Capgemini

Future Role of the CISO

Basement or Boardroom?

Research and Analysis by

IDC
Analyze the Future

Security Transformation Road Maps

Overview

This research, developed by IDC and commissioned by Capgemini, positively shift the perception of security among stakeholders by building on insight gained through 1,000 interviews with IT and business senior leadership across the U.K., France, the Netherlands, the U.S., Germany, Australia, China, India, Japan, and Singapore.

The research highlighted how the role of the CISO and the way in which they are perceived by the business is changing. This road map shows how CISOs, business managers, and transformation leaders can build on that change in perception and establish security as a business enabler.

Based on the research, IDC has identified eight key attributes/ themes for the contemporary CISO role as follows:

- **Risk oriented -** engagement with business over common metrics -> risk
- **Trust enabler -** guarantee digital trust in transformation
- **Relationship builder -** bring together stakeholders to form a shared vision
- **Financial acumen -** know and show the value of money invested
- **Communicator -** be the voice of security that is understood by others
- **Overseer -** enforce and control policy that evolves with business
- **Technically competent -** comprehension is key for interpretation for non-techies
- **Crisis handler -** increase the focus on the response side of security

Content

CEOs and Business Leaders

Securing Business Strategy

Phase 1 Security Strategy by Design & Default

From Security Issues …

- If security is not bound up with the process of Digital Transformation (DX) you open your business up to substantial financial and reputational risks.
- Security delays reduce flexibility, introduce inefficiency, undermine agility, and impact speed to market.
- If security does not keep pace with the modern transforming business, it will hold change and progress back, resulting in digital deadlock.

… to Security Outcomes

- Security enabled at the beginning of the transformation results in higher levels of success. Security by design is considered the key DX element by 57% of organizations.
- Innovation processes with security at their core will incubate and scale far more effectively.
- Wastage and costs from failed projects are reduced, and impacts on business risks mitigated.
- A change in the way security is viewed as a business enabler leads to improved competitive advantage and shareholder value.

The digital strategy of your organization must include security as a milestone

Approach strategy with security as an embedded part of the planning process. It is your responsibility to make this a reality.

Treat security as an enabler and involve the security function earlier in the process to reduce risk and increase efficiencies in process.

Bring the CISO function higher up the decision-making process and embed them in all strategic decision-making activity.

Define a Blueprint for Success

Phase 2 **Build** the **Plan** for **Security**

Security Alignment for DX

Define and formalize the role security should play in all processes, functions, and initiatives, such as DX. Demonstrate that business and security are on the same page with the same goals.

Endorse Security Change

Formalize and strengthen the role of security in the governance structure. Communicate the enhanced role of security with senior stakeholders. Ensure they are supported in their transformation.

Empower the Security Function

Ensure your security function has the right skills and language to hold the conversations needed to change perception and role. Support them by providing a sufficient level of authority.

Formalize Security Change

Failures in security are hugely impactful on the business. Instil the need for change, the process of change, and the implications of not going through this — financial and reputational.

Evangelize Security as Risk Mitigation

Phase 3 Bring Security into Constant Board Discussion

Risk Mitigation Becomes a Core Function

Communicate the progressive role of security in the overarching business strategy in the context of risk mitigation.

Highlight and support outcomes and business advantages.

Change the Measures of Security

Determine business-relevant security and performance metrics and KPIs. Empower all functions to track and report these.

Shift security KPIs and traditional measures of security to align with those of the wider business.

Enshrine Security in Business Process

Bring security in early as part of the business strategy and transformative process.

Be the one that forces security by design and by default into all business activities and processes.

Define the Future-Fit CISOs

Ensure you have a CISO in place that can address these issues, speak the business language (or create a function that can for them on a day-to-day basis) and understand mitigating risk, not just tech and back office.

DRIVE PROGRESS

Demonstrate progress by empowering wins to develop and maintain momentum and create sticky change. Do not let this issue drop from consciousness.

Do not rest. Build on Security change

Phase 4 Empower Security to Continue to Evolve

Do Not Rest!

