imagine your future®

THE CISO AS A BUSINESS ENABLER

Transforming Security into a Competitive Advantage

Andreas Dietrich

ISG WHITE PAPER

INTRODUCTION

The modern enterprise is experiencing constant change. New digital technologies like big data, artificial intelligence, machine learning and multi-cloud environments provide new opportunities and challenges to the established role of the chief information security officer (CISO), requiring a transformation of this role.

The CISO in the digital age will be a role that embraces change and new business opportunities by shifting from a protective “detect and respond” model to a business-driven “predict and prevent” model. In this new way of thinking, the CISO will enable new business opportunities and explore new business models with the help of digital technologies that transform companies into agile enterprises.

✓

The CISO role should enable new business opportunities.

CISO's can meet these challenges by building and harnessing the power of alliances in the business organization, shifting the security organization into a pro-active provider of directly integrated, consumable solutions and using tools with proactive and predictive capabilities to act on threats before they affect the organization.

ISG, a leading global technology research and advisory firm, can help companies, CISO's and their security organizations meet these challenges and transform into business enablers.

Traditional Understanding of the CISO Role: Control and Check

The CISO is typically known as a rather responsive role primarily focusing on reacting to threat potentials and incidents. **Wikipedia defines the CISO** as follows:

“A CISO is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. The CISO directs staff in identifying, developing, implementing, and maintaining processes across the enterprise to reduce information and information technology (IT) risks.

They **respond to incidents**, establish appropriate **standards and controls**, manage security technologies, and direct the establishment and implementation of **policies and procedures**. The CISO is also usually responsible for information-related **compliance** (e.g., supervises the implementation to achieve ISO/IEC 27001 **certification** for an entity or a part of it).”

According to digitalguardian.com, 59 percent of CISO's have an IT background and only eight percent have a business background.

This leads to a situation in which the CISO, until recently, focused on protecting the perimeter, managing security by using policies and controls, and focusing on a responsive behavior.

Additionally, in companies that use operational technology (OT) for production or manufacturing, CISO's rarely integrate both the IT and OT worlds because OT is typically driven by a "safety first" paradigm, with the goal of keeping production uninterrupted.

✓

Traditionally, CISO's focus on the protection of the perimeter from an IT point of view.

When looking at the CISO role from a business perspective, security is often perceived as an inhibitor or disabler to innovation and change. The phrase, "this is not allowed because of security requirements," is used regularly by traditional security organizations to block changes to the existing infrastructure. Consequently, projects are stopped, or features are stripped down.

Digitization and Connected Everything: A Changed World

When compared to today's security requirements, the easy answer to the question, "What has changed?" is simple: everything.

With today's digitization impacting our everyday lives, even companies that operated with an analog-only approach are faced with customers or new employees aiming to embrace a digital user experience and need to digitize their business models.

This leads to an ever-growing amount of data. Business models are increasingly relying on information derived from analyzing mass data. Likewise, with this change, the role of the CISO is changing. Governments are passing new data privacy and protection regulations, and data and information are becoming a far more important business asset that needs to be protected. This data also needs to be available for integration and consumption, and this integration spans across the entire lifecycle, from the customer to the company's backend systems and back to the customer.

In production and manufacturing, most companies strive toward an integration of their IT and OT to leverage business value and enable digital manufacturing models that integrate customer and business applications with the manufacturing process. This integration also has a significant effect on the role of the CISO. The need to protect these integrations goes beyond yesterday's plan to "just separate IT and OT" toward a protective model that integrates both worlds.

In this changed world, protecting the assets by saying, "we cannot do this," is not feasible anymore. Security needs to proactively find solutions that can enable today's businesses to leverage all these possible integrations and be an integral part of the value creation chain and not just a quality gate keeper.

A proactive approach to security is required.

Transforming the CISO into a Business Enabler

The CISO must strive to:

- Enable entry into new markets that are heavily regulated and require extensive security measures
- Enable market entry into new regions or countries that have severe security or data privacy requirements
- Use new digital technologies like analytics or cloud computing for process automation and improving user experience
- Establish a company reputation based on quality, data protection and security

The key question for the CISO is therefore: "How can I shift my security organization from applying a prohibit and control perspective to being a predictor and enabler while still retaining a high level of protection?" The following sections explore people, processes, and tools to provide initial answers to this question.

People: The Organizational Aspect

The biggest impact a CISO can have is to break up the silos in the security organization. There are two approaches of breaking up the silos: first, the top-down approach of finding meaningful alliances within the larger context of the organization, and second, the bottom-up approach of enabling networks of the people across organizational boundaries.

When forming meaningful alliances there are three questions to be answered:

1. How did the targeted role behave so far?
2. How does the targeted role have to behave in the changed world?
3. How can the CISO help that role act as an enabler?

The chief digital officer (CDO), chief technical officer (CTO) and chief executive officer (CEO) are focused on innovation. To ally with these roles, the CISO needs to showcase what security can do to penetrate new markets, leverage new technologies and grow emerging ideas. This means the security organization needs to develop thought models on how to innovate in the security space and how to improve implementation speed. Helping these three roles as part of an alliance means exploring what is possible and not why something is off limits.

