CY360 Effective Security Program

Whitepaper

Sven Bruelisauer
sb@cyway.one

Fabian Gasser
fg@cyway.one

Executive Summary A better approach is needed to protect businesses from cyber threats effectively. Too many security programs today fail to adequately protect the businesses they serve. They often introduce unnecessary complexity, impeding business instead of enabling it. In response, regulators have released directives and regulations affecting companies both in the EU and in Switzerland (NIS2, DORA, Cyber Resilience Act (CRA)), yet many organizations still struggle to incorporate such standards effectively.

We propose a real-world validated methodology that has helped dozens of organizations promote effective cybersecurity programs that fundamentally align with the businesses they protect. The CY360 approach continues to deliver strong results for our clients and by making it publicly available we hope to contribute to a more cyber-resilient world.

Organizations find CY360 valuable because it ...

1. Enables business rather than blocking it

2. Breaks down complexity of modern threats using globally adopted benchmarks (e.g. NIST CSF 2.0)

3. Delivers holistic visibility to key executives

4. Optimizes cost and effectiveness through prioritized actions and quick wins

5. Transforms regulatory compliance (e.g. nDSG, DSGVO, NIS2, DORA) into strategic advantage

I. Introduction

Modern organizations find it increasingly difficult to protect themselves from cyberattacks. With core business value hinging on IT, many businesses rapidly adopt new technologies – particularly cloud services and AI – creating added complexity and leaving cybersecurity measures lagging behind.

Combined with rising cyber criminality – up 75% year-over-year in 2024 [1] – global annual cybercrime damages are expected to reach $9.5 trillion [2], with the average data breach costing $4.88 million [3]. Regulators address these challenges with more stringent security requirements (e.g. NIS2, DORA, CRA), imposing significant fines of up to 4% of annual revenue and even personal liability on executive boards [4]. Unsurprisingly, cyber risk remains the top concern for Swiss business leaders in 2025, with 65% of Swiss executives prioritising the mitigation of cyber risks over the next 12 months [5].

Risk-based frameworks (NIST CSF, ISO 27001) can help navigate these challenges and are increasingly popular. Yet, they can be complex to implement and, if not applied properly, often impede core business operations. The cybersecurity skills gap intensifies the problem, as organizations struggle to find CISOs who are skilled at aligning security practices with business goals.

In this paper, we present the CY360 methodology – a framework that helps organizations focus on what truly matters. It empowers them to design and run effective cybersecurity programs, fully aligned with NIST CSF, and thus to benchmark internationally. Refined over the past five years, CY360 has helped numerous organizations become cyber-resilient, and we hope that its wider adoption will enable more businesses to focus on core activities while implementing robust security.

II. Non-effective Programs

Many cybersecurity programs falter and fail because they:

- Do not reflect actual business needs and priorities
- Lack executive buy-in and support
- Induce decision paralysis through overcomplication
- Misallocate resources and budgets
- Strive for completeness without enabling decisive action

The result is a protection gap – and often worse: the security program itself begins to hinder the organization it was meant to protect. Poorly designed stopgap measures, implemented without strategic alignment, create friction, slow down operations, and stifle innovation. What begins as a risk mitigation effort can end up undermining business performance.

To be effective, cybersecurity must be embedded into the fabric of the business – treated as a core risk and managed with the same strategic intent. Only then can organizations build lasting resilience in a dynamic threat landscape.

III. CY360 Methodology

Cybersecurity should be tailored to each organization's business context. Every dollar spent should ultimately improve the organization's core objectives. We here outline key aspects of the CY360 approach to building cyber resilience.

CY360 provides a pragmatic approach to building and running an effective security program to drive cyber resilience in the specific context of the business. It is structured to reflect the full lifecycle of a security program – from understanding the organization's strategic direction to continuously improving based on measurable outcomes.

Panel 1: Each component in CY360 builds on the last, with the core idea that cybersecurity is not a siloed technical function, but a critical enabler of business success. The methodology integrates cybersecurity into a cohesive cycle that is agile and business relevant.

1. *Understand the Business*

The starting point is always the business. Without a clear understanding of context: what the business does, where it is heading, and what it values most, security measures are at risk of being irrelevant or even obstructive. The first step is to conduct interviews with senior stakeholders – typically members of the Executive Board (EB) and Board of Directors (BoD). The objective is to establish the organization's North Star: the minimum target state for cybersecurity that will enable strategic goals of the business. This typically means understanding not only what needs to be protected, but why – whether it's regulatory requirements, market competitiveness, or business continuity.

