Cybersecurity@
Capgemini Consulting
Leader in Digital Transformation
Company Profile:

About Capgemini

Strategic Cybersecurity Consulting:

Our service portfolio

References and contact information:

Our publications, experience and contact persons
With 180,000 employees and offices in 44 countries, Capgemini is the largest consultancy with European origins.

More than 10,000 strategy and management consultants globally, supporting the design and operationalization of strategies.

Conception, development and implementation of a wide range of (IT) projects on system integration and application development for our clients.

Support of our clients in complete or partial outsourcing of their IT systems and business processes.

IT services for our clients, which are adjusted according to local needs, as well as highly specialized, cost efficient testing strategies.

As full service provider we offer a wide array of services from one source, which range from strategy development to technical services and operations of IT systems.
WE ACCOMPANY YOU IN ALL PHASES…
… from strategy development to monitoring of the implementation success

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Concept</th>
<th>Implementation</th>
<th>Steering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development of company/ case specific vision</td>
<td>Design of detailed target picture for processes and systems (business and technical concept)</td>
<td>Setup of organization structure, processes and IT landscape in line with concepts</td>
<td>Definition of milestones to achieve implementation goals</td>
</tr>
<tr>
<td>Definition of strategic targets and cornerstones</td>
<td>Development of organization and governance model with roles and responsibilities</td>
<td>Concretization of concepts through instructions and job specifications</td>
<td>Definition of escalation processes</td>
</tr>
<tr>
<td>Analysis of internal and external parameters and derivation of business cases</td>
<td>Definition of change and communication strategy</td>
<td>Coordination of process and system adjustments including test of processes, systems and interfaces</td>
<td>Application of steering instruments such as jour fixes</td>
</tr>
<tr>
<td>Definition of high-level target conditions and development of end-to-end implementation strategy</td>
<td>Development of implementation plan</td>
<td>Documentation, coaching, training, post go-live support and handover to business</td>
<td>Ongoing monitoring and steering of project progress</td>
</tr>
</tbody>
</table>

© Capgemini Consulting 2016. All rights reserved.
CAPGEMINI CYBERSECURITY CAPABILITIES

**Strategy, Governance, & People**
- Digital security assessment & strategy and risk management
- Cybersecurity awareness & Training

**Transformation**
- Security transformation & operating model implementation
- Program management & change and communication management

**Build & Operations**
- Application security testing & technical security testing (e.g. SCADA)
- Implementation of security solutions & managed security services (e.g. SOC)

2,500+ Capgemini resources with Cybersecurity skills

© Capgemini Consulting 2016. All rights reserved.
TRENDS IN CYBERSECURITY

Old Paradigm

Perimetric defense
Zero-risk dream & Compliance
Control-centric
Prevent & protect

New Paradigm

Security Strategy & Asset Inventory
Risk Management & Information Classification
People & Awareness
SIEM & Security Operations Centre (SOC)

SOLUTIONS

Data-centric defense
Digital risks & Information life cycle
People-centric & Security by design
Predict, monitor & respond

© Capgemini Consulting 2016. All rights reserved.
OUR CYBERSECURITY CAPABILITIES

OUR STRATEGIC CYBERSECURITY CONSULTING ADDRESSES C-LEVEL AND BUSINESS CONCERNS TO ENABLE A SECURE DIGITAL TRANSFORMATION. IT WILL HELP YOU TO

MATURITY ASSESSMENT & STRATEGY
“gain a profound understanding of your current Cybersecurity situation and support you in a strategic realignment.”

DIGITAL RISK & DATA PRIVACY
“identify your critical assets, manage business-oriented risks and protect the privacy of your data.”

“AWARENESS & TRAINING
“foster a people-centric security culture and a holistic security by design based on awareness and training programs.”

SECURITY TARGET OPERATING MODEL (ISMS)
“establish an effective Cybersecurity organization, governance, policies and processes for a digital resilience.”
MATURITY ASSESSMENT & STRATEGY

“gain a profound understanding of your current Cybersecurity situation and support you in a strategic realignment.”

