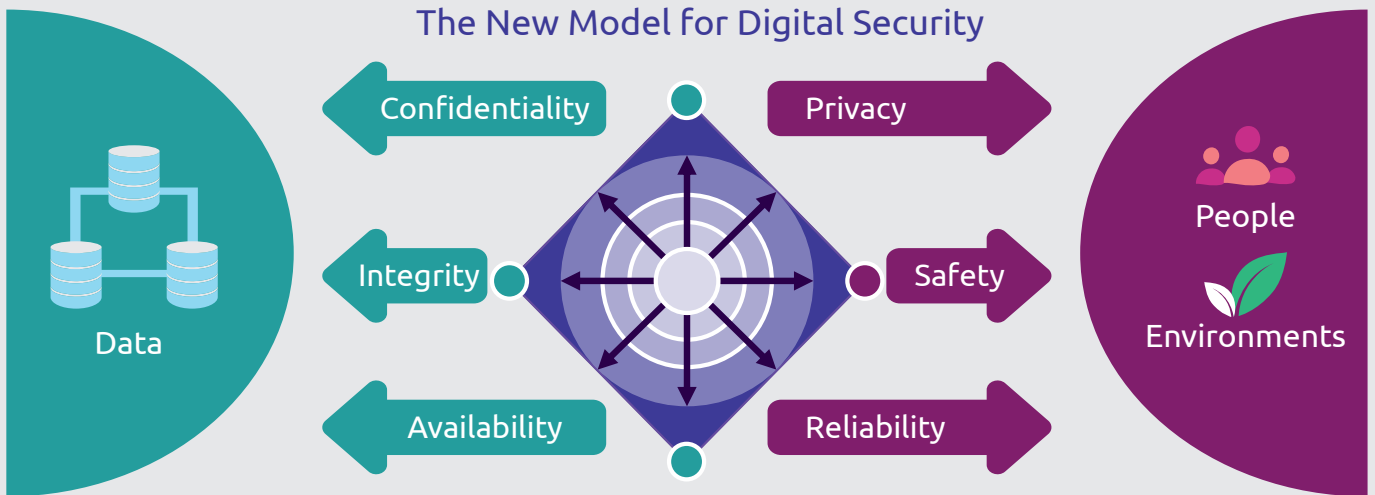


Figure 4: Toward Digital Trust and Resilience

## Safety, Reliability and Privacy: Digital Security Imperatives



Gartner Security & Risk Management Summit : "Tutorial: Gartner Essentials: Top Cybersecurity Trends for 2016-2017," Earl Perkins, 12-13 Sept 2016

### Impacting Industries on the long term

Cybersecurity is a business enabler for building trust and resilience in the digital world <Figure 4>. We have deep experience in cyber security & data privacy transformation across Financial Services, Utilities, IT Services, Manufacturing, Automotive, Government. Our clients are from all sectors.

Our consultants help to increase risk control (security and privacy) throughout an effective change management process that balances the risks and opportunities of your digital journey. The impact of successful cyber attacks or data leaks is felt not just on corporate IT, but on the business and its executives too. Our clients are C-level.

We have helped diverse organizations increase management awareness of the importance of cyber security and data privacy to define their cyber defense strategies.

- Clients of all sectors have drawn on our Strategic Consulting services. This features maturity questionnaires / models and workshops to establish a proper digital security strategy. We drive multiyear program management to enable consistent implementation of target operating models. We help clients to develop their security and privacy culture (on site, online/e-learning and COOC, KPI), their organization and process (key functions and roles, RACI, skills, training program). We build methodologies and processes for "security & privacy" by design (GDPR, DevSecOps) with business and data owners. Finally, we design "security & privacy" platforms for key

processes (GRC, IAM, SOC, DLP) based on technology and organization with business and IT managers.

- Clients of all sectors have drawn on our Operational Consulting services. This complements Strategic consulting services. It features the definition and implementation of policies and standards, guidelines and procedures. We provide strong expertise on security & privacy frameworks related to Information Security Management (ISO27001/27002, NIST, ISF, ISACA), Data Privacy / Protection (ISO27018, ISO29101, NIST, IAPP), Cloud Security and Privacy (CSA-CCM, ISO27018, NIST) and Critical infrastructures (NIS Directive, NIST). We contribute to prepare certifications of digital services, applications and systems.
- Clients of all sectors have drawn on our Assessment services. This features the implementation of security & privacy controls and tests, metrics and dashboards. It aims to demonstrate compliance and effectiveness and to define adequate remediation plan. We use and develop specific tools and methodologies for pentesting and cyber-attack simulation, audit of organization, processes and architecture. These services are strongly connected to Strategic Consulting (to review target operating models and roadmap), Operational Consulting (to use consistent frameworks and metrics), Protection Services (to build the solutions on strong foundations) and Managed Services (ie. Code audit and Application Security Testing).

## Why Capgemini?

### 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 cyber security and data privacy concerns from a business risk perspective.

We work closely with Chief Information Officers, Chief Digital Officers and Chief (Information) Security Officers, Data Protection Officers, Business leaders and Executives to ensure cyber security and data privacy are effective business enablers.

As you would expect from a global leader in cybersecurity, we work with the highest security and privacy standards and technologies to propose managed services and protect:

- Personal and sensitive data incl. Big data and AI
- Critical infrastructures
- Cloud and mobile technologies and services
- Operation technologies for digital factories
- Connected objects

**Keep your organization ahead of current and emerging practices in a rapidly changing business and digital landscape with cyber security and data privacy consulting from Capgemini.**



*Gartner reports Capgemini #10 for worldwide Security Consulting Services market share in 2017; overall market totaled \$19.0 billion in revenue."*

Source: Gartner Inc.: "Market Share: Security Consulting Services, Worldwide, 2017" Elizabeth Kim, 26 July 2018



*Capgemini was positioned as 'Challengers' in ALM Vanguard Report and 2nd in terms of 'Breadth of Consulting Capabilities'.*

*"Capgemini exhibited several capability ratings that were quite strong, finishing in the Challenger section of the Vanguard and showing positive momentum."*

Source: Gartner Inc.: ALM Intelligence's 2017 Vanguard Report on Cybersecurity Consulting Worldwide

Disclaimer: Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



## About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2016 global revenues of EUR 12.5 billion.

Visit us at

[www.capgemini.com](http://www.capgemini.com)

### For more details contact:

**Geert Van der Linden**

EVP, Cybersecurity Business Lead

*[geert.vander.linden@capgemini.com](mailto:geert.vander.linden@capgemini.com)*

**People matter, results count.**

The information contained in this document is proprietary.  
©2018 Capgemini. All rights reserved.