Questions are intentionally open-ended:

- What are the crown jewels of your core business?
- What is your top cyber concern today?
- What do you need from cybersecurity to feel confident making business decisions?

By capturing these perspectives early, the security program can be designed to support – not hinder – strategic priorities. Importantly, this phase also builds the foundation for executive buy-in and sustained support. It is an opportunity to frame the security program as a strategic enabler - one that will ultimately provide the metrics, the KPIs, and the clarity needed to support informed decision-making.

It is important to maintain an adequate abstraction level during these interviews and to avoid getting into deep technical detail. The focus needs to be centered on the main objective: safeguarding the business. To ensure holistic coverage across the business, the interview pool should be tailored to reflect the organizational structure.

2. Validate Crown Jewels

Once initial insights have been gathered, the organization's most critical assets – its crown jewels – are validated. Rather than compiling exhaustive asset inventories, assets are grouped into classes that reflect business relevance: critical cloud environments, customer data repositories, R&D platforms, etc.

This abstraction keeps the discussion business-focused and manageable. It also enables different stakeholder groups - from technical to non-technical – to have a shared understanding of what's at stake.

Cross-referencing this abstraction with available inventories, operational maps, and SME interviews, ensures completeness. Where necessary, simple but effective structures are introduced for tracking assets, risks, and controls going forward.

3. Risk Analysis

With business priorities and key assets identified, the next step is to conduct a structured risk analysis. Asset classes are mapped to risk scenarios, which align with real-world threat models (e.g. ransomware, data leakage, or regulatory breaches) in the context of the organization's specific business environment. The risk scenarios act as a "story layer" for the program and often help re-focus later discussions should they be at risk of derailing e.g. into niche technical details.

CY360 uses NIST CSF 2.0 as its primary framework, providing broad coverage, clear benchmarking, and compatibility with other standards (e.g., ISO 27001, TiSAX). By limiting questions to a focused and tailored set, insights gathered are rich, meaningful and business relevant.

Evidence checks for key components (e.g. patching processes / incident response plans) increase the assessment quality by making the answers more tangible. Technical spot checks in critical areas (e.g. Microsoft 365, external exposure, security operations) provide practical validation and further increase assessment quality. They support verifiability both for the

organization running the program, as well as with auditors of regulators or certification bodies.

The result is a clear picture of current risk, mapped against business priorities and visualized in matrices that support action planning.

4. Action Planning

Security measures must produce business value. In CY360, all proposed risk treatment actions are explicitly linked to business outcomes such as compliance readiness (e.g. NIS2, DORA, CRA, ISO 27001, TiSAX, HIPAA), customer trust, operational continuity, or strategic differentiation.

The shortest path to achieving the desired business outcomes, based on the North Star and outlined risk is identified. In many cases, substantial improvements in resilience can be achieved with minimal investment. Treatment actions are grounded in established best practices and enhanced by real-world experience from comparable organizations and industry environments.

Each candidate action is evaluated based on ROI – its projected risk reduction compared to its estimated cost. This allows for prioritization and rapid identification of quick wins. Linking the actions back to core business assets and key risk scenarios ensures they are mutually understood by all stakeholders. By forecasting their potential impact on the organization's NIST CSF score, tangible, trackable goals are created.

The result is a treatment plan that is relevant, feasible, and optimized for both impact and cost.

5. Executive Steering

CY360 treats executive steering as the heart of program governance. Held bi-annually, or quarterly for fast-moving organizations, steering sessions are designed not as status updates, but as decision forums.

Each session provides situational awareness through a *Current Threat Radar* – contextualizing external risks and recent developments in the context of the organization's own environment. The action plan is condensed and presented for validation and sign-off.

Clear ownership is established using structures like RACI matrices, and decisions are tracked formally. Progress is reported through concise dashboards showing the overall NIST CSF score, per-function metrics (Govern, Identify, Protect, etc.), and a handful of business-critical KPIs or KRIs.

Executive Steering ensures that cybersecurity remains visible, actionable, and tied to strategic objectives.