Prevent your organization from "snapping back" to old habits. Empower change and "unlearn" all ways of working.

Ingrain security into the business and promote the development of process and training for all employees, partners, and ecosystem players.

Actively drive to improve engagement and functionality of security in the context of risk mitigation and the need for change.

Embed Security as Business Enabler

Embed security change in the processes of the business. Think about compliance as an example of how well some things are addressed and whether security meets this standard.

Encourage and mandate collaboration. Measure and target departments and individuals on collaborative working and on security involvement.

Focus collaboration on speed to market, agility, cost efficiency, and productivity — all balanced against risk — as the future security role.

Security Supports Wider Ambitions

Support your security function moving to automation and selective outsourcing, allowing staff to focus on essential business outcomes.

Enable security teams to become focused on strategic value and added-value tasks and outputs.

Empower your CISO or security lead, to become a strategic function. Support them in becoming a go-to source of strategic input to change and transformation initiatives.

Think of …

Employing security by design and default as an organizational principle, not a formal "tick-box" exercise

Endorsing and advocating security change across the organization's stakeholders to ensure change "stickiness"

Using security as a value-added component to your services and products to harness digital trust

Digital and Transformational LEADERS

Security as an Enabler of Transformation

Phase 1 Security Strategy by Design & Default

From the Burning Platform

- By lowering the priority of security in DX and prioritizing change, you open your business up to substantial risks as well as additional cost.
- The lack of dialog with security during the blueprinting stages will most likely cause frustration and holdups/rollbacks in the implementation phase.
- DX drives the deperemiterization of enterprise with cloud, IoT, and extended ecosystem supply chains, risking the initiative survival.

…to the Promised Land

- Transformational initiatives backed by security have greater chances of delivering change and value for the enterprise.
- Security implemented at the core of digital platform and processes accelerates agile implementations, reduces time-to-market, and increases the flexibility of entire operations.
- Security-by-design as a strategic imperative in the long run will support rollout of new DX initiatives, and provide guidance and guardrails for innovation.

Security is an essential baseline for the organization's digital transformation strategy

Engage into communication with security and build a strategy to support cross-functional collaboration underpinned by business objectives.

Treat security as an enabler and involve the security function earlier in the process to reduce risks and increase efficiencies in process.

Assess DX objectives in terms of potential risks and work collaboratively on making the core of the transformation future-proof.

Define A Blueprint For Success

Phase 2
Build the Framework for Secure Transformation

Alignment & Coalition

Define and formalize the role security should play in all processes, functions, and initiatives within the enterprise DX strategy. Establish a use-case-driven engagement framework.

Communicate Change

Jointly communicate with all C-level and senior staff that security and the business are aligned and working towards a common business aim.

Ensure Security Engagement

Support security transformation within strategic initiatives through co-innovation and by establishing feedback loops and a “champions” network across DX and security domains.

Innovation

Reposition (if required) or reinforce that security is essential to innovation and progress as a core strategic priority of the business.

Build Security Change Into Transformation

Phase 3 Enable Security to Support Continual Change

Communicate Vision & Advantage

Clearly stated vision of DX for an enterprise should highlight the role of security as the provider of trust for both internal initiatives and third-party interactions.

Change Measures of Security

Transformation alters traditional processes and architecture. The new deperimeterized environment requires altering the risk assessment framework, functional stack, and the model of interaction between security and DX.

Embed Security in the Business Process

IT governance for enterprises in transformation admittedly gets overly complex, which generates gaps. Reducing the risk and avoiding digital deadlock requires business-aware and -aligned security.

Evangelize Security

Be the change you want to see — becoming chief security evangelist to spread the word and harness the security-aware behavior both inside and outside your organization.

Demonstrate Progress

Demonstrate progress through unrestricted innovation that maintains momentum and creates sticky change without restraints.

Security Change Must Be Continuous

Phase 4 Empower Security to Continue to Evolve

Do Not Rest!

As an advocate of change your role is to support and guide the change across all enterprise domains. Security as a business enabler should underpin the change process.