People, processes and tools support the transformation journey.

The chief financial officer's (CFO) role is very similar to the CISO's: in many cases, this role used to be a watchdog and was perceived more as a disabler than an enabler. In times of digital transformation, this role and the corresponding financial models have changed from a fixed annual budgeting plan to **lean budgets that focus on enabling innovation**. So the main contribution the CISO can provide to the CFO is to ensure that all the security considerations are already included in ever-changing projects and that the CISO will not arrive at some point with additional unexpected requirements and security controls. The CISO also can ally with the CFO to make sure that investments are paying off and do not incur later debts in terms of attacks or the inability to penetrate a certain market because of failed regulatory or compliance requirements.

Most chief information officers (CIO) originated from leading infrastructure operations roles, and this role struggles the most with the shift from in-house IT to as-a-service resources and the shift from traditional infrastructure management to managing cloud resources and service providers.

The CISO can ally with the CIO by closely collaborating and showing how security can help. For example, instead of saying, “No, going to the cloud is very difficult because of security reasons,” an enabling statement would be, “Let us try this cloud offering with the following additional security components for business unit XYZ.” That way, the CIO might benefit from increased flexibility for their business case, and IT, as well as security, is seen as an enabler.

For those companies that have it, the next positive alliance for CISO's to forge is with OT departments. Most OT departments are faced with an increasing need to integrate their prior stand-alone machines and processes into the supply chain to create an information flow in Industry 4.0 efforts. If the CISO is engaging with these departments in a positive, solution-oriented manner, use cases that benefit from an IT/OT integration will be far easier to achieve.

✓

The CISO can ally with the CIO by closely collaborating and showing how security can help.

Looking only to the CISO's own organizations is not enough, however. If your direct competitors or business partners are attacked, the likelihood is you will be next. Alliances that share and gain information on current threats are critical for the modern CISO to act before an attack has hit the company.

For all alliances, it is helpful to analyze threat scenarios and raise awareness for necessary business (not technology) decisions in these scenarios. Providing sample business cases and models will help the modern CISO be seen as capable of acting in the traditional role of protecting, but also as a capable business-centric and forward-thinking person.

Process: Agile and the Product-oriented Organization

Taking agile practices and structures into account, the CISO should also reconsider how processes in the security organization should interact with the rest of the business and, above all, product-centric teams. Before teams were organized across silos, the security organization used to be a governance authority releasing security policy and a gatekeeper as a final test and approval step.

For the CISO and the security organization to enable business, this is no longer a viable model. The enabling model consists of the following major building blocks:

First, the security organization needs to provide team members to the product-centric teams to be an integral part of developments and ideas. This placement of people directly in the product pipeline, working seamlessly together, manifests itself in the term of DevSecOps in which security is an integral part of the DevOps organization.

Second, the security organization needs to provide easily consumable services that the product-centric teams can use to produce products that are secure by design. As an example, this could be automated penetration tests or other artifacts for the **continuous delivery pipeline** to which developers can subscribe via self-service. Another example could be code-snippets for developers on how to integrate the company's security services to speed up development and provide thought leadership on how to integrate security into the core of each product.

✓

A common understanding for the different drivers in IT and OT is crucial for tomorrow's security organizations and their processes across the entire supply chain.

Third, the security organization needs to provide the traditional building blocks to guide, detect, protect and respond in a positive fashion that embraces new developments. These building blocks can, for example, be achieved and enhanced by using fast and compliant deployments that undergo security testing and allow a high-volume repetitive re-use that produces secure results in each execution, in contrast to any classical manual effort.

Fourth, the security organization needs to predict and prevent breaches, shift its focus from inward to outward and integrate current developments.

One way to address these changes is for the CISO to lead a community of people keen on security and provide knowledge directly to the teams instead of checking and controlling only their outcomes.

When a company aligns its organization in a product-oriented way, this rarely means "IT-only services," but integrates aspects of the whole supply chain. These end-to-end services, which provide value to the customer, are a combination of IT and OT components. A crucial aspect of tomorrow's understanding of IT and OT is that the previous priorities will merge into an overall picture of process safety, availability, confidentiality and integrity. A common understanding for the different drivers in IT and OT is crucial for tomorrow's security organizations and their processes across the entire supply chain.

Tools: Predict and Prevent Added to Detect and Respond

Traditionally, the security organization worked in an inward-looking and reactive manner, meaning that threats were detected once they attacked the perimeter and then the security organization reacted to those threats. In addition, in most development projects, security provided some policies as input and worked as a quality gate at the end, either approving or rejecting "because of security reasons," which then often lead to security exemptions.

In today's world this is not sufficient. For the CISO and the security organization to become an enabler, the tools need to support business goals. Instead of only looking inward at basic and essential security, the modern security organization needs to focus on proactive security.

✓

Instead of only looking inward at basic and essential security, the modern security organization needs to focus on proactive security.