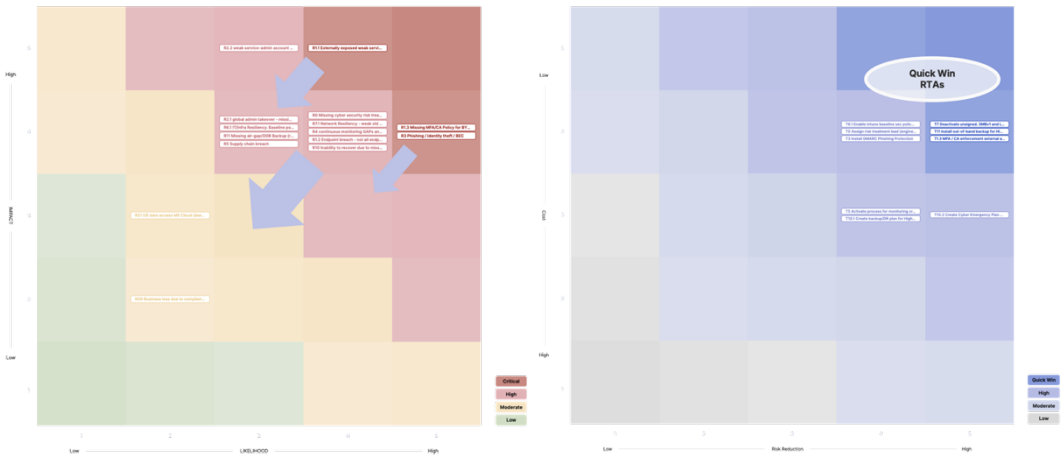
6. Continuous Improvement

CY360 is not a one-off project. It creates a repeatable, adaptive cycle that keeps the organization aligned with evolving business needs and maintains resilience against external threats.

Continuous Improvement is the governance framework that surrounds the program. It encompasses routine feedback loops – drawing on security incidents, changes in business operations, audit findings, and new regulatory demands.

Adjustments to risk definitions, asset scopes, or priorities feed directly into the next steering session. Using consistent visuals and tracking mechanisms ensures that change is both measurable and comparable over time.

Ultimately, Continuous Improvement sustains the momentum generated by executive steering and ensures that security stays relevant, efficient, and forward-looking.



Panel 2: The risk matrix (left) visualizes key risks to the business holistically, while the treatment effectivity matrix (right) helps weigh candidate actions against one another trading off risk reduction vs. cost. Quick Wins are highlighted in the top right corner.

IV. Case Study

For illustrative purposes, we share a case study of a typical engagement:

The client - a Swiss-based manufacturing group with subsidiaries in 15 countries and with 4'000 employees - faced mounting cybersecurity demands as part of their digital transformation. Innovative AI-driven systems and global supplier-customer integrations created substantial complexity. Although the firm had no history of major cyber incidents, rising attacks on peers heightened board-level concerns. In parallel, new cybersecurity regulations and customer requirements (especially with respect to NIS2) increasingly led to disqualifications from RfPs, thereby directly impacting the firm's sales.

Following an unsuccessful attempt at achieving an ISO 27001 certification on global company scope (which stalled after six months due to complexity and internal resistance), the executive board sought external guidance to reshape the security program for both compliance and long-term business viability. They selected CY360 to streamline the effort.

1. *Understand the Business*

Executive Alignment
We began by interviewing the executive board and key functional leads from each of the three main business units (BUs). This provided a top-level view of the company's drivers: two BUs prioritized availability to maintain consistent production output, while the third BU, serving sensitive R&D-intensive customers, required stronger confidentiality.

Securing Buy-In
By clarifying that the program would enable (rather than impede) core business processes and provide a competitive advantage for the company - we secured leadership support early – critical for the subsequent risk mapping.

Strategic Focus
The interviews uncovered that the stalled ISO 27001 initiative had overburdened staff with granular documentation tasks. Our immediate pivot was to keep essential processes but trim non-critical red tape. Early consensus on "*CY360 as an enabler*" helped maintain high-level executive involvement.

2. *Validate Crown Jewels*

High-Level Asset Segmentation
Instead of chasing an exhaustive asset list, we grouped assets into logical categories: shared IT infrastructure for BUs A&B, specialized R&D environments for BU C, and global corporate services. This allowed the team to focus on the most impactful areas first and cleared the way to realize quick wins.

Stakeholder Validation
We cross-referenced interview findings with existing IT asset inventories and consulted subject matter experts within the company to ensure no critical production lines or data repositories were missed.

