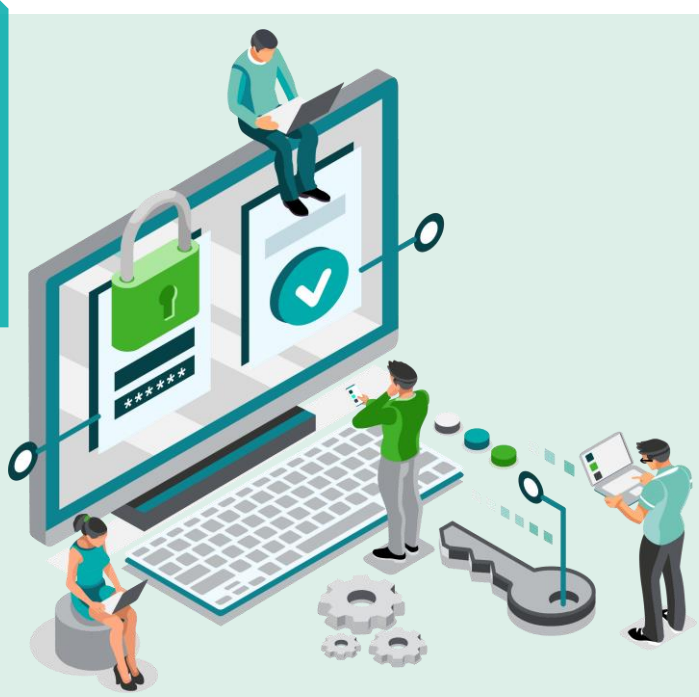
Deloitte.

Chief Information Security Officer as a Service

Cyber everywhere. Innovate anywhere.

August 2020

The evolving face of cybersecurity and transformational role of the Chief Information Security Officer (CISO)



In July 2019, the personal details of about 106 million individuals across the US and Canada were stolen from a leading financial services firm. It was later reported that the firm had replaced its CISO since 2017, with the company's CIO, while it looked for a full-time replacement. The company in a statement mentioned that it expects the incident to cost them hundreds of dollars- mainly for customer notifications, credit monitoring and legal support- in 2019 alone.

The Chief Information Security Officer's (CISO) position has become critical, especially in managing enterprise risk, deploying security analytics, and minimising the financial, reputational or compliance risks that may arise from a data breach. However, as the scale and seriousness of cyber threats being faced by businesses has evolved, so has the role of the new-age CISO. It has elevated beyond the technical cyber proficiency of one person, to articulating solutions from a business perspective by making cybersecurity a board-level conversation.

CISOs have a vital role to play as the catalyst for achieving top-level engagement by making cybersecurity business-relevant to the top management. Organisations with cyber-committed CEOs, CIOs and boards can better manage cyber-risk, better protect against cyberattacks, and better leverage cybersecurity for strategic opportunities.

Better engagement and threat response readiness at the CEO and board level requires CISOs to become more strategic in their board communications and interactions, eventually managing risk and minimising the attack and risk surface. They are also required to control the regulatory requirement well, and succeed in the attaining a desirable security posture.

The challenges of a traditional CISO

Decision-makers understand the increased focus on cybersecurity, and are keen to hire a CISO and set up a team dedicated to the information security of their enterprise. Cybersecurity is now being dealt with higher up the corporate ladder, with the CISO being viewed as a business partner and not just a business protector. CISOs of an organisation recognise they can benefit from constant upskilling, greater focus on strategy, and greater executive interaction, but they face several obstacles in their attempts to get these initiatives rolling. Let us explore some data from the Deloitte Review on the new CISO, to understand the barriers traditional CISOs most commonly face when building a more proactive and business-aligned security organisation:

01

Over 90 percent of CISOs hope to improve the alignment between the security organisation and the business, yet nearly half (46 percent) fear the inability to accomplish that alignment. This misalignment between the security goals and organisational objectives results in poor cybersecurity maturity.

02

Only 22 percent of respondents work in an organisation where the CISO reports directly to the CEO, while 40 percent still report to the CIO. This has the potential to reduce the strategic impact and independence of their decisions.

03

Only 18 percent of CISOs have held managerial roles before moving into security organisation. Since most are technologists by training and trade, the individuals will be more focused on operations, tactical moves and managing compliance, rather than focusing on the maturity of the cyber-security graph of the organisation.

These challenges pose an important question for decision-makers, 'Should my enterprise hire a resource to manage information security, or would it be more prudent to opt for a team of external experts as a service that can navigate their way through this complex and evolving role?'

