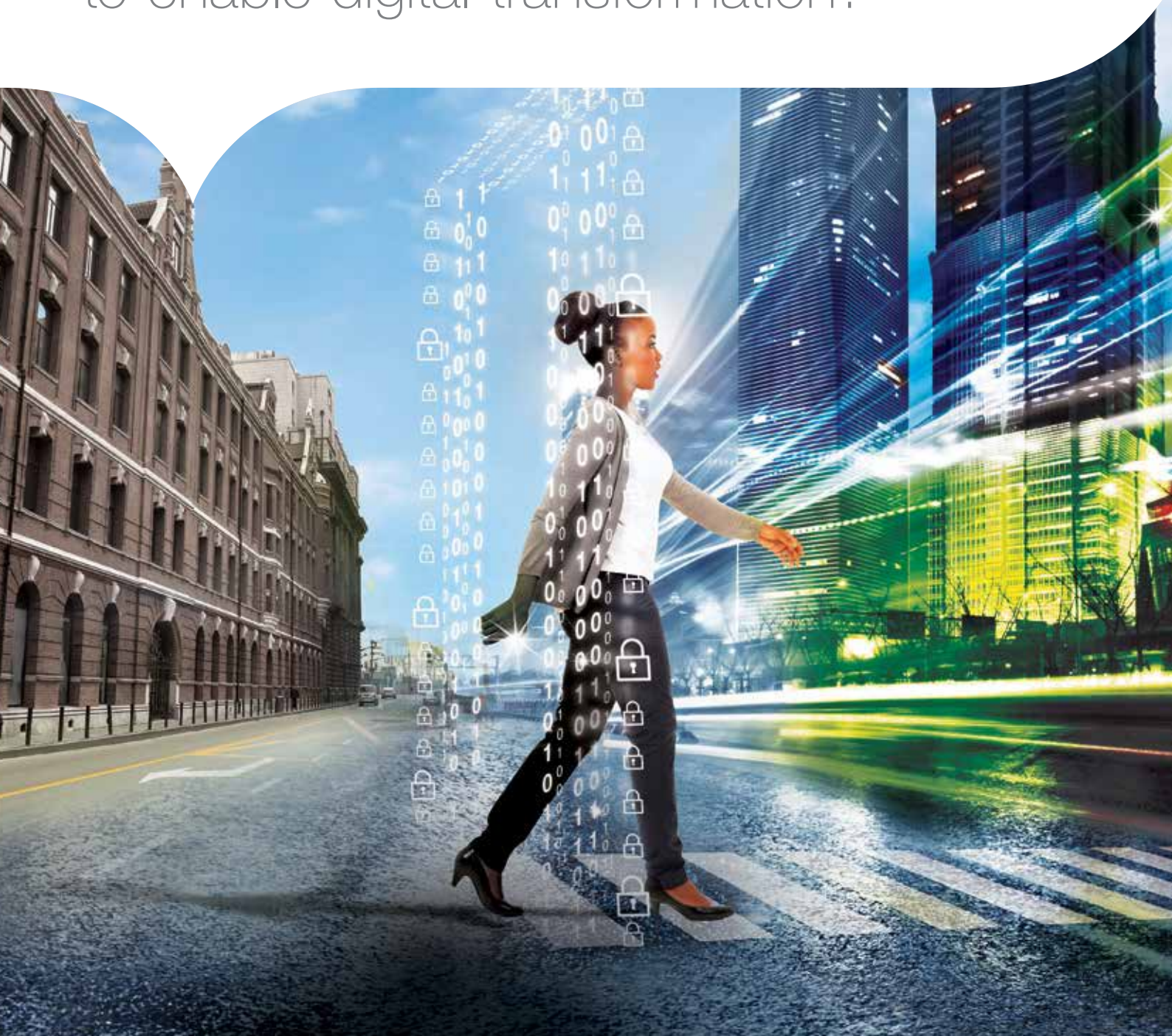# Capgemini Consulting

How should CxO address Cybersecurity and Data Protection to enable digital transformation?

We support and secure digital transformation with assessments, diagnosis and audits of your organization, the protection measures you have implemented and your security monitoring capabilities related to sensitive data, critical infrastructures and digital services. This enables you to define a consistent cyber security strategy and transformation roadmap focusing on Data, risks and people.

Understand your position and increase your cybersecurity practices

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, **Cloud, Internet of Things, Big data 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. 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, Operational Technologies (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 as well? Is it possible to combine digital transformation with acceptable risks, and how secure are your websites, IT infrastructures, applications and data?