Security Maturity Assessments

- Holistic assessment of your security maturity
- Conduction of focused assessments, e.g. critical infrastructure, BSI Cyber Security Check, client data
- Assessment of partners and supply chain security
- Peer group benchmarking using extensive database

Transformation Roadmap & Strategy Development

- Definition of sustainable information security strategy including mission and vision statement to position security as integrated business partner
- Development of a transformation roadmap and business cases in alignment with business and IT

Security Operations Center (SOC) & Control Centers

- Conduction of feasibility studies to evaluate SOC readiness for office and process IT
- Definition of functional/technical requirements
- Design and evaluation of scenarios
- Definition of strategies for security control centers

References

- Assessment of security maturity and definition of group-wide security roadmap for Germany's leading retailer
  **Benefits:** Transparency, synergies leveraged, clear strategy

- Evaluation of digital resilience capabilities based on BSI Cyber Security Check and development of prioritized gaps for a leading investment bank
  **Benefits:** Identified critical gaps, effective mitigation plan

- Evaluation of detection and reaction capabilities for operational technology (OT) of German’s major utility company
  **Benefits:** Clear requirements, transparency on costs and target business model

© Capgemini Consulting 2016. All rights reserved.
DIGITAL RISK & DATA PRIVACY

“identify your critical assets, manage business-oriented risks and protect the privacy of your data.”

References

- Evaluation of business processes using a business impact analysis to define security concepts for a financial institute
  **Benefits:** Focus on critical assets, targeted system protection at reduced costs, regulatory compliance

- Design and implementation of an integrated IT risk management aiming at a stronger involvement of business and IT in the risk evaluation and mitigation process
  **Benefits:** Business-driven risk exposure, higher awareness

- Design and implementation of a global privacy by design methodology at a multinational Dutch bank
  **Benefits:** Reduced privacy violations, increased awareness structures

**Information Asset Inventory & Business Impact Analysis**

- Identification of information assets derived from business processes
- **Business-oriented impact analysis** of assets
- Evaluation of **protection levels** and development of **security concepts** for IT systems

**Digital Risk Management**

- Development of threat and risk catalogues for effective, **business-oriented identification of risks**
- **Strong involvement of business** in risk assessment
- Definition of **risk registers** and management reports
- **Alignment** with enterprise risk/vendor management

**Data Privacy**

- Conduction of **privacy impact analyses** for insights in gaps and risks within IT infrastructure and systems
- Design of **privacy governance framework**
- Definition of **policy frameworks** (e.g. binding rules)
- Creation and implementation of **awareness actions**
SECURITY TARGET OPERATING MODEL (ISMS)

“establish an effective Cybersecurity organization, governance, policies and process for a digital resilience.”

References

- Design of organizational structures including role profiles, sizing analysis, HR strategy and the integration of security competence center structures for a leading retailer
  **Benefits:** Strong business engagement, clear responsibilities

- Based on a gap analysis of the existing framework, formulation of policies in alignment with ISO 27001 and SITB standard for a German investment bank
  **Benefits:** Regulatory compliance, clear responsibilities

- Definition of a business-oriented role concept and adoption of roles and privileges for a financial service provider
  **Benefits:** Transparency, revised and simplified structures

Organizational & Governance Design

- Definition of roles and responsibilities for people-centric and business-oriented security organizations
- Design and implementation of governance structures
- Development of security KPIs and reporting
- Communication and training of CISO/stakeholders

Policy and Compliance Framework & GRC Automation

- Development of policy frameworks based on common standards, e.g. ISO 27001, BSI, SITB
- Definition of statement of applicability (SOA)
- Formulation of level 1 – level 4 policies
- Selection and implementation of GRC/ISMS tools

Identity and Access Management & Security Processes

- Definition of business-oriented, functional roles
- Development of segregation of duty matrix, policies, functional role concepts and processes
- Analysis and optimization of privileges in IT systems
- Design and implementation of security processes

© Capgemini Consulting 2016. All rights reserved.
**Employee Awareness Programs & Change Management**

- Design and implementation of a holistic concept for employee awareness programs
- Development of print and digital awareness initiatives based on implementation-ready tool box
- Use of various communication channels and KPIs

**Target-group Specific Awareness**

- Development of awareness initiatives for top management
- Conduction of targeted trainings for high risk business profiles
- Preparation and conduction of face-to-face trainings

**Security Training**

- Design of training concepts for IT staff, e.g. IT demand manager, developers or operations
- Development of training concepts for security staff, e.g. administrators or ISOs
- Conduction of trainings and live-hacking demos