Share agile best practices across security and technology domains to streamline and automate for evolving business demands and a dynamic threat landscape.

Involve security in shaping the digital strategy to give an impetus for its transformation in line with requirements of DX enterprise.

Embed Security as Business Enabler

Embed security change in the processes of the business. Think about compliance as an example of how well some things are addressed and whether security meets this standard.

Encourage and mandate collaboration. Measure and target departments and individuals on collaborative working and on security involvement.

Focus collaboration on speed to market, agility, cost efficiency, and productivity — all balanced against risk — as the future security role.

Security Outcomes

Support your security function moving to automation and selective outsourcing, allowing staff to focus on essential business outcomes.

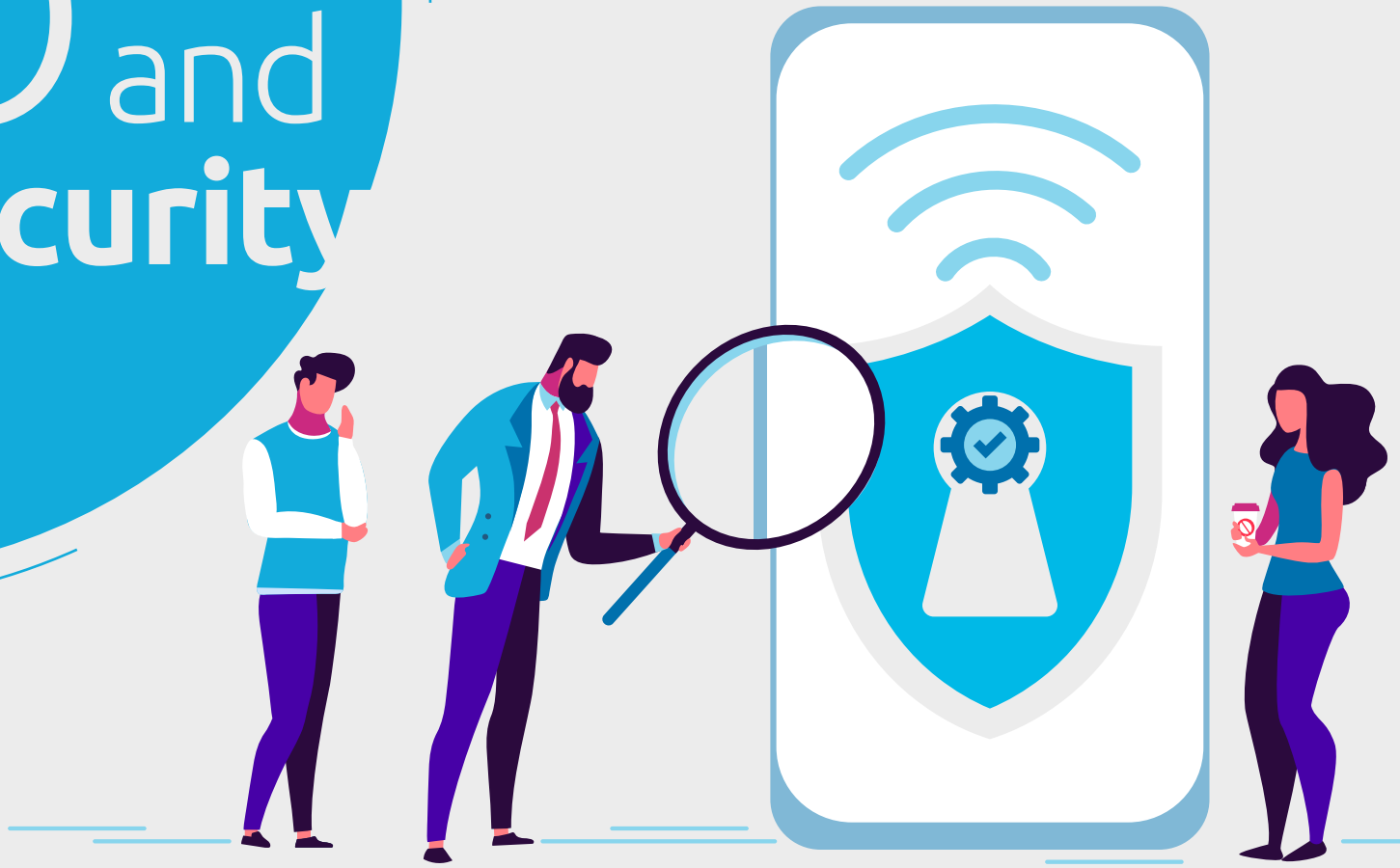
Adding flexibility to the security function you change the supply chain of trust in the organization to seamless, timely, value-focused delivery.