Capgemini Consulting helps 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

Figure 1: The cybersecurity challenges

Cyber threats (sabotage, fraud, theft, intrusion, 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 infrastructure protection. Investment must be balanced between a cycle of cybersecurity activities comprising: anticipation, prevention, protection, detection, reaction (as depicted below). It embraces cloud services and Agile practices <Devops>.

How to align the new cybersecurity vision with business as part of the digital journey to deliver deep changes in the security function. Protection should be focused on personal / sensitive data and Identity & Access Management (IAM), consistently with applications & database, endpoints, and infrastructures.

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).

can strengthen your organization with effective solutions and procedures for governance, risk and compliance (GRC).

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 and data protection practices that do not hinder businesses performance. Based on a clear "Target and Roadmap", we define and manage transformation programs enabling our Consulting teams to implement standards (ISO 27k and others) and relevant solutions.

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 (Data protection (structured and unstructured), identity access management (IAM), security information and event management (SIEM), etc.).

Some examples: 2012 - 2017

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.

Figure 2: 5 key pillars of Digital Security Strategy and Architecture

5 key pillars of a Digital Security Strategy and Architecture
Datacenters & Networks/Application & Database/Data in transit/Endpoints/Identity & Access

Security policies & control processes (5 pillars)

People awareness

Security & Privacy by design

Security architecture (5 pillars)

Data protection & leak Prevention

Application security testing, system penetration testing

Threat Intelligence

Vulnerability assessment

Threat hunting

Security Operations Center (SOC)

Computer Security Incident Response Team (CSIRT)

Security incident remediation actions

Apps · IAM · Infrastructure · Endpoints · Capgemini/Sogeti · Data · Cybersecurity

The cycle of cybersecurity operations
Investment must be wisely balanced between these 12 activities

The World Economic Forum "Global risk report 2017" highlights four technological risks among the 30 most important macro risks:

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

A global resource pool of consultants and experts

Capgemini Strategic Consulting services are a key component of our broader Cybersecurity Global Practice. This comprises more than 3,000 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 Digital and Cloud 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 Strategic Cybersecurity 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.

Figure 3: Why are we different
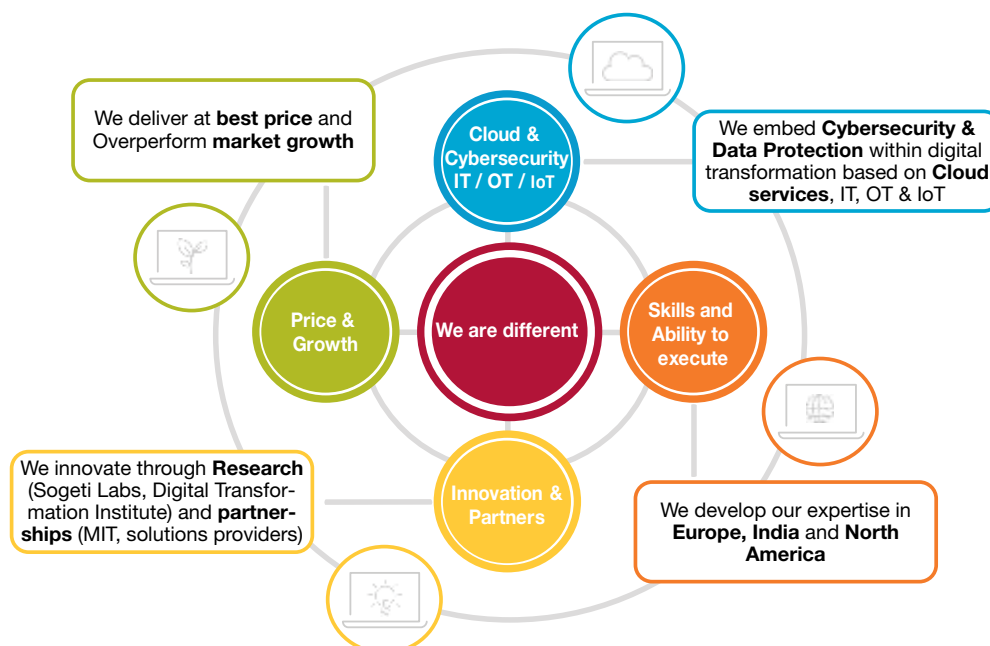
Four packaged services to accelerate your cyber security transformation

