Msafe

Cyber Security Business Canvas

9 steps to compliancy & control

Why this Canvas matters now

In an era where data flows freely across systems, borders, and platforms, secure file sharing is no longer just a technical issue—it's a business imperative. Organizations face increasing pressure from regulators (NIS2, DORA), partners, and their own employees to ensure confidential data is handled with care.

Yet many security strategies are reactive and fragmented. That's where the Security Business Canvas comes in. This tool helps you structure security thinking, involve the right people, align with strategic goals, and ensure cultural adoption.

This report walks you through all nine elements of the canvas. It's practical, reflective, and designed for CISOs, IT managers, security officers, and digital workplace leads who want to move from firefighting to foresight.

“Security is not a side job. It’s a full-time responsibility.”

Thijs van der Linden | Msafe

Content

“Culture eats compliance for breakfast.”

Bjorn Brinkman | Deerns

Field Insights

The overlooked reality of everyday security

In the world of security, no two days are ever the same. Professionals working at the intersection of physical and information security often find themselves supporting high-risk organizations across diverse sectors: from cultural institutions to high-tech cleanrooms. The variety of environments brings both complexity and insight.

One day might involve conducting a penetration test; the next could be spent drafting policy for a public-facing institution. This kind of broad scope offers a unique, cross-sector view of what security looks like in real-world practice.
In many organizations, the role of CISO s no longer a defined, full-time position. Instead, it is often added to an existing job.

But those in the field know better: security is not a side task. It requires focus, attention, and authority to be truly effective.

This reality highlights a growing shift: physical and digital risks are converging, and organizations need clearer frameworks to navigate the overlap. This is why the concept of a Cyber Security Business Canvas resonates so strongly.

Too often, companies zero in on compliance or tooling alone, overlooking behavior, workflows, and partnerships. A canvas that brings all those elements together offers more than structure. It creates overview, clarity, and direction.

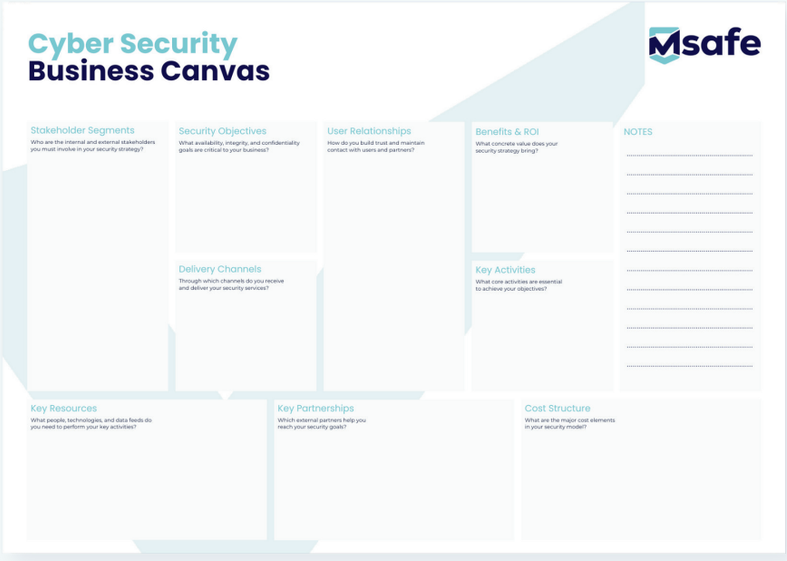
The insight is clear: sustainable security starts with structure and ends with culture. And anyone who’s seen the day-to-day realities knows: true security isn’t static or siloed. It’s evolving, human, and deeply connected to context.

The Cyber Security Business Canvas

The **Cyber Security Business Canvas** helps teams design their security posture collaboratively. It includes nine building blocks, each representing a key component of a security strategy. Each step includes a guiding question and an assignment to reflect and take action.

You can use this canvas in workshops, management sessions or project kick-offs. Use the printed canvas, draw it on a whiteboard, or use the digital version to co-create.

Would you prefer help from an external party? We are here for you! Our experts can guide you and your team through the Cyber Security Business Canvas so you can make the most effective use of it. Interested? Contact us.



TIP

Organize a team workshop using this document. Set 90 minutes aside, use the large version of the canvas, and work through each building block as a team. Use the insights to feed your annual planning or upcoming security roadmap.

“The human factor is still the weakest and most overlooked link.”

Atze Zwirs | Msafe

Step 1
Stakeholder Segments

Organize a team workshop using this document. Set 90 minutes aside, use the large version of the canvas, and work through each building block as a team. Use the insights to feed your annual planning or upcoming security roadmap.

Who are the internal and external stakeholders you must involve in your security strategy?

Brainstorm in pairs about all relevant stakeholders (e.g., CISOs, IT teams, end users, suppliers, auditors, regulators, cyber insurers).

Place their titles in the "Stakeholder Segments" area and sort by influence & relevance.

Step 2
Security Objectives

Security objectives should not be vague aspirations. Measurable, specific goals help justify investments, track improvements, and communicate impact to stakeholders.

What availability, integrity, and confidentiality goals are critical to your business?

For each C.I.A.* principle, formulate one SMART objective.

Write them on Post-its and place them in "Security Objectives".

*

The CIA Principle: Core of Information Security

The CIA principle is the foundation of modern information security. It stands for Confidentiality, Integrity, and Availability: three pillars that define the quality and resilience of your data and systems.

1. Confidentiality

Only authorized individuals should have access to specific information.
This prevents sensitive data, such as customer records, trade secrets, or contracts, from falling into the wrong hands. Confidentiality is typically enforced through access controls, encryption, and identity management.