Streamlined Decision-Making
By segmenting assets into broad classes, the organization could quickly set different Service-Level Agreements (SLAs) per business unit without overcomplicating the asset catalogue. This resolved prior confusion, letting teams advance to risk analysis rapidly.

3. *Risk Analysis*

NIST CSF Alignment
Transitioning from a sprawling risk register of hundreds of loosely tracked items to a concise, NIST CSF–based assessment helped the organization to pinpoint and prioritize its most relevant risks. Each core business asset class was mapped to relevant threat scenarios - e.g., ransomware or DDoS for shared infrastructure, or IP theft for specialized R&D data.

Effort vs. Clarity
Stakeholders were initially skeptical, having invested much time in the old registers. However, a more focused set of pointed questions - supplemented by specific evidence checks - made risk scoring both simpler and more accurate.

Targeted technical validation
We ran targeted technical evaluations in Microsoft 365 environments and tested the resilience of identity services. This surfaced real-world proof points (e.g., misconfigured authentication components) that validated and refined the abstracted risk scenario findings.

4. *Action Planning*

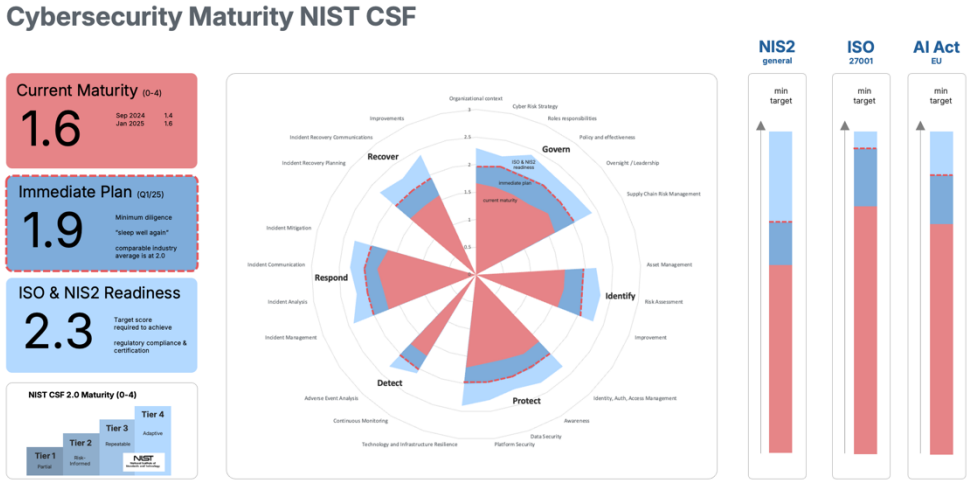
Outcome-Centric Business Alignment
Visual risk matrices clarified "why" each risk mattered to the business, tying each risk back to a concrete business consequence. Each proposed action was mapped directly back to a defined business requirement or risk scenario, creating a clear line of sight from technical improvement to business value. Decision-makers saw, for example, that a moderate cost to improve identity management directly mitigated a high-risk scenario impacting global operations.

Quick Wins Delivered
Immediate actions were launched with minimal friction: These included low-effort, high-impact measures such as formalizing existing technical and organizational measures (TOMs), which immediately unlocked multiple pending RfPs. The ability to show concrete progress early helped shift organizational momentum and demonstrated that meaningful improvements were possible without major disruption or investment.

ROI Analysis
Candidate mitigation projects were visualized in an ROI matrix. Comparing cost vs risk reduction on a holistic level proved vital in facilitating budget planning across the three BUs.

5. *Executive Steering*

Steady Executive Drumbeat
A bi-annual Cyber Risk Steering Committee was embedded into the company's governance rhythm. Each session began with a contextual threat radar, reviewed progress vs. plan, and concluded with a decision log – ensuring meetings led to tangible outcomes



Panel 3: Example overall risk reporting showing current maturity and planned improvements. The immediate plan directly actions grave exposure risks, upon which the light blue plan shows incremental business relevant certification and compliance targets.

with clear ownership. This consistent cadence sustained executive attention and drove measurable progress.

Strategic Roadmapping and Prioritization
A visual treatment roadmap linked initiatives to business outcomes (e.g., ISO 27001, NIS2) and projected NIST CSF score improvements. This enabled BU-level alignment, clarified trade-offs, and allowed sequencing or merging of overlapping efforts for greater efficiency.