Support the changing role of the CISO by providing access to broader resources and embedding security into DX strategy as an advisor and facilitator of change.

Think of …

1. Putting digital trust as a cornerstone for building services, products, and initiatives
2. Supporting and advocating the automation and integration of security into processes across the organization
3. Supporting a collaborative spirit for organization wide security transformation by empowering champions

CISO and Cybersecurity Leaders



Reinforce The Platform For Change

Phase 1 Business Security Strategy by Design & Default

Move perception from …

- Security is involved far too late in the process and as a result risks becoming a barrier to change and transformation.
- This restricts an organization's ability to become agile and flexible, slows progress, and in turn diminishes the role and perception of security.Security as a blocker restricts innovation, creativity, and progress.
- As a consequence, shadow IT rises and increases the risk of stakeholders circumventing best practice.

… and move towards

- Engaging security at the start of transformation processes or strategic initiatives where it will have the biggest impact.
- Security must be involved early on, with appropriate authority, seniority, and measurement.
- Empowering the overall business strategy by shifting security to the left of the business strategy process (in planning, execution, and new initiatives).
- This means: security by design and default.

Security must be an integral component, spanning key areas of the digital strategy of your organization as a prerequisite and measurement of success

Place security as a stakeholder and contributor, not as a tick box, by involving it early in business decision making as well as strategic and digital initiatives.

Drive greater security collaboration and involvement in strategic decisions in order to rise the CISO function up through the business.

Avoid a downward spiral where security comes late to the party and tells everyone why something won't work. Change perceptions!

Blueprint For Success Across Functions

Phase 2 Build the Plan for Security Transformation

Alignment & Empowerment

To achieve this, you need alignment across the functions of the business and within the C-Level. Frame the security agenda along business risks and opportunities, not technical solutions.

Strategic Leadership & Communication

Drive and invest in buy-in and awareness, as well as highlighting successes and business enablement. Encourage feedback and act on it. CISOs must help themselves to establish their position on the board.

Business Language & Business Bias

Develop the business skills/language in security to support the transformation. Start talking their language and show willingness. Actively become a business function, delivering business value.

Coalition Across Business Functions

Build a strong cohort of supporters and evangelists across functions. Develop a network of influencers across the business. Aim at becoming part of the powerbase for business ecosystem change.

Empower Security Within Wider Business

Phase 3 Lead Security Change Across the Organization

Create Formal Security Program Leads

Formalized security roles that act as the business interface. They bridge the functions to ensure alignment and understanding by bringing back business cases for security to implement.

Align Security Metrics & KPIs with Business

Determine business-relevant security and performance metrics and KPIs. Track and report these via dashboards, not as threat detection and vulnerabilities, but as business KPIs and outcomes (time, cost, NPS, etc.).

Distribute Security Responsibility

Define security roles within the program and business unit leads. Disseminate security responsibility.

Define roles and responsibilities AND show the positive impact on compliance, governance and ultimately business value.

Define the Security Role for your Sector

Evangelize the broader role of security specific to your sector and its business dynamics.

Demonstrate the wider risks and risk-mitigation that needs to happen within that sector and the impact this will have on business in the future.

Demonstrate Progress

Demonstrate progress through small wins to develop and maintain momentum and create sticky change and prevent backward steps. Consider assembling Tiger teams to drive the change and prove the concept faster.

