Cybersecurity and Privacy Services

Fear Cyber attack?
Attack Cyber fear!

Our Services

With the wide range of information security and cyber security services provided by our professional team, who are experienced, specialised in their fields, solution oriented and can access the best practices promptly as a part of the global network, we help you to ensure information security using the most up-to-date strategies, independent of the context of the information, based on the business priorities of your corporation.

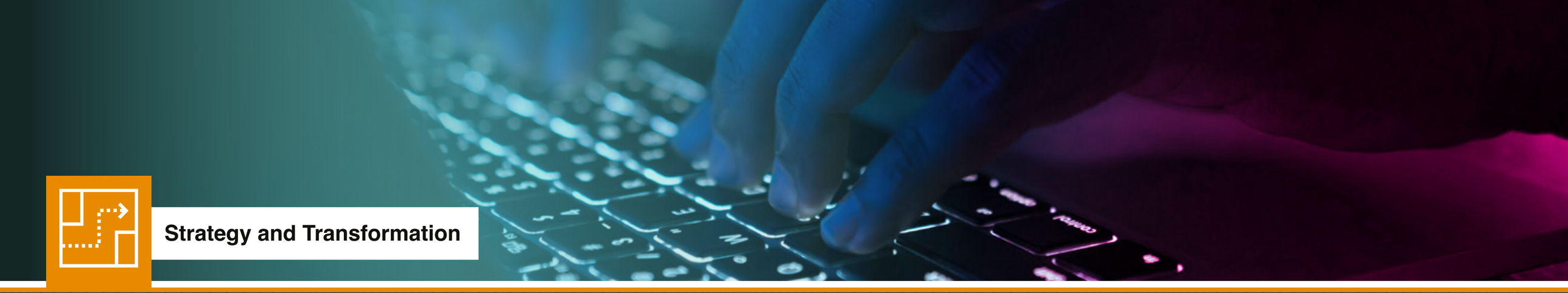
How can we help?

As companies pivot toward a digital business model, exponentially more data is generated and shared among organizations, partners and customers. This digital information has become the lifeblood of today's interconnected business ecosystem and is increasingly valuable to organizations—and to skilled threat actors. Business digitization also has exposed companies to new digital vulnerabilities, making effective cybersecurity and privacy more important than ever.

Contact

Ulvi Cemal Bucak
Cybersecurity and Privacy Leader,
0212 326 6838
cemal.bucak@pwc.com

Özkan Kıvanç
Cybersecurity and Privacy Partner,
0212 326 6886
ozkan.kivanc@pwc.com



Strategy and Transformation

Information Security Strategy

Information security is part of the organization's business culture and should be managed as a whole, in line with business objectives consistent with growth strategies. This strategy should encompass not only the organization itself but also its suppliers and service providers.

Our Services

- Corporate Information Security and Cyber Security Strategy
- Information Security Organization
- Information Security Management System
- Third Party Security Risk Management

Compliance with Regulation & Standarts

Having and keeping your information security quality at a certain level is one of the important factors in providing a trust environment regarding the confidentiality and protection of your critical information.

Compliance with ISO 27001 and PCI-DSS standards has become a legal requirement in some industries. We are at your side with our services for compliance consultancy and compliance audit.

Since we are members of the Information Security Forum, we have the opportunity to determine your institution's level of information security maturity and benchmark it with its counterparts around the world.

Our Services

- Information Security Maturity Evaluation
- ISO 27001 Audit and Consultancy
- PCI-DSS Audit and Consultancy

CISO Support & Development Services

We can help you with your organizational needs with information security outsourcing service or co-sourcing service.

Our Services

- Identifying and reviewing the Information Security framework, promoting information security within the group through awareness sessions
- Identification of Information Security risk assessment activities and related controls, second level review activities (examination of logical and physical access, security in projects, etc.)
- Determining key performance and security indicators (KPI / KRI), measuring them regularly with control tests.
- Daily IT security checks on IT activities (security impacts of change, verification of firewall rules, etc.).

SWIFT Customer Security Program

No need to ask why attackers in the cyber space target money transfer systems. Because money is there! SWIFT Customer Security Program (CSP) is the name given to the security program created by SWIFT for this reason. In 2020, all SWIFT users are required to perform independent audits according to the Customer Security Controls Framework (CSCF).

Our Services

- Current State Assessment According to SWIFT CSCF
- Penetration Testing for SWIFT Systems
- SWIFT CSCF Compliance Consultancy
- SWIFT CSP Compliance Audit

Privacy and Data Protection

Data Protection Services

How can you prevent your most sensitive corporate or personal information from falling into wrong hands?

Information has become the most valuable asset for institutions today, and taking measures to protect it is no longer a choice, it is a must.

Our Services

- Personal Data Protection Law (KVKK) Compliance
- Data Privacy Compliance Assessment
- Data Privacy & Protection Strategy
- Data Classification
- Data Loss Prevention (DLP)

Cybersecurity & Awareness Training

Whose responsibility is information security in an institution?

The answer to this question asked in almost all information security awareness trainings should be “information security is the responsibility of everyone in the institution”. Creating a consistent information security process and ensuring the sustainability of this process can only be achieved with the participation of all employees.

The corporate culture that will keep the awareness level of employees at the highest level is the backbone of sustainable information security.

Our Services

- Game of Threats
- Security Awareness Programs for Corporate and Senior Management
- Information Security Awareness Training
- Personal Data Protection Training
- Phishing Tests
- CISO and CSO Coaching

Game of Threats™

Educating the Board on cyber security threats

PwC’s Game of Threats™ is a unique way to help educate and raise awareness of cyber security - helping organisations experience the key decisions that need to be made during a cyber attack.

