TREE SOLUTION
SECURITY AWARENESS SINCE 2005

Report

Security Culture Code

20 Years of Security Awareness Radar— Strategic Guidelines for an Effective Security Culture

Version 1.1, September 1, 2026

A personal note from the author

When I laid the groundwork for the Security Awareness Radar more than two decades ago at the International Institute of Management in Technology (IIMT) at the University of Fribourg as part of my dissertation, information security was still very much a technical field. Firewalls and antivirus programs dominated; people were viewed primarily as a source of errors, hardly as a strategic resource for resilience.

The vision was to make information security culture—which had previously been considered a “soft” topic—measurable, comparable, and thus manageable. Over the course of 20 years, this research question has given rise to one of the most comprehensive time series on information security culture in the German-speaking world.

Based on 88 surveys with over 100,000 participants, the data set shows that some early hypotheses have been confirmed, while other results have been surprising. This assessment is therefore more than just a long-term analysis. It reflects the maturation process of an entire discipline—and it crystallizes into what I now refer to as the **Security Culture Code.**

Over the past two decades, the Security Awareness Radar has tracked the evolution of information security culture in numerous organizations. This publication is not intended merely as a retrospective. It deciphers the strategic guidelines that determine whether security culture remains merely a formal facade or becomes the effective operating system of a resilient organization.

The report is therefore intended both as a retrospective and as a roadmap for a security culture that can withstand a highly interconnected and volatile future.

Warm regards

Dr. Thomas Schlienger

TREESOLUTION

Management summary: Security Culture Code

The results from 20 years of the Security Awareness Radar show that technological and structural upgrades alone are not enough. True resilience comes only through the **Security Culture Code**—the strategic decoding of what drives security culture at its core.

The long-term analysis confirms a broad trend toward professionalization; the proportion of organizations with insufficient maturity has dropped significantly. However, only a few have succeeded in achieving cultural excellence. The reason: Higher levels of maturity are not driven by greater knowledge—which is often already at a good level—but rather by how deeply they are embedded in the social and organizational structure.

The **Security Culture Code** for an effective security culture is defined by four strategic levers:

1. System logic before geography: Shared frameworks form the infrastructure for effectiveness.
2. Leadership as a catalyst: Setting an example and demonstrating maturity go hand in hand.
3. Practicality: Motivation increases when clear processes make it possible to experience a sense of security in everyday life.
4. Attention, not knowledge: Success is measured not by the amount of information, but by the management of organizational attention.

Conclusion for decision-makers: The next stage of maturity rarely requires additional training, but rather the visible integration of security into leadership, communication, and routines. The goal is to make security culture an integral part of the organization's operating system.

Based on this, the report outlines a roadmap for 2026 through 2030.

A high level of maturity emerges when leadership visibly prioritizes security, communication and empowerment work in tandem, and security is embedded in processes and routines.

Table of contents

TreeSolution

List of figures

List of tables

1. Why culture is key to resilience today

Today, information security is no longer determined solely by technical safeguards. Firewalls, identity management, and endpoint protection remain essential, but they are not enough to ensure organizational resilience. Security only becomes effective when employees understand the requirements, prioritize them, and put them into practice in their day-to-day work. This is precisely where security culture becomes a decisive factor.

The central question, therefore, is not only whether organizations have appropriate security measures in place, but how deeply security is embedded in day-to-day management, routines, communication, and collaboration. A mature security culture is not primarily evident in campaigns or formal guidelines, but rather in the fact that secure behavior has become established in everyday work as practical, expected, and professionally sound. The “human factor” thus shifts from being a risk factor to a driving force behind organizational resilience.

What is the Security Awareness Radar (SAR)?

The Security Awareness Radar (SAR) is a standardized tool for assessing information security culture in organizations. It measures security culture not only in terms of knowledge, but across multiple domains at the individual, group, and organizational levels, including knowledge, values, perception, communication, leadership, and organizational embedding. Surveys are typically conducted anonymously and on a recurring basis; this makes them suitable for assessing the current state, tracking progress over time, and deriving practical measures.

For the sake of comparability, responses are converted into scores on a scale from 0 to 100. The aggregated total score is called the Security Awareness Indicator (SAI). For the theoretical and methodological basis, see Schlienger (2003, 2006) and Keller (2026).