Metrics that Drive Visibility and Accountability
Reporting centered on a concise dashboard combining NIST CSF scores with select KPIs and KRIs. Metrics exposed critical collaboration interfaces – e.g. for patching and to contain security incidents the IT Operations team was required to execute certain actions – and reinforced accountability by consistently tracking progress over time in a transparent format.

6. *Continuous Improvement*

Tangible Improvements Without Disruption
Within two quarters, the leadership team could see tangible improvements in security posture, notably in patching discipline and AI model access controls. Crucially, these improvements did not stall AI innovation; rather, they provided guardrails that satisfied customers' security demands while sustaining rapid R&D.

Adaptive Cycles That Stay Aligned
Feedback from incidents, audits, and business changes fed directly into roadmap updates and steering discussions. This ensured the program stayed relevant over time and could adjust quickly to emerging risks or shifts in business focus – sustaining both momentum and strategic alignment.

Increased Leadership Confidence
Progress was tracked using a consistent quarterly format: risk matrices, ROI charts, and overall NIST CSF scores. This structure gave senior leaders a high-level view of where the program stood, which risks were being addressed, and how resources translated into results – reinforcing sustained executive backing. The CFO remarked, *"With CY360, we focus on what truly matters: the biggest risks and the highest returns on our security investments."*

Results & Feedback

Reduced Organizational Friction
Teams across all business units reported smoother collaboration with partners and internal stakeholders, supported by a clear, consistent cybersecurity program. The streamlined program design avoided unnecessary complexity, allowing each unit to implement improvements with minimal disruption to core operations, including R&D and production environments.

Accelerated Sales Through Competitive Advantage
Demonstrable alignment with best-practice frameworks and clear evidence of compliance maturity enabled the company to respond more confidently in RFPs and partner assessments. Security became a commercial asset – improving sales effectiveness, shortening procurement cycles, and contributing to increased deal volume across multiple markets.

Executive Alignment and Lean Delivery
The program delivered measurable results on time and within budget, without the typical overhead of large-scale security initiatives. Senior leadership, including the CFO, appreciated the lean approach and praised the program's ability to focus on the highest-impact risks, translating complex technical efforts into clear business outcomes.

Future-Proofing and Regulatory Readiness
The flexible structure of the program made it easy to extend into new compliance areas such as NIS2 and the EU AI Act. By building on already established priorities and structures, the organization minimized rework and ensured continued alignment with evolving regulatory expectations - strengthening both resilience and long-term agility.

V. Rationale

The CY360 methodology enables effective cybersecurity programs by resolving common failure points found in traditional approaches. This chapter outlines why CY360 delivers measurable results - structured around its key differentiators.

1. Enables Business Rather Than Blocking It

Traditional security programs often operate in isolation, focusing on technical controls without understanding the business context. This leads to friction, project delays, and wasted investments.

CY360 solves this by starting with executive and stakeholder engagement. Interviews at the Board and Executive levels identify key business priorities and risk perceptions early, establishing a clear mandate for the program. By doing so:

- Security becomes aligned with actual business value streams.
- Leadership buy-in is secured from the outset, accelerating decision-making.
- Security measures support innovation and operations rather than inhibit them.

Aligning cyber risk management with organizational strategy is a critical paradigm shift [6] and research consistently shows that top management commitment is key to success [7].

2. Breaks Down Complexity of Modern Threats using Globally Adopted Benchmarks (e.g. NIST CSF 2.0)

Modern IT environments - hybrid clouds, AI models, API integrations - introduce vast complexity at speed. Attempting to address this complexity with exhaustive asset lists or checkbox controls leads to analysis paralysis and implementation fatigue. Misconceptions of what matters most are a resulting problem [8].

CY360 reduces this complexity through:

- Asset abstraction: Grouping assets into business-relevant classes makes them easier to understand, prioritize, and secure.
- Risk scenario mapping: Anchoring risk in tangible threats and consequences focuses discussions on what truly matters.
- Use of NIST CSF 2.0: This globally recognized, modular framework allows for complete yet flexible coverage of security domains, ensuring no critical area is overlooked while avoiding overreach.

Through NIST CSF - which maps to ISO 27001, DORA, TiSAX, etc. - organizations can benchmark across industries while reducing framework fatigue. With it being the most widely adopted cybersecurity risk management framework [9], it is ideally suited to enable benchmark comparisons within and across industries.