What is Game of Threats™?

Game of Threats™ is a head-to-head digital game that simulates the experience of executives when their company is targeted by a cyber attack. During the game, participants play as both attackers and defenders, working against the clock and with limited resources in a race to beat their opponents. Moderators guide the participants about their preferences by making real-time feedback to the participants during the game.

Game of Threats™ challenges participants to make quick, high-impact decisions. It helps them to understand the activities that can make the biggest difference and provides valuable insight into emerging cyber threats.

Scope

To get the most out of a Game of Threats simulation, it is recommended that a session should be held with min. 6 max. 16 participants, session length should be between 150 to 180 minutes, a planning meeting with IT and Cybersecurity management before the session and an evaluation meeting with all the participants a week after the session should be held.

Who should attend?

Company partners, CEO, Board Members, General Manager, Assistant General Managers, Finance Director, Human Resources Leaders, Chief Legal Advisors, Information Technology Directors, Risk Management Leaders, Internal Audit Leaders, Information Security Managers.

Implementation and Operation

Identity and Access Management

Do you manage your digital identity correctly? What about access rights?

With the increasing dependence of technology from accounting systems to production applications, door entry systems to human resources applications, we can say that our identities in the digital world and their access rights on these identities have also gained importance. We can say that institutions with poorly managed identity and access management processes are easy targets for attackers in the digital world.

In order to control the risk of unauthorized use and sharing of your critical information, it is necessary to make sure that the right person within the organization has access to the right information at the right time. For this, it is necessary to design the related processes, and then to automate the processes with the help of applications.

Our services

- Identity and Access Management Maturity Assessment
- Integration of Identity and Access Technologies
- Privileged User Management

Infrastructure and Operation Security

IT infrastructure and operations should have a design suitable for your organization's business priorities. Technology and products selected in accordance with this design should be matured to support the business objectives of the organizaiton and should be managed in the most appropriate way.

Our services

- IT security architecture
- Selection of security technologies and products
- Integration of security products and corporate processes
- Managed security services

Security Architecture

With the increasing dependence on technology and the need to share information both internally and externally, the threat landscape of organizations is also expanding. It requires establishing security controls at all levels of communication to implement the layered security approach, which is one of the most reliable security approaches.

Implementing internal and external network security controls is the first step in protecting organizations' digital assets. After the implementation of these controls, the design and effectiveness of these controls should be tested regularly.

Our services

- Corporate Security Architecture Assessment
- Target Corporate Security Architecture Implementation

Cloud Security

The deployment of cloud technology is no different from the deployment of other IT functions. A good governance model and architecture should be designed and put into place. However, the governance model needs to be feasible and should be designed so as not to undermine the benefits of cloud technology. Using the globally accepted ISO 27017 Cloud Security Information Security Standards, helps reassure both employees and business partners.

Our services

- Cloud Security Assessment and Audit
- ISO 27017 – Cloud Security Consulting

Incident and Threat Management

Threat & Vulnerability Management

If the vulnerabilities in your organization's infrastructure are not detected and remediated before the attackers, security violations may occur, which may lead to reputation and financial losses. By assessing the security of your information technology operation from the perspective of the attackers, you can prevent potential security breaches.

Our Services

- Application security tests
- Penetration tests and social engineering
- Load tests (DDos / DoS)
- Vulnerability and patch management
- Mobile application tests
- Configuration analysis

DDoS/DoS Tests

DDoS / DoS (Denial of Service) attacks are among the most common attack vectors. These attacks negatively affect the lives of both organizations and their customers. With our DDoS testing service, we aim to determine the resistance levels of institutions against possible DDoS attacks. We can perform safe and controlled DDoS tests to assess specific scenarios or network infrastructure.

Attack Vectors

- HTTP Get Flood
- Slowloris
- DNS Query Flood
- SYN Flood
- ACK Flood
- FIN Flood
- UDP Flood
- ICMP Flood
- Functional Web Tests

Security Operations Center

Are you prepared for cyber attacks?

Cyber attacks are one of the biggest risks for organizations in the modern business world. In the event of a possible attack, the continuity of critical business processes is vital for organizations despite this attack. If there is personal data in the systems in such an event, the case takes a completely different dimension.

In the event of a cyber attack, we serve with our experts who can provide technical and legal support. We also assist organizations that want to proactively increase the effectiveness of cyber incident response in preparation and simulation.

Our Services

- Technical and Legal Consultancy in Personal Data Violations
- Cyber Incident Response
- Post-Event Detection and Analysis
- Evaluation and Design of Cyber Incident Response Processes
- Cyber Crisis Management Simulation

Source Code Analysis

How much do you trust the software you use?

Nowadays, with the widespread use of internet and mobile devices, the importance of software security is increasing. Source code analysis must be integrated into the Software Development Life Cycle (SDCL) to ensure software security in your organization, meet compliance requirements by focusing on the right targets, create a continuous control environment, have the appropriate software security features, and have the expected level of assurance by the software development process.

Our Services

- Assessing the Software Development Life Cycle (SDLC) and determining the improvement areas
- Reviewing your existing software and identifying vulnerabilities with Source Code Analysis
- Adapting the Source Code Analysis tools and creating a continuous control environment by integrating it with the Software Development Life Cycle (SDLC)
- Analysis of static source codes without the need for separate systems for your software on different platforms (Windows, Android, IOS, Linux, etc.)
- Scanning projects that have not reached the compile level (Continuous Integration)
- With the feature of scanning only changed codes (three previous and three next), optimizing scan times without needing to re-scan the entire project (Incremental Scan)
- Quick and easy customization of security queries with object-based script language
- Integrated tools supporting large numbers of vulnerabilities

2020-0215