88
Surveys

100k
Participants

4.5M
Individual responses

20
Years

This report is based on 88 organization-wide surveys involving over 100,000 participants and approximately 4.5 million individual responses from 2004 to 2025. The goal is not to demonstrate universally valid causal relationships, but rather to provide a data-driven analysis of typical developmental trajectories and practical differences between organizational forms.

The report has two objectives:

1. to provide an empirical and practical assessment of the evolution of security culture over the past 20 years;
2. to derive specific recommendations for action tailored to different maturity levels and organizational contexts.

2. The evolution of maturity—a look back at two decades

The overall analysis from 2004 to 2025 paints a clear picture: The majority of organizations fall within the middle range of the maturity scale. 35% have a security culture with room for improvement, while 30% have a good security culture. In contrast, 23% have insufficient maturity and 13% have very good maturity.

This points to a significant increase in professionalism across the board, but also to limitations on the path to excellence. Security culture is no longer a marginal issue in many organizations; however, a solid foundation does not automatically lead to a deeply rooted, cross-functional security culture.

Maturity levels as a framework for guidance

The levels were derived theoretically and validated empirically. They are not rigid categories, but rather reliable reference points for classifying differences and developments in organizational security culture.

Maturity level	Security Awareness Indicator (SAI)
Insufficient	<55
Developing	55 to 62.9
Good	63 to 69.9
Very good	>=70

Table 1: Maturity levels and their thresholds

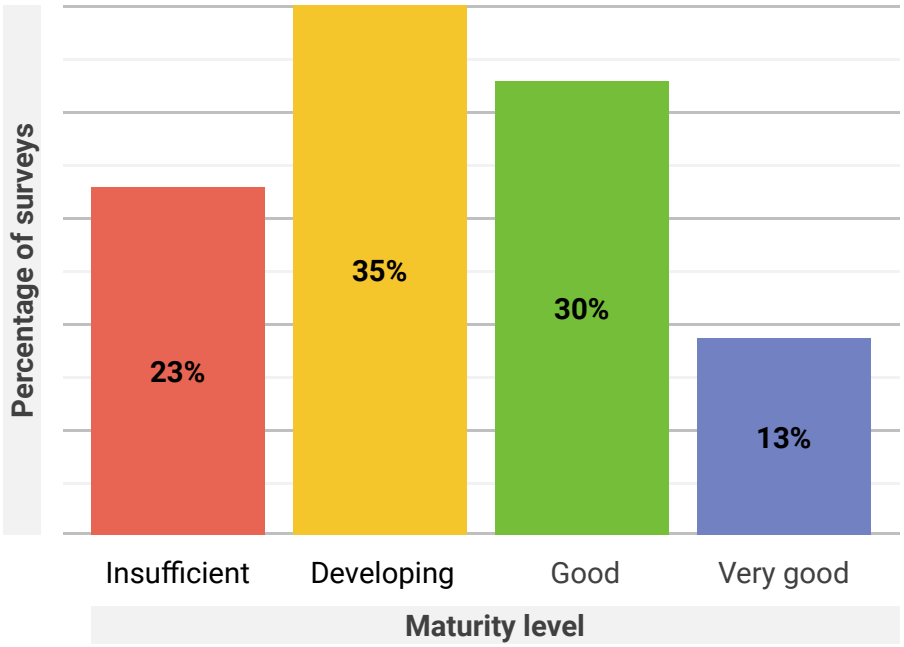


Figure 1: Distribution of maturity levels, 2004–2025

2.1 Differentiation by domain: What are the differences?

The twelve domains show that levels of maturity do not differ primarily in terms of knowledge or general values. These values are already comparatively high even at lower levels of maturity. The most significant differences arise when security is integrated into day-to-day organizational operations.

The distances are particularly large in:

- Communication: from 30 to 68 points
- Leadership: from 39 to 62 points
- Training: from 29 to 67 points
- Work and technology design: from 46 to 74 points

Greater maturity thus arises above all in environments where security is not only discussed but also structurally supported, made visible, and championed by leadership.