3. Delivers Holistic Visibility to Key Executives

Security programs often fail at the communication layer - overwhelming decision-makers with detail or offering metrics disconnected from business impact.

CY360 ensures visibility through:

- An executive dashboard, typically visualized on one page.
- Condensed decision items visualizing risk vs cost tradeoffs.
- Metrics that link security to business outcomes (e.g., certification readiness, regulatory compliance, business continuity).

Executives engage meaningfully when security is framed as part of business risk – not buried in technical jargon – enabling informed decisions, sustained buy-in, and faster traction across the organization.

4. *Optimizes Cost and Effectiveness Through Prioritized Actions and Quick Wins*

Security budgets are finite, and the opportunity cost of poor prioritization is high. Many programs overspend on low-impact controls while leaving critical risks untreated.

CY360 introduces structured, ROI-based prioritization by:

- Mapping candidate actions against cost and expected risk reduction, enabling transparent decision-making.
- Surfacing quick wins that can deliver measurable improvements with minimal disruption.
- Using KPIs and KRIs to validate progress and inform future budget cycles.

This approach shifts cybersecurity from reactive spending to strategic investment, helping organizations achieve more with less while building executive confidence in the program's value.

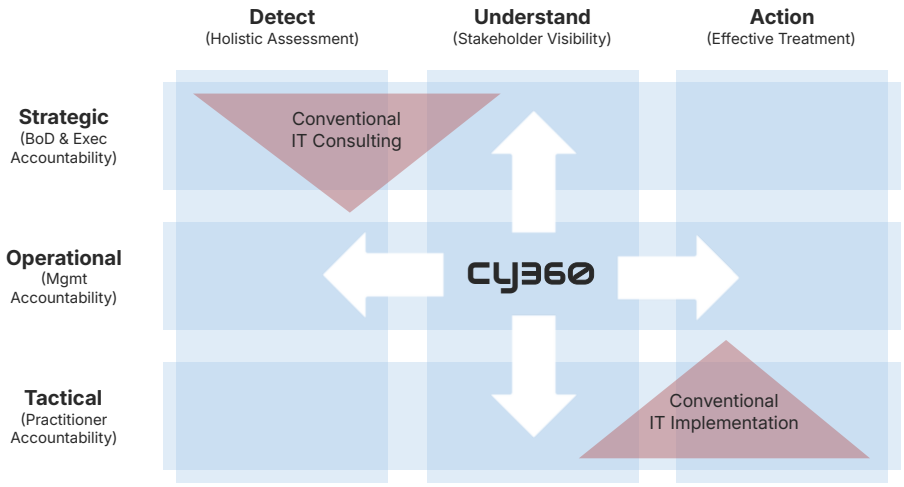
5. Transforms Regulatory Compliance (e.g. nDSG, GDPR, NIS2, DORA) Into Strategic Advantage

While some organizations view compliance as a necessary burden, CY360 helps reposition it as a business differentiator.

By embedding compliance into the core of the risk and resilience program:

- Regulatory needs are addressed proactively and aligned with business goals.
- Evidence and assessments are reused across frameworks, minimizing duplication and audit fatigue.
- The organization can demonstrate maturity in RfPs, customer reviews, and partner assessments - turning compliance into a competitive edge.

With CY360, compliance is no longer a standalone obligation but part of a unified structure that strengthens both security posture and market positioning. Some of our MSSP clients use CY360 as a sales enablement tool [10].



Panel 4: Conventional IT consulting often remains too theoretical and fails to get traction on the ground. Conventional IT implementation often executes head-down, without a clear connection to, or mandate by, strategic initiatives. CY360 strikes a balance and connects between layers to enable an effective security program. Transparency on key risks and decisions both ensures holistic completeness of cyber resilience initiatives, as well as the realization of quick wins along the way.

VI. Conclusion & Outlook

In rapidly evolving digital landscapes, cybersecurity is more than a technical requirement - it is a fundamental business imperative. Rising threats, regulatory pressure, accelerated technology adoption, and a cybersecurity skills gap mean the status quo of "security for compliance's sake" often falls short of real business needs.

The CY360 approach offers a structured, business-aligned methodology that converts cybersecurity from a regulatory burden into a strategic enabler. By focusing on stakeholder engagement, risk-driven prioritization, and clear KPI tracking, CY360 ensures security investments deliver measurable business value while maximizing efficiency.