The security organization should actively pursue threats that could target the larger organization and prevent them before they take place. This adds practices like active defense, threat hunting, threat intelligence and behavior analysis to the agenda of the security organization.

The second goal is to provide all the necessary tools that enable the agile and product-centric organization, as shown in the earlier section **"Process: Agile and the Product-oriented Organization."** As part of this building block, security organizations should link these tools directly to the proactive security tool landscape. For example, an automated security test would also include scanning for known vulnerabilities and require changes if the test fails or add additional security exploration activities and hardening measures if the organization's data were found to be compromised by threat intelligence.

The third goal is to adapt traditional security approaches to modern multi-cloud environments to enable the digital backbone of a digital business. This includes shifting from an IP-based network security model to a certificate-based network security model. It also means security organizations should leave the idea of a "trusted perimeter" behind and evolve a zero-trust approach with the different infrastructure and application components being exposed to the open internet. The questions are, "How strong and multi-cloud ready is our encryption," and "What do we need to do to be ready for encryption in the quantum-computing age?"

Managerial Recommendations

To outline the change in the CISO role, the following examples illustrate the transformation process. They provide recommendations for changes in the business strategy and their implications to the CISO role.

Manufacturing Company Integrating IT and OT

A manufacturing company that used a strategy saying, “We are a leading manufacturer and seller of our product,” is implying the following aspects to the CISO role:

- OT and IT are mostly separated in terms of people, process and tools.
- OT focuses primarily on production at stand-alone sites.
- Safety, reliability and resilience of the production site and the critical processes have the highest priority.
- Since OT is separated, cyberattacks are not considered possible or likely.
- IT focuses on the office IT aspects.
- Since IT is separated, cybersecurity initiatives focus on IT only.

Now, the manufacturing company is using the new strategy, saying “We are the leading provider of e-solutions with an end-to-end view on the whole lifecycle.” For the automotive industry, this means meeting the requirements of the UNECE regulations. This has the following implications:

- IT and OT need to be integrated allowing direct interfaces to business, partners and customers in both directions.
- Safety, reliability and resilience of the production site and the critical processes still have the highest priority. However, IT and OT are integrated, and cyberattacks are very likely and can directly affect safety, reliability and resilience.
- Since IT and OT are integrated with each other, cybersecurity initiatives focus on the business, including and integrating IT and OT.

With the new strategy, the role of the CISO changes in the following manner:

- The CISO enables OT to be integrated into the whole cybersecurity lifecycle, taking the priorities for safety and process resilience of OT into account.
- The CISO's organization provides security solutions with the following benefits:
  - Adding to safety to prevent attacks targeting the OT
  - Adding to availability by preventing attacks that halt production
  - Enabling digital initiatives that generate business value by integrating IT and OT.
- The CISO can showcase new possibilities for IT and OT integration, both from a value as well as from a threat perspective that includes business-targeting scenarios.
- The CISO evolves into a trusted partner for IT and OT connected manufacturing and ensures safety and security in this interconnected world.

Company Shifting its Products to a Digital Business Approach

A company that used the old strategy based on "Our products are developed in a waterfall approach" is implying the following aspects to the CISO role:

- There are three to four big releases per year
- Security served as a quality gate control in the test phase
- If the security test fails, the whole release is endangered, providing no business value for the next release cycle
- A control and audit mentality lead to a silo-thinking model between developers and security.

Now, the company is using the new strategy based on "Our products are developed focusing on business value and agility," which has the following implications:

- The order of magnitude changes drastically, targeting three to four releases every week/hour/minute/second according to the speed required by the business.
- Security is directly integrated into the development lifecycle, for example, the continuous exploration-integration-deployment) pipeline.
- Security testing is fully automated.

- Development of features happens in direct interaction (for example, Extreme Programming) between security-enabled developers and development-enabled security specialists.
- Security test fails are rare and lead to some rollbacks on some of the releases. Still, business value is created constantly in short cycles.

With the new strategy, the role of the CISO changes in the following manner:

- The CISO is an integral part of the development process and fulfills a leadership role in a **lean-thinking manager-teacher approach** to enable security.
- The CISO is the go-to resource for every potential security question requiring a thorough understanding of modern, fully automated development practices.
- The CISO is the provider of a development-enabled security specialist to the teams and provides solutions that can easily be consumed by the developers.
- The CISO is the training provider for security training to grow developers to security-enabled developers.
- The CISO is the provider for security services that can easily be consumed and are laid out in architectural runways.
- The CISO is the community of practice enabler for all security specialists across all teams.

ABOUT THE AUTHOR

The CISO as a Business Enabler
Transforming Security into a Competitive Advantage

ANDREAS DIETRICH

With over 17 years of experience in the industry, Andreas Dietrich supports customers in the space of security and enterprise service management. Andreas bridges the gap between strategic security consulting and architectural understanding.

ISG®

imagine your future®

ABOUT ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 75 of the top 100 enterprises in the world, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data.

www.isg-one.com

Let's connect NOW...

ISG®

imagine your future®