In practice, this means: It is not knowledge alone that matters, but whether security is communicated clearly, exemplified in day-to-day leadership, and embedded in processes, tools, and routines.

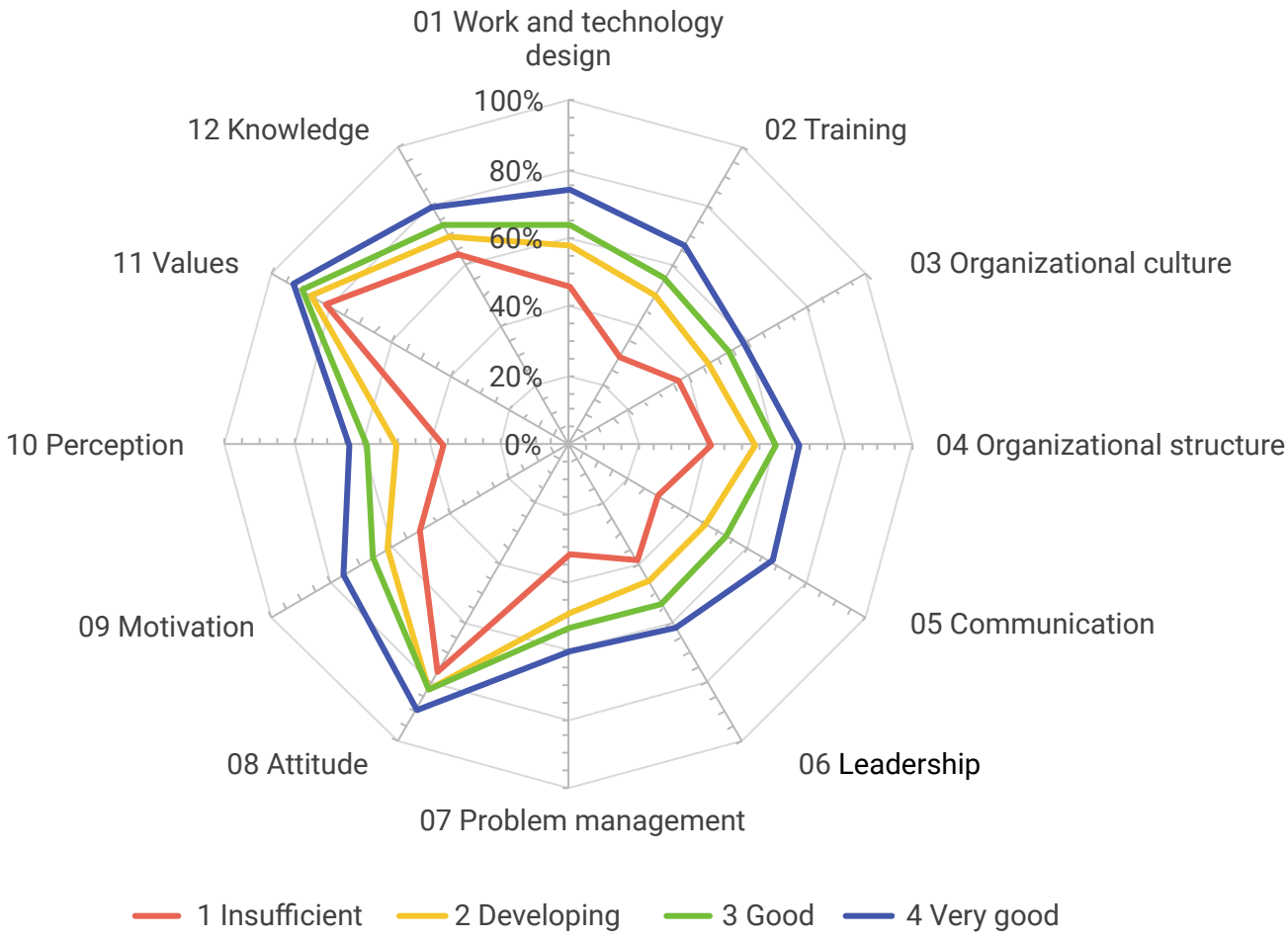


Figure 2: Domain adoption, 2004–2025, by maturity level

2.2 The three eras of security culture

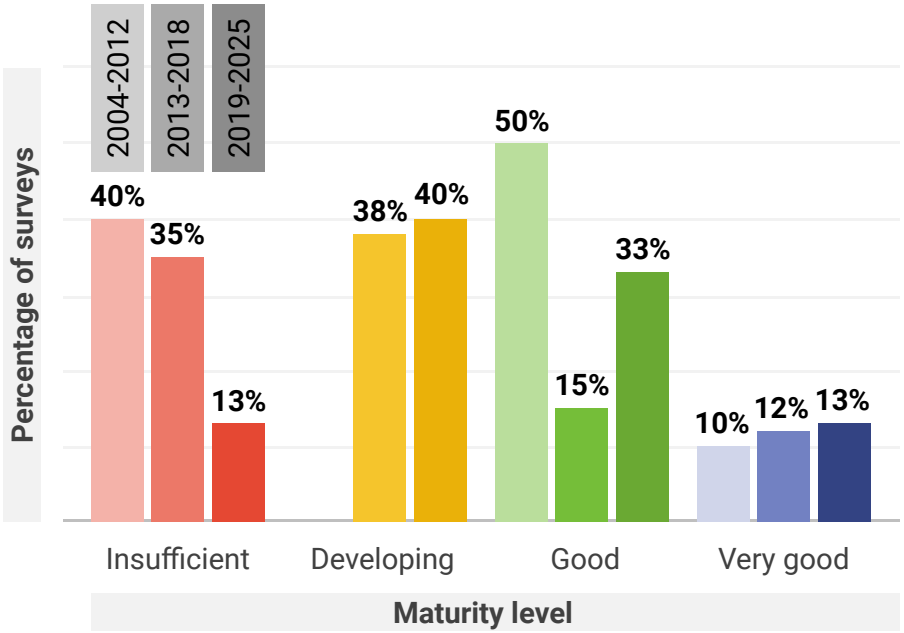


Figure 3: Distribution of maturity levels by era
Note: Percentages are rounded; therefore, the totals do not always add up to exactly 100%. During the 2004–2012 period, there was no survey with a maturity level of "2: Developing."

The glass ceiling to excellence

Throughout the entire observation period, the proportion of organizations with a very high level of maturity has remained remarkably stable, fluctuating only between about 10% and 13%. While many organizations can now achieve fundamental progress, the transition to a deeply rooted, cross-functional security culture remains a significantly greater challenge.

To analyze long-term trends, the data was divided into three time clusters:

1. 2004–2012: Pioneering phase

In many places, security awareness was still dominated by technical security approaches and formal compliance. About 40% of organizations had an inadequate security culture. Awareness initiatives were often ad hoc and rarely embedded as an ongoing management or oversight responsibility.

2. 2013–2018: Professionalization