Chief Information Security Officer as a Service (CISOaaS)

CISO Mind Map: Immersive role of the CISO

CISO'S ARENA: The role of the CISO is a multidimensional, immersive one that faces accountability from several pillars within an enterprise. A CISO is required to not only possess technical expertise, but also have the strategic outlook to drive security-oriented business decisions. They have to understand and adapt to the cyber culture of an organisation, and have the experience to guide it through a breach with resilience. The MindMap of the CISO illustrates the expansive and complex role that a CISO is expected to perform:

Business Enablement

Merger/Acquisition
- Acquisition Risk Management
- Integration Cost
- Identity Management

Cloud
- CSP Evaluation - Security
- Secure Cloud Architecture
- Strategy and Guidelines
- Cloud Risk Evaluation
- Compliance
- Ownership/Liability/Incidents
- SaaS Strategy
- Log integration

SMAC Technology
- Policy
- Technology
- Lost/stolen devices
- BYOD
- Mobile Apps Inventory

Process
- HR on boarding/ termination
- Business Partnerships

Identity Governance & Management

- Provisioning and De provisioning
- Single Sign on (SSO, Simplified Sign On)
- Repository (LDAP/Active Directory)
- Federation
- 2-Factor Authentication
- Role-based Access Control
- Ecommerce and Mobile Apps
- Password resets/Self Service
- HR Process Integration
- Integrating cloud-based identities

GRC - Governance Risk and Compliance

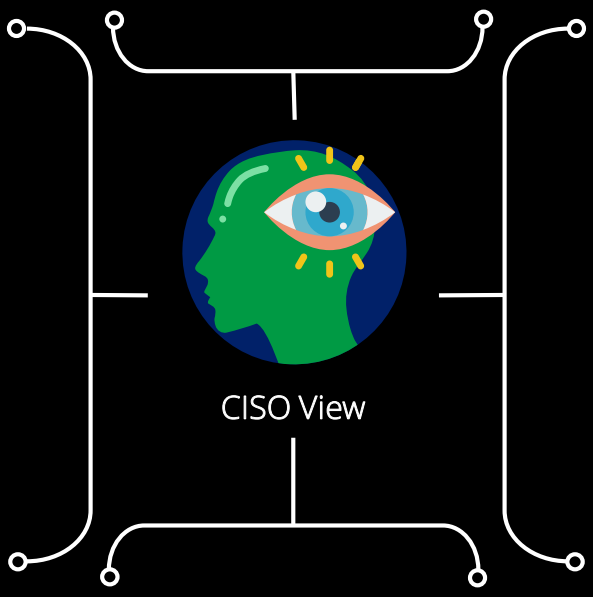
- Strategy & Business Alignment
- Risk management framework
- Resource Management
- Role and Responsibilities
- Metrics and Reporting

Selling InfoSec (Internal)

- Aligning with Corporate Objectives
- Continuous Management Updates
- Innovation and Value Creation

Technology and Ops Risk

- Physical Security
- Vulnerability Management
- Ongoing risk Assessments/Pam testing
- Integration to project Delivery (PMD)
- Code Reviews
- Risk Assessments Methodology
- Policies and Procedures
- Associate Awareness
- IoT Technologies
- Operational Continuity



Security Budget

- Security Projects
- Business Case Development ROSI
- Alignment with IT Projects
- FTE and Contractors
- Balancing Budget for People Training and Tools/ Technology

Projects

- Requirements
- Design
- Security Testing
- Certification and Accreditation

Cyber Fusion

Threat Prevention
- Network/Application Firewall
- Vulnerability Management
- Application Security
- Identity Management
- Information Security Policy
- DLP/EDR
- Anti Malware, Anti-Spam
- Proxy/Content Filtering
- Patching
- DDoS Protection
- Hardening guidelines
- Desktop Security
- Encryption SSL
- PKI

Threat Detection
- Log Analysis/ Correlation/SIEM
- Altering (IDS/IPS,FIM, WAF, Antivirus, etc.)
- Net Flow analysis
- DLP
- Threat hunting
- MSSP Integration
- SOC Operation

Security Incident Management
- Incident Response
- Media Relations
- Incident Readiness
- Forensic Investigation
- Data Breach Preparation

Security Architecture & Engg

- Network Segmentation
- Application Protection
- DevSecOps
- Defence-in-depth
- Remote Access
- Encryption Technologies
- Backup/Replication/Multiple Sites
- Cloud/Hybrid/ Multiple Cloud Vendors

Compliance and Audits

- PCI
- SOX
- SOC2
- ISO
- HIPAA
- Regulatory Exams
- FEDRAMP
- GDPR/CCPA

Legal & Human Resources

- Data Discovery
- Vendor Contracts
- Investigations/Forensics
- Integrating into IDM Process