2. Integrity

Information must remain accurate, complete, and unaltered by unauthorized parties. Any modification to data should be traceable and validated, ensuring you can trust that your information has not been tampered with. Mechanisms like audit logs, digital signatures, and versioning support integrity.

3. Availability

Authorized users must have reliable access to the information and systems they need—when they need them. Availability requires protection against disruptions such as system failures, cyberattacks (e.g. DDoS), and natural disasters. This is typically addressed through redundancy, uptime monitoring, and incident response planning.

Step 3
Delivery Channels

Security delivery depends on visible, usable interfaces. Whether it's a DLP alert, a phishing training, or a secure file sharing API, your delivery channels define how well your strategy reaches people.

Through which channels (tools, APIs, reports, training) do you receive and deliver your security services?

Perform a quick scan:
What tools/processes do you currently use? What are you missing?

Fill in both lists in the canvas.

Step 4
User Relationships

Trust is built before a crisis occurs. How you prepare and communicate during incidents determines user confidence, partner retention, and reputational impact.

How do you build trust and maintain contact with users and partners (e.g. onboarding, incident response)?

Describe the ideal user journey during a data leak.

Sketch it on the canvas using arrows and notes.

Step 5
Benefits & ROI

Security is often perceived solely as a cost. Demonstrating measurable returns helps position it as a value driver and supports continued investment.

What concrete value does your security strategy bring (cost reduction, efficiency, reputation)?

Define 3 KPIs (e.g. number of DLP incidents prevented, number of phishing clicks avoided).

Add target values and frequency of measurement.

Step 6
Key Activities

Knowing your key security processes creates clarity, continuity, and improves resilience in times of stress.

What core activities, from risk assessments to threat hunting, are essential for achieving your objectives?

Build a process flow for one critical activity (e.g. incident response).

Note each step and responsible actor on the canvas.

Step 7
Key Resources

Security requires specialized capabilities. Mapping your critical resources ensures readiness, avoids dependency risks, and supports effective planning.

What people, technologies, and data feeds do you need to perform your key activities?

List at least 5 items (e.g. analysts, SIEM tools, threat intelligence feeds).

Label each as internal/external and strategic/operational.

Step 8
Key Partnerships

Security ecosystems are too complex to tackle alone. Strategic partnerships enable scalability, access to expertise, and shared responsibility.

Which external partners help you reach your security goals?

Brainstorm current and desired partnerships (e.g., MSSPs, regulators, technology vendors).

Add each to the canvas with a short description of their role.

Step 9
Cost Structure

Transparency in cost structure enables prioritization, budget planning, and better communication with finance stakeholders.

What are the major cost elements in your security model?

List your cost items: licenses, staffing, integration, training, SOC hours.

Estimate annual costs for each item.

Reflection & Next Steps

You've now mapped out your security foundation. The next step is reflection:

- Which canvas blocks are still unclear or empty?
- What are your top 3 gaps or opportunities?
- Who should you involve to complete the canvas?

Use your answers as the basis for action planning. Here's how:

Identify quick wins

Look for areas that can be improved rapidly with minimal resources (e.g. adding 2FA to your file sharing system or updating user onboarding).

Prioritize major improvements

For larger gaps, assign ownership, define timelines, and allocate budget. Use the SMART objectives you've defined in the canvas.

Involve the right stakeholders

If a canvas block lacks clarity, it often means the right people weren't in the room. Bring in HR, Legal, or IT Ops to help fill in what's missing.

Translate the canvas into a roadmap

Turn your completed canvas into a phased implementation roadmap, grouped by quarter or maturity level.

Schedule review sessions

Revisit your canvas every 6–12 months. Use it as a tool to track progress, identify new risks, and adjust course.

New Insights

The State of Secure Sharing

Sharing sensitive files is one of the most overlooked risks in modern organizations. While endpoint protection and firewall rules are top-of-mind, documents often leave the organization through unsecured email, unauthorized cloud services, or poorly configured APIs.

Common challenges

Shadow IT
Employees using tools such as WeTransfer, Dropbox, or Gmail without approval.

Over-permissive sharing
Internal documents becoming accessible.

Lack of traceability
No audit logs for who shared what, when, and with whom

Cultural gaps
Security seen as a blocker, not an enabler

With rising regulatory pressure (NIS2, GDPR enforcement, supply chain security), organizations can no longer rely on ad hoc solutions. Secure sharing must be an embedded part of the company culture and IT architecture.

How Msafe supports your Secure Sharing Strategy

At Msafe, we help organizations embed secure file sharing into their daily operations and long-term strategy. We understand that compliance, technology, and user behavior must work together and that security should be as frictionless as possible.

Our platform is purpose-built to simplify secure file exchange while maintaining control, usability, and compliance. Whether you're dealing with sensitive client documents, intellectual property, or operational data, Msafe provides a trusted environment where information can be shared safely, transparently, and in line with your internal policies.

Msafe empowers IT and Security teams with auditability, integration capabilities (including Outlook and API support), and strong encryption. But more importantly, we support cultural change by making secure sharing intuitive and accessible to every employee.

Our approach reflects the core message of this report: that secure sharing must evolve from being a technical checkbox to a strategic, organization-wide mindset.

"The Security Business Canvas helps you map out where to go. Msafe helps you get there."

With Msafe, security feels simple

At Msafe, we believe that sharing sensitive information should be both easy and truly secure.

Our solutions are designed to help organizations protect their most critical files, while ensuring that employees can work seamlessly without added complexity.

From end-to-end encryption to compliance-ready audit trails, Msafe provides the tools organizations need to stay in control of their data.

Designed for sectors where security is non-negotiable, such as critical infrastructure, energy, and manufacturing, Msafe combines simplicity with uncompromising protection.

Linnaeusweg 9a | IJsselstein
+31 88 88 53 010
info@msafe.nl
msafe.co