With the rise of phishing, digital work models, and international security standards, the human factor has come into sharper focus. The proportion of organizations with inadequate security cultures fell to 35 percent. At the same time, a large number of organizations still had room for improvement in this area. The issue has gained broader attention, though high levels of maturity have not yet become widespread.

3. 2019–2025: Modernity & resilience

The proportion of inadequate security cultures has dropped significantly to 13%, while one-third have reached the "good" level. Driven by regulatory pressure (NIS2, DORA, revDSG) and the realization that cyber resilience is a top priority, security culture is becoming an integral part of overall management rather than merely a technical afterthought. As a result, organizational resilience is finally taking center stage in strategic focus.

Across all three phases, a dual pattern emerges: clear professionalization across the board, but persistent limitations at the top. Weak performance is declining; very high maturity remains rare.

2.2.1 Stability within maturity levels

A key finding is the relative stability of approval ratings within each maturity level. The maturity levels thus describe not merely snapshots but relatively stable states of organizational security culture. Change is primarily evident in the distribution of organizations across the levels, not in a fundamental change in the levels themselves.

Maturity level	Security Awareness Indicator (SAI)		
	2004-2012	2013-2018	2019-2025
Insufficient	48.9	49.7	48.5
Developing	-	59.6	60.2
Good	65.9	66.8	66.5
Very good	74.3	73.9	74.7

Table 2: Average SAI by maturity level and era
Note: During the 2004–2012 period, there were no surveys with a maturity level of "2: Developing."