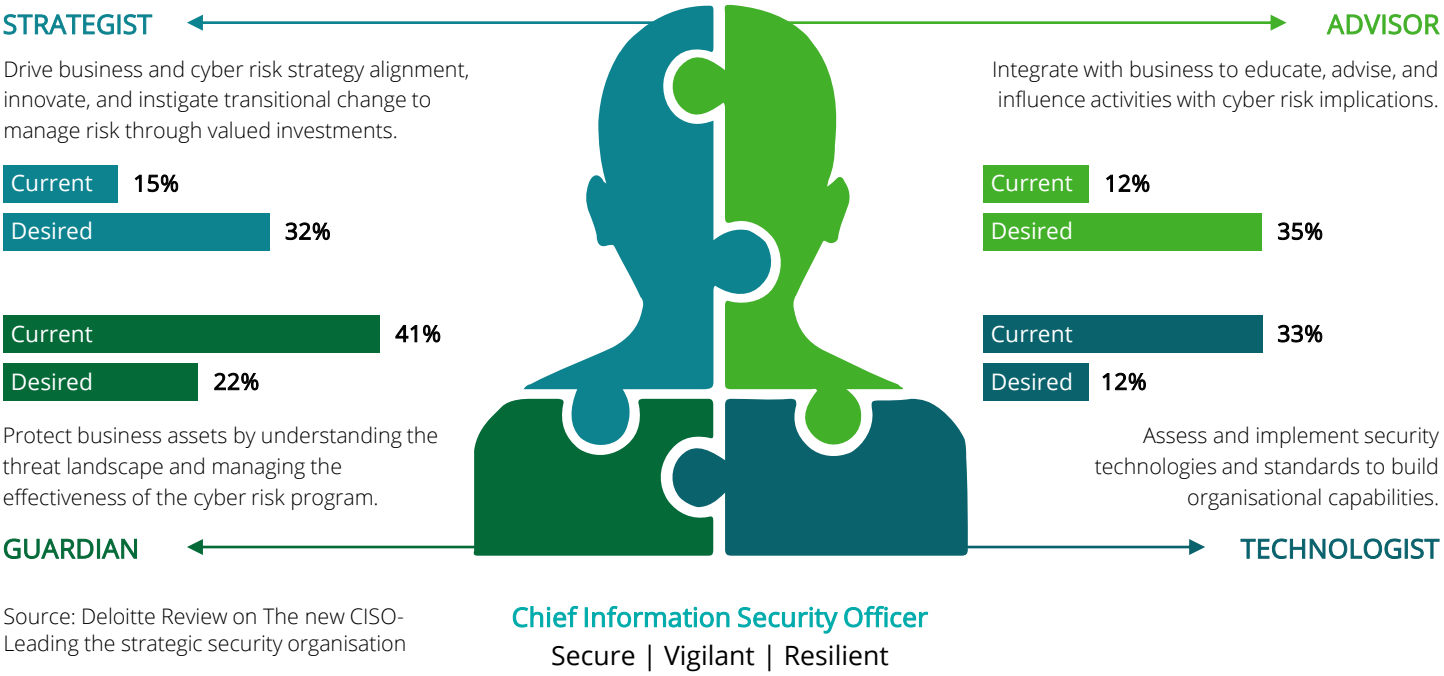
Introducing Deloitte's Chief Information Security Officer as a service offering

CISOaaS is a new-age holistic solution that brings in experienced practitioners who add leadership, value and commitment to your organisation's information security. Opting for CISOaaS provides you with access to a vast pool of industry experts, strategic frameworks that fit the requirements of your enterprise and the requisite tools to execute and measure the outcome of these frameworks. This extension to your information security capabilities will fulfil the immersive role of a CISO and ensure that risks are mitigated before they can cause unacceptable business losses.

The CISO's role has evolved from being an afterthought to being at the forefront of today's digitally disrupted and focused business acumen. In response to this disruption, Deloitte has increased the value in the depth and breadth of CISO service.

The CISOaaS system balances challenges and priorities' under the 'four-face' model, mainly: technologist, guardian, advisor and strategist.