Organizations leveraging CY360 have reported significantly reduced cyber risk, optimized security spending, better executive and business alignment, and enhanced market credibility.

We encourage security leaders and business executives to adopt CY360 principles for effective, business-driven security programs supporting sustainable growth and resilience.

References

[1] C. Research, “A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide,” 2024. [Online]. Available: https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/.

[2] C. V. &. eSentire, “Cybercrime To Cost The World $9.5 trillion USD annually in 2024,” 2023. [Online]. Available: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/.

[3] Ponemon_Institute_&_IBM, “Cost of a Data Breach Report 2024,” 2024. [Online]. Available: https://www.ibm.com/reports/data-breach.

[4] EU_Council, “Directive (EU) 2022/2555 of the European Parliament and of ...,” [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng.

[5] PwC, “Bridging the gaps to cyber resilience,” [Online]. Available: https//www.pwc.ch/en/insights/cybersecurity/global-digital-trust-2025.html.

[6] F. Mizrak, “Integrating cybersecurity risk management into strategic management: a comprehensive literature review,” *Research Journal of Business and Management,* 2023.

[7] S. P. Raymond Young, “Top management support—almost always necessary and sometimes sufficient for success: Findings from a fuzzy set analysis,” *International Journal of Project Management.*

[8] Reuters, “ESG Watch: Companies ‘complacent about cybercrime’, despite rise in risk from AI,” 2025. [Online]. Available: https://www.reuters.com/sustainability/sustainable-finance-reporting/esg-watch-companies-complacent-about-cybercrime-despite-rise-risk-ai-2025-02-03.

[9] S. K. H. P. Marion Toussaint, “Industry 4.0 data security: A cybersecurity frameworks review,” *Journal of Industrial Information Integration,* 2024.

[10] Open_Systems, “Navigating the Compliance Labyrinth,” [Online]. Available: https://go.open-systems.com/Compliance_Guide.html.

[11] Creative_Commons, “Creative Commons Attribution-NoDerivs 4.0 International License,” [Online]. Available: https://creativecommons.org/licenses/by-nd/4.0/deed.en.

About cyway

Cyway GmbH (www.cyway.one), based in Horgen, Switzerland, specializes in protecting organizations from modern cyber risks. Through risk-based strategies, business alignment, and actionable analytics, cyway delivers cyber resilience that enables strategic business advantage. We serve clients of all sizes across sectors including manufacturing, financial services, technology, pharmaceuticals, government, and NGOs. Our team brings together senior professionals with deep, hands-on experience in offensive security, cloud and software architecture, security operations, analytics, and cyber risk governance. With backgrounds spanning both leadership and engineering, we operate at the intersection of strategy and execution – helping clients navigate complexity, make informed decisions, and achieve security outcomes that hold up under pressure.

Sven Bruelisauer

Sven is a partner at cyway, bringing over 20 years of hands-on expertise in Digital Transformation. With a multifaceted career as a Chief Security Officer, Sales Executive, Engineer, and Red Teaming Auditor, he excels in managed IT security, Cyber Risk Management, Cloud Adoption, Intelligent WAN Networks, and comprehensive Security & Compliance. Sven earned his Master’s degree as Dipl. Ing. ETH from the Swiss Federal Institute of Technology in Zurich and holds certifications including CISSP, Microsoft Azure Cloud, and Unix/Linux specialist. He has served as representative of FIRST (Forum for Incident Response and Security Teams), SWIRT, CH-CERTS (Swiss Computer Emergency Response Teams) as well as of SISA (Swiss Internet Security Alliance).

Fabian Gasser

Fabian is a partner at cyway, focusing on Analytics, Engineering, and Operational Excellence. With over 15 years in cybersecurity, he has supported more than 100 organizations in optimizing security operations and aligning cybersecurity initiatives with core business objectives. Throughout his career, Fabian has built and led global teams exceeding 90 professionals and has contributed to shaping the strategic direction of two major MSSPs as part of their senior leadership teams. His expertise spans software development, architecture, product and service engineering, as well as general management. Fabian holds a Master of Science in Electrical Engineering and Information Technology from ETH Zurich. His research applying data science to cybersecurity resulted in academic publications and the founding of an ETH spin-off.

contact

cyway GmbH Switzerland
https://www.cyway.one
info@cyway.one