The average SAI rises from 43.8 points in 2005 to 65.2 points in 2025. The lower values observed during the middle phase can plausibly be explained by a broader and more heterogeneous data set. In the early years, participants tended to be organizations that were already more deeply engaged with the topic. The fact that the scores in the current period—despite greater heterogeneity—are once again reaching or exceeding the early levels suggests a substantial increase in professionalism across the board.

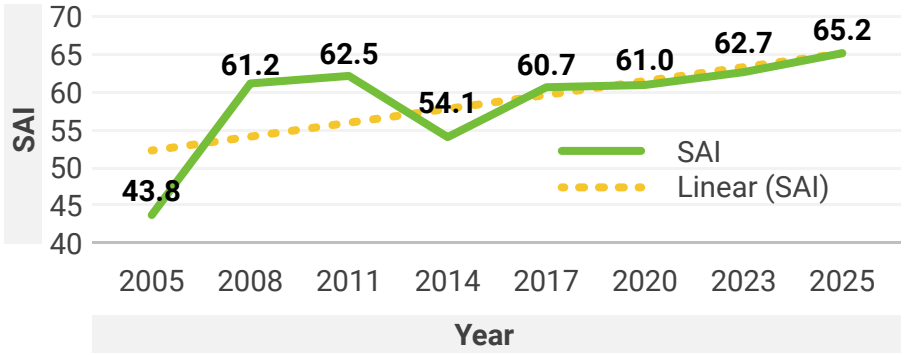


Figure 4: The average SAI from 2004 to 2025
Note: Data has been aggregated in 3-year intervals, except for the last year. The dashed line shows the trend.

Domain	Approval rating		
	2004-2012	2013-2018	2019-2025
01 Work and technology design	56	56	63
02 Training	47	49	53
03 Organizational culture	55	45	49
04 Organizational structure	56	48	59
05 Communication	47	43	51
06 Leadership	49	51	49
07 Problem management	37	44	52
08 Attitude	81	81	82
09 Motivation	63	61	63
10 Perception	57	45	55
11 Values	88	85	89
12 Knowledge	72	70	73

Table 3: Average domain agreement by era

2.3 Longitudinal development trajectories (case studies)

The analyses conducted so far reveal robust patterns at the aggregate level. In practice, however, it is equally important to understand how security culture evolves within individual organizations over the years. Complementing the broad-based analysis, three case studies (Keller, 2026) now demonstrate how maturity trajectories can vary—ranging from gradual improvement to leaps in maturity to short-term fluctuations.

Comparability over time

For the case studies, only those items that were identical across all four measurements were included in the calculation of SAI and domain scores for each organization. This approach follows the anchor-item method and prevents bias caused by varying sets of questions. Depending on the organization, 17 to 27 anchor items were included.

2.3.1 Case study: Organization A

A

Organization profile: Nationally active organization with 1,000–5,000 employees, Sector 3

Time period: 2012 bis 2025 (13 Years, 4 Measurement times)

SAI development: from 54.6 to 66.6 points, or +12.0 points, or about +22%

Organization A shows a clearly positive overall trend. After a largely flat trajectory between 2012 and 2017, the SAI score rose significantly in the second half of that period. Progress is particularly evident in organizational structure, leadership by example, communication, and knowledge. At the same time, the “Attitude” domain declined significantly. This case demonstrates that substantial progress toward maturity is possible, but it does not occur simultaneously across all areas.