---

**References**

- Design and implementation of a multi-lingual awareness campaign for 22,000 employees of Austria’s largest oil company
  **Benefits:** Increased awareness, reduced security risks, improved acceptance and visibility of security organization

- Support of a financial service provider in the conception of campaign to sensitize employees for privacy risks
  **Benefits:** Improved awareness for customer data/ privacy

- Training of business data owners, architects and developers to introduce security by design at an international retailer.
  **Benefits:** Holistic protection through security-by-design

“AWARENESS & TRAINING

“foster a people-centric security culture and a holistic security by design based on awareness and training programs.”
## MANAGED SECURITY SERVICES

### Security Offerings

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC(aaS)</td>
<td>Security Information &amp; Event Management (SIEM)</td>
</tr>
<tr>
<td>Intrusion Detection/Prevention (IDS/IPS)</td>
<td>DLP (Data Leakage Prevention)</td>
</tr>
<tr>
<td>Encryption(aaS)</td>
<td>Vulnerability Management</td>
</tr>
<tr>
<td>DDoS Protection</td>
<td>IAM(aaS)</td>
</tr>
<tr>
<td>Firewall, Network Security Web Gateway &amp; Content Filtering</td>
<td>EndPoint Security(aaS), Anti-Malware &amp; Anti-SPAM</td>
</tr>
<tr>
<td>Forensics Investigations &amp; Incident Response</td>
<td>Public Key Infrastructure (PKI)</td>
</tr>
</tbody>
</table>

### Offering Basis
- Flexible, modular offerings
- Unit based pricing approach
- Hosted or CPE based delivery model
- Flexible support model (business hours or 24x7)
- Alignment to industry leading practices and compliance requirements
- Services delivered out of centers across the globe to support local data protection requirements

### Security Operations Center (SOC)
- SIEM (log/packet collection, correlation, analysis)
- Scanning, vulnerability assessment
- Sandboxing
- Security analytics

### Support

Supports you in the transition and transformation of managed security services.

© Capgemini Consulting 2016. All rights reserved.
OUR ANNUAL PUBLICATIONS & BOOKS

- Annual global Information Security benchmarking study assessing the security situation of organizations
- Discussion of current trends, security risks, breach costs and best practices
- Insights into security budgets and organizational structures
- Comprehensive evaluation of security maturity level and industry-specific analyses make individual benchmarking with specific peer groups possible

- Latest insights and recommendations for securing digital organizations
- Selected articles from Cybersecurity experts regarding digital security, among others:
  - Cybersecurity frameworks
  - Open data
  - Privacy
  - Security operations center
  - Cyber stress testing

- Global study about application quality assurance and security testing
- State of quality and trends on outsourcing, technologies, tools and methodologies
- Industry- and region-specific analyses
- Guidance for strong testing units
- Recommendations for automated security testing

- Book about the most recent and relevant Cybersecurity topics
- Focus on dimensions around security organization, management and governance
- Introduction to current developments and their relevance for organizations
- Discussion why and how organizations should tackle security in a different way
- Discussion of risks and trends in industries providing critical infrastructures
- Indication of implications derived from legislations
- Presentation of a pragmatic approach for a security health check
- Industry-specific discussions, e.g. for energy/ utilities or food

- Point of View about Cybersecurity in context of Industry 4.0 and Internet of Things (IoT)
- Discussion of current security situation, challenges and risks from unprotected IoT devices
- Description of specific measures for organizations to improve security of their IoT

- Discussion of trends and requirements in SOC
- Approach for setting up a security operations center
- Considerations of threat intelligence, security monitoring and security response
- Integration of internal and external data for improved monitoring and efficient response to security threats

- Point of View about Cybersecurity in connected cars
- Security relevance for cars as part of the extended organizational network of OEMs
- Holistic view on security aspects as part of interconnected mobility
- Customer trust and competitive advantages based on cybersecurity in connected cars

- Example of a successful implementation of a holistic awareness campaign for a global organization
- Indication of challenges and pitfalls to design and implement effective campaigns
- Discussion of best practices such as risk-driven approach, KPIs or multiplier networks
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.

Learn more about us at

www.de.capgemini-consulting.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.

Learn more about us at

www.de.capgemini.com