Cybersecurity Maturity Assessment & Transformation
Elaborate a strategy and roadmap based on market standards and a 360° approach (technology, people, process, regulation) based on maturity and compliance assessments. Implement the relevant transformation program based on deep insight and analysis validated with stakeholders. Balance achieved security and efforts with economic impacts, budgets and cyber-insurance.
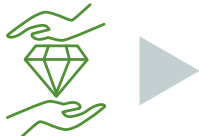
Data Classification, Privacy & Protection
Focus the Security & Privacy Transformation Program on critical and personal data based on deep insight, exhaustive assessment and proper classification. Be prepared to comply with GDPR through a consistent vision and program. Monitor the implementation of « end to end » solutions and processes.

Cybersecurity Organization Transformation and Professionalization
Support clients' Digital Transformation whilst repositioning cybersecurity as a topic at the appropriate level of enterprise governance. Move from "Fortified castle" to "Airport" security model and consider Security & Privacy as a Risk & Compliance and Competitiveness subject. Propose Target Operating Models for IAM, SOC and incident / crisis management.

Cybersecurity Acculturation & Change Management
Consider the human factor at the heart of cybersecurity. Reduce the weak link by testing users behavior (phishing, passwords, etc.). Deploy communication, awareness and training measures covering different topics considering target audience, resources and timing.

Operationalize Strategic Consulting Services
We complement cyber security transformation with 6 additional services

CIO/CSO/CISO Assistance for Security Transformation and Compliance Program

Risk analysis for IT project and Cyber Security objectives

DPO Assistance for Data Privacy and Protection Transformation and Compliance Program

Security professionals training program and certification preparation
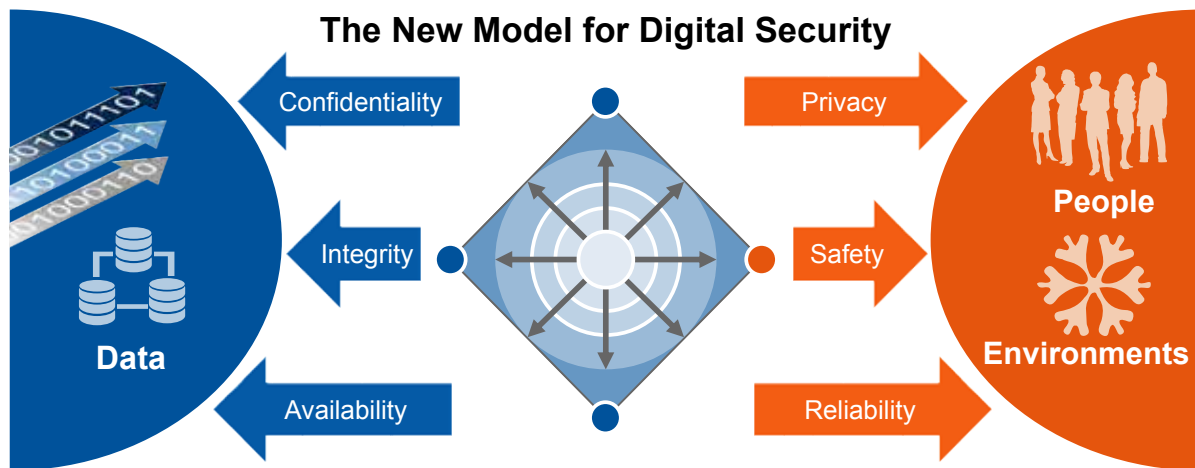
ISO 27k implementation and certification preparation

Control / Test / Audit of security measures (incl. pentest, ethical hacking, code audit)

Safety, Reliability and Privacy: Digital Security Imperatives

The New Model for Digital Security

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

Impacting Industries

Cybersecurity is a business enabler for building trust and resilience in the digital world <Figure 4>. We have deep experience in cybersecurity transformation across Financial Services, Utilities, IT Services, Manufacturing, Government, and other sectors.

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.

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

- Clients of all sectors have drawn on our Cybersecurity Maturity Assessment & Transformation service. This features maturity questionnaires / models and workshops to establish a proper strategy (security & privacy). We ensure multiyear program management to enable consistent implementation of policies, standards and target operating models.

- Our Data Classification, Privacy & Protection service has helped to protect data assets for a number of international groups (Banks, Insurance, Oil & Gas, Public services). We use assessment questionnaires, classification methodology and tools and deploy best practices for information lifecycle protection with strong focus on GDPR requirements*.