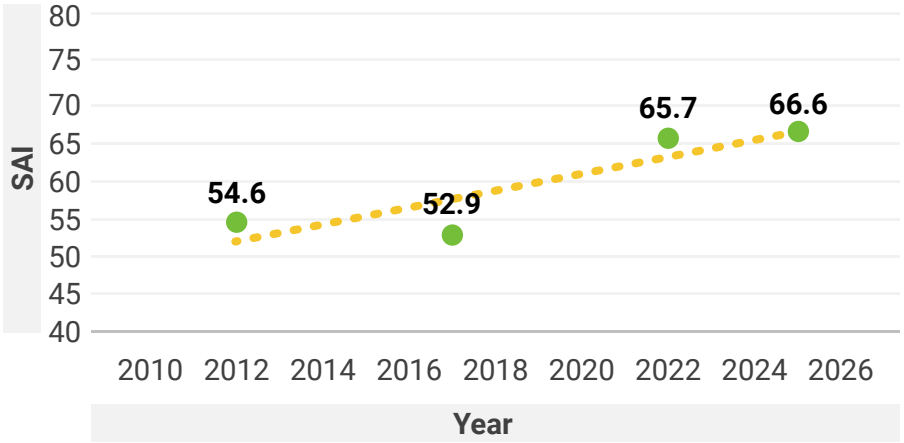
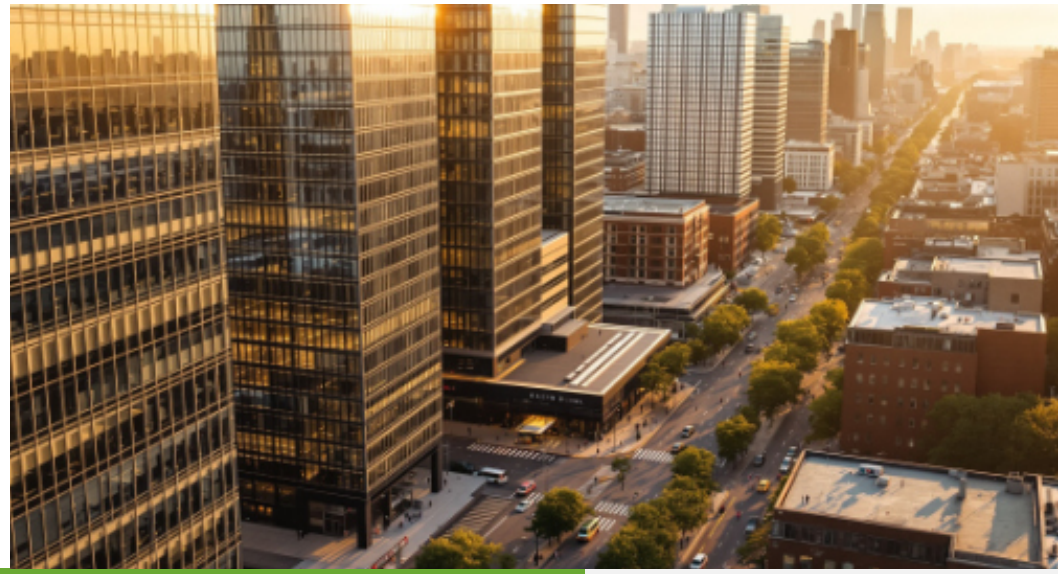


Figure 5: Organization A: SAI development across four measurements (The dotted line represents the trend.)

Domain	2012	2025	Change
Organizational structure	34	63	+29
Knowledge	58	79	+21
Leadership	44	64	+20
Communication	49	67	+18
Problem management	41	58	+17
Training	56	73	+17
Attitude	83	50	−33

Table 4: Organization A: Selected changes at the domain level (in points). Note: The figure shows selected domains with particularly noticeable changes between the first and last measurement points. The values are scores on a scale from 0 to 100.



TreeSolution

2.3.2 Case study: Organization B

B

Organization profile: Multinational organization with 25,000–50,000 employees, Sector 2

Time period: 2016 to 2023 (7 years, 4 measurement points)

SAI development: from 49.1 to 71.1, or +22.0 points, or +44.8%

Organization B shows the most significant leap in maturity among the three cases. Its development encompasses several domains central to cultural maturity simultaneously. Training, awareness, communication, and problem management show particularly strong improvements; work and technology design, as well as attitudes, also improve significantly. This case demonstrates that major leaps in maturity occur particularly when multiple organizational and communicative levers are activated simultaneously.