Drive Business Value From Security Change

Phase 4 Show Security Change as an Investment in Value

Security Evolution

Benchmark your capability against peer organizations within the performance context to demonstrate the impact and your effectiveness.

Focus on targets and achievements. Balance technical security KPIs and metrics with relevant business metrics. Demonstrate and communicate the causal links.

Continue to demonstrate the role of security in delivering competitive advantage and shareholder value. Show the impact of security on cost mitigation and successful DX.

Business Alignment

Continue to focus your efforts on mitigating risk outlined in digital and business strategies. Perform horizon alignment to support and influence longer-term enterprise strategy.

Drive, encourage, and enable greater collaboration between the security function and business departments. Build security capability within LOBs.

Focus your efforts and language on key business metrics and outcome-oriented goals: speed to market, agility, cost, productivity, NPS, etc.

Building Digital Trust

Automate and outsource low value-add routines to focus on activities strategic for business, as well as to standardize and unify approaches across the enterprise.

By blending security into enterprise governance, ensure you are building resilience through awareness and operational excellence.

Aim to become a strategic function of the business and a go-to source of business-enablement and strategic input, not the last to know.

Think of …

Formalizing the security program and integrating it with the overall governance framework

Distributing security liability to corporate stakeholders enabling them to evaluate and accept risks in support of business strategy

Building business connections with the set of cross-functional KPIs that blend security and other functions' responsibilities

How does **Covid-19** affect **Security?**

As the world comes to terms with a new reality amid the Covid-19 pandemic, the focus on security has never been higher. In the short term, the increase in remote working has accelerated identity management, reliance on VPNs, and a ratcheting of cloud-based delivery. But the impact of Covid-19 outlasts the immediate rises in security tooling.

For CEOs and Business Leaders, the priority must always be to secure their business and their employees. An increase in exposure results from remote working and increased cloud usage, where users, apps, and data sit (probably permanently) outside your organization's perimeter. The volume of attacks from opportunistic attackers in the pandemic's early days will persist as a long tail of vulnerable firms provide a rich feeding ground for the nefarious actor.

In the short term, organizations need to focus first on business survival and then RoI as they slide into slowdown. But as the economy stabilizes attention turns to business resilience and, eventually, acceleration back to growth. The security of your business should be at the heart of each of these phases.

For Digital and Transformational Leaders, this is a great time to stress-test your DX programs. How truly digital are they? Paper trails and manual processes don't translate to remote working and social distancing. Can you use the prolonging situation to accelerate your DX initiatives? Moving faster to digital business models could create competitive advantage, allowing you to stretch away from rivals.

Baked-in security capability allows DX approaches to be deployed quickly but safely. Get ready to apply DX techniques to new, but perhaps more mundane, business processes. Securing an ERP system for remote access or a warehousing app for automation may not be transformative, but it makes security integral to the business.

For CISOs and Cybersecurity Leaders, Covid-19 makes remote working and cloud usage BAU. The perimeter is dead. We'll never go back. We need to learn to live with it.

Security was always the enabler of the business — and now you have evidence. You'll look back in ten years and laugh at how businesses insisted on having staff in the office and apps in an on-premises datacenter.

Not only is cloud being used to host apps and data, it's also being deployed to host security capability itself. Security as an outcome is distinct from the location from which it is consumed. The resilience of the security operation itself is in sharp focus, so ensure your processes are updated to reflect the new way of securing business.

Finally..., a word on Trust. Security has trust at its roots. But other business operations have also shown that trust is central, including customer experience, human capital management, and finance. Covid-19 presents an opportunity to pull these various business units together under a "trust purpose," the effect of which will persist in your organization for a decade.

People matter, results count.

About Capgemini

Capgemini is a global leader in consulting, digital transformation, technology and engineering services. The Group 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. Today, it is a multicultural company of 270,000 team members in almost 50 countries. With Altran, the Group reported 2019 combined revenues of €17billion.

Visit us at

www.capgemini.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,100 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG), the world's leading tech media, data and marketing services company.

To learn more about IDC, please visit

www.idc.com

For more details contact:

cybersecurity.in@capgemini.com