The four faces of the CISO



Source: Deloitte Review on The new CISO- Leading the strategic security organisation

Chief Information Security Officer
Secure | Vigilant | Resilient

From scoping and strategising to implementation, here is how the four-face model of the DNA of our service manages the complete portfolio:

- Provides a ready set-up of a CISO with their entire team of experts having in-depth knowledge across domains.
- Puts together an information security strategy, ensuring that the basics are implemented and maintained. Reduces risks and raises the maturity of information security via a clear outlined roadmap of secure principles.
- Helps an organisation identify its current information security maturity, the threat landscape, what needs to be protected and the level of protection required, as well as the regulatory requirements it needs to meet.
- Provides the organisation with a cost-effective way of maintaining information security systems and managing risks

The CISOaaS service can be customised to meet the requirements of small, medium and large enterprises. A thorough assessment of your organisational requirements enables us to understand which offering will suit you the best. We then propose a tailored solution created by combining our various modes of engagement and delivery options.

The various modes of engagement of the CISOaaS are elaborated upon, below. These can be delivered through the model that best suits your needs, from the Team, Project-based and Strategic options.

Modes of engagement

BOARD
Assess and advise

Communicates directly with the board to asses the current cybersecurity maturity of the enterprise and advises on frameworks to be adopted. Suggests and implements practices that solve specific problems within a defined timeline

FULL TIME
Dedicated, focused CISO

Manages all your cyber security requirements from the start to the end of the journey via a dedicated team of experts in various domains

INTERIM
Transitional CISO

Typically follows a lean model by temporarily fulfilling certain, specific requirements that may arise during the transition phase. Reduces the learning curve considerably via seasoned professionals who have a prior understanding of the business objective

VIRTUAL
Virtual dedicated – Strategic deliverables

Provides strategic deliverables and solutions via a virtual dedicated advisor who is unbiased and experienced

DELIVERY APPROACH

TEAM APPROACH

Organisations may ask our CISOaaS to provide a team of specialists to handle security activities around tasks such as DLP, policy framework, overall security and application layers. The customer is less worried about the team's skills, as the virtual CISO is the point of contact.

PROJECT-BASED

Enterprises opt for a project leader who works with the CIO to handle multiple layers of security - the network, applications, data, Identity and access management, as well as people and processes to design a security process and manage it for a stipulated period.

STRATEGIST

This third model (gaining prominence in the new norm) is about moving from a people-centric model. CEOs assign the virtual CISO with the task of understanding the enterprise risk. For example, the virtual CISO here is expected to conduct a top 10 risk-based study to establish the risk posture of an organisation. The virtual CISO then helps create a security structure, and helps deploy a known baseline framework.

Our service framework

Deloitte's CISOaaS framework is the optimum amalgamation of strategic and tactical CISO responsibilities, along with capabilities outlined in Deloitte's CSF that drive the security of an organisation. It follows a three-pronged approach of understanding the organisation's maturity levels, identifying and anticipating potential threats and executing comprehensive solutions to overcome these threats.

KNOW THYSELF

Comprehensive business focused security risk and exposure assessment

Provides a range of solutions from Cyber Immunity Assessment to execution of Internal Risk Assessments.

KNOW THE ENEMY

Customised assessments to identify relevant cyber threats

Includes technology and processes from Threat Assessment and Analysis to Security Architecture and Design.

ADAPT AND OUTSMART

Prioritised, intelligent and actionable plans to cost-effectively drive programme inception and maturity

Creates not only the function and operating model based on the defined agile cybersecurity strategy but also delivers precise rapid response and readiness to outpace modern attacks.

CISOaaS and your enterprise

A CISOaaS model provides subject matter experts that allow your organisation to cost-effectively access their strategic security experience and technical skills. This will enable you to leverage the wide range of experiences, solutions, and skill sets we have invested in, without the added capital expenditure to a traditional CISO model.

While CISOaaS is cost-efficient, its flexible and scalable on-demand nature also provides a host of benefits:

01 Access a pool of experienced, specialised, senior cyber security professionals

02 Access resources quickly and eliminate the need to attract and retain talent

03 Lower your costs by only paying for the support required

04 Cleary define cyber and information strategy with a roadmap

05 Gain experience to educate and present to all types of senior executives, board members and non-technical senior staff

06 Secure cross-business support and achieve your information security goals

CONTACTS

ROHIT MAHAJAN
President, Risk Advisory
rmahajan@deloitte.com

DEEPA SESHADRI
Partner, Risk Advisory
deseshadri@deloitte.com

VIKAS RAINA
Associate Director, Risk Advisory
viraina@deloitte.com

Regional

North and East

GAUTAM KAPOOR
Partner, Risk Advisory
gkapoor@deloitte.com

South

GAURAV SHUKLA
Partner, Risk Advisory
shuklagaurav@deloitte.com

West

ASHISH SHARMA
Partner, Risk Advisory
sashish@deloitte.com

Deloitte.