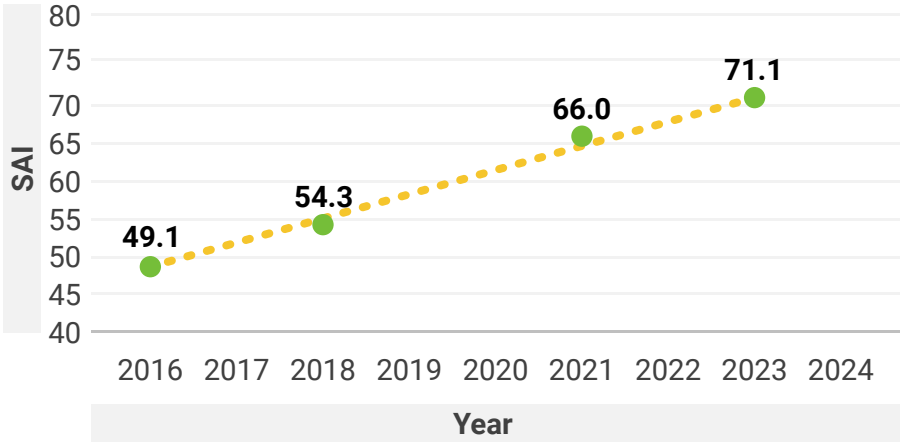


Figure 6: Organization B: SAI development across four measurements (The dashed line represents the trend.)

Domain	2016	2023	Change
Training	20	66	+46
Perception	25	61	+36
Communication	28	61	+33
Problem management	42	70	+28
Work and technology design	47	73	+26
Attitude	52	76	+24

Table 5: Organization B: Selected changes at the domain level (in points). Note: The figure shows selected domains with particularly noticeable changes between the first and last measurement points. The values are scores on a scale from 0 to 100.

TreeSolution

2.3.3 Case study: Organization C

C

Organization profile: Multinational organization with 5,000 to 25,000 employees, Sector 2

Time period: 2022 to 2025 (4 years, 4 measurement points)

SAI range: between 55.3 and 61.4, a total of 6.1 points or 11%

Organization C is evaluated annually; this makes short-term fluctuations more visible. The SAI rises from 55.3 to 61.4 and falls back to 57.7 in 2025. The trend should therefore be interpreted as short-term volatility rather than a stable long-term trend. The results make it clear: While structural adjustments often have a lasting effect, successes in communication and leadership are highly fleeting and require constant management to prevent a return to the initial level within a year.

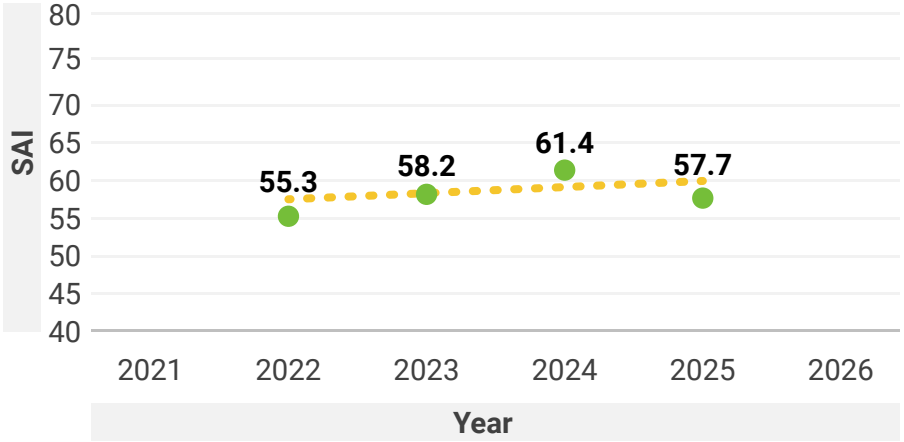


Figure 7: Organization C: SAI development across four measurements (The dashed line represents the trend.)

Domain	2022	2024 (Peak)	2025	Balance sheet
Structural domains				
Work and technology design	58	66	68	+10 (Sustainable)
Problem management	58	67	63	+5 (Moderate)
Social domains				
Perception	41	48	42	+1 (Fleeting)
Leadership	48	57	48	0 (Fleeting)
Communication	46	53	46	0 (Fleeting)

Table 6: Organization C: Selected changes at the domain level (in points). Note: The chart shows selected domains that are particularly indicative of short-term trends. The values are scores on a scale from 0 to 100.