- We have provided Cybersecurity Awareness & 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 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 cybersecurity & data protection models (organization, key functions and roles, skills, RACI, training program,…) for organizations in Industry, Financial Services, High Tech and the Public Sector. This is performed at different levels: corporate and IT governance, IAM and SOC initiatives, Cloud and DevOps deployment.

*: Capgemini proposes a specific "end-to-end" Data protection and GDPR global offer. Contact our Leader.

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 and data protection 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 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.
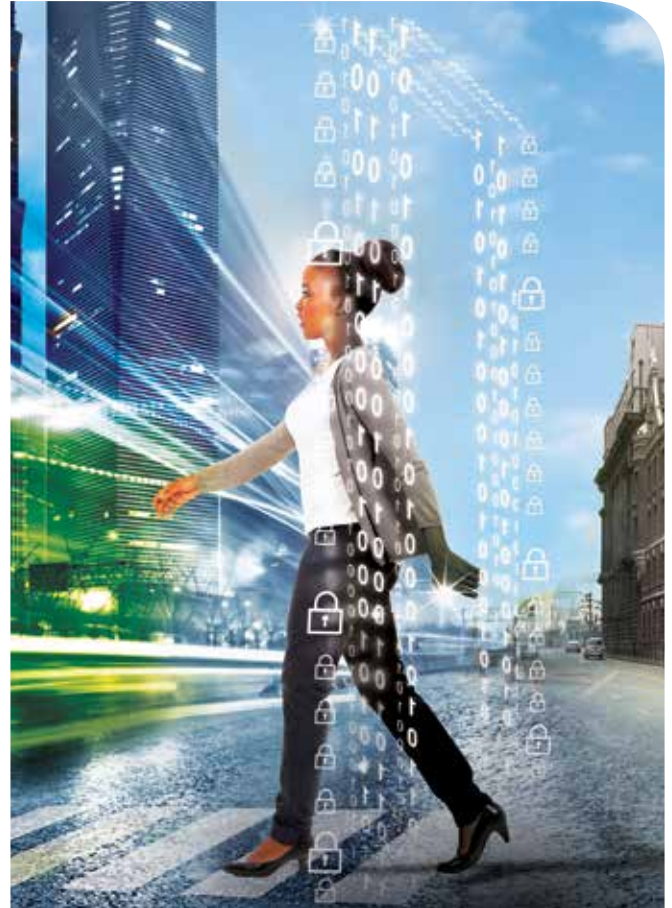
"Gartner reports Capgemini #12 for worldwide Security Consulting Services market share in 2016; overall market totaled $17.8 billion in revenue."
Source: Gartner Inc.: "Market Share: Security Consulting Services, Worldwide, 2016" Elizabeth Kim, 9 May 2017

"Gartner acknowledges Capgemini as a representative vendor for Security Consulting Services in Market Guide published on Sep, 2016."
Source: Gartner Inc.: "Market Guide for Security Consulting Services, Worldwide, 2016," Jacqueline Heng, Elizabeth Kim, 29 Sept 2016
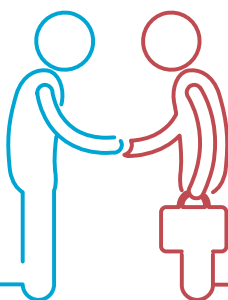
Capgemini Consulting

For more details contact:

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

Paul Lokuciejewski
Capgemini Consulting DACH
paul.lokuciejewski@capgemini.com

Isabelle Budor
Capgemini Consulting FRA
isabelle.budor@capgemini.com

Tim Van de Water
Capgemini NA
tim.vandewater@capgemini.com

Sandeep Kumar
Capgemini Consulting UK
sandeep.j.kumar@capgemini.com

Stéphane Joguet
Capgemini Consulting FRA
stephane.joguet@capgemini.com

Erik Hoorweg
Capgemini Consulting NL
erik.hoorweg@capgemini.com

Karri Tomula
Capgemini Consulting SweFi
karri.tomula@capgemini.com

About Capgemini

With more than 190,000 people, Capgemini is present in over 40 countries and celebrates its 50th Anniversary year in 2017. A global leader in consulting, technology and outsourcing services, the Group reported 2016 global revenues of EUR12.5 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, the global team of over 3,000 talented individuals work with leading companies and governments to master Digital Transformation, drawing on their understanding of the digital economy and leadership in business transformation and organizational change.

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