2.3.4 Conclusions from the case studies

Security culture develops very differently from one organization to another. Progress does not result from the passage of time alone, but rather occurs primarily where organizational, communicative, and leadership-related conditions work together. At the same time, developments do not always follow a linear path: In addition to long-term improvements, short-term fluctuations may also occur—especially when measurements are taken at frequent intervals—but these should not be taken as evidence of a stable trend.

3. The anatomy of security culture (2019–2025)

Chapter 3 focuses on the time frame from 2019 to 2025 because this period best reflects today's organizational, technological, and regulatory conditions. The goal is to provide a practical analysis of current patterns and differences across organizational contexts.

3.1 Current overview of the security culture

The current period presents a mixed picture: The baseline level has improved, yet at the same time, a large portion of the sample remains concentrated in the mid-range of maturity. It is precisely this broad middle range that is crucial in practice, because here the challenge lies not so much in a lack of basic awareness as in further embedding the culture.

The distribution is clear: 40% of organizations have room for improvement, 33% are good, 13% are inadequate, and 13% are very good. Fundamental requirements of security culture are thus established in many organizations; however, the transition to cultural excellence is achieved significantly less often.

In terms of content, the threshold for cultural excellence lies less in basic attitudes or knowledge—these are already at a high level even at the lower stages. The real differentiation occurs in the organizational and communicative domains. The greatest gaps between an inadequate and a very good security culture are evident in training, communication, and leadership by example. Work and technology design also contribute significantly to increasing the maturity level, while problem management becomes particularly important when moving into the intermediate maturity levels.

In practice, this means: Knowledge remains an essential foundation. However, the next stage of maturity occurs primarily where security is communicated more visibly, exemplified in day-to-day leadership, and embedded in processes and working conditions.

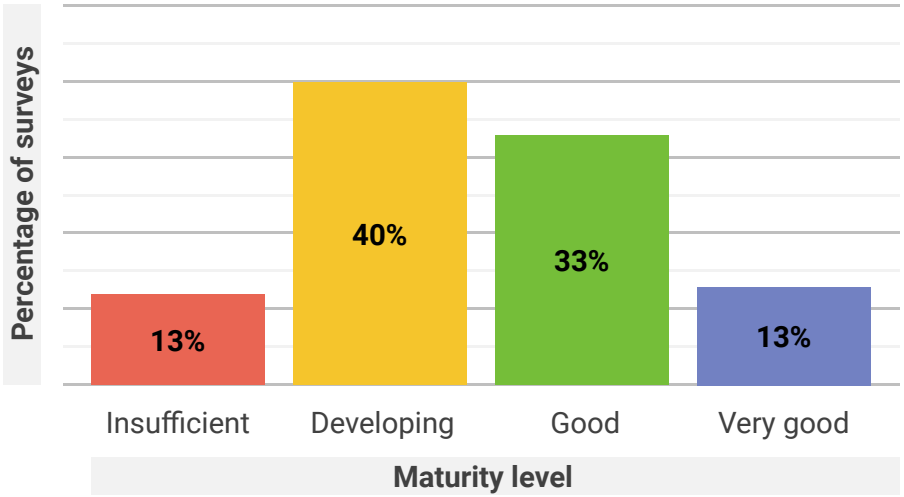


Figure 8: Distribution of maturity levels, 2019–2025

Domain	Approval rating			
	Insufficient	Developing	Good	Very good
01 Work and technology design	49	59	65	76
02 Training	28	50	56	69
03 Organizational culture	33	47	52	58
04 Organizational structure	43	58	62	65
05 Communication	29	48	54	68
06 Leadership	32	43	55	63
07 Problem management	35	51	58	61
08 Attitude	80	80	81	90
09 Motivation	45	62	65	76
10 Perception	39	52	59	62
11 Values	83	88	90	95
12 Knowledge	62	70	75	81

Table 7: Average domain agreement, 2019–2025

3.1.1 What is evident at the level of statements?

To supplement the domain analysis, individual statements were examined that were available in a sufficiently comparable form from at least 20 different organizations between 2019 and 2025. The statement level illustrates specific strengths and weaknesses in day-to-day security; the systematic comparative analysis deliberately remains at the domain level.

Statement	Consent	Perspective
Do not share passwords	94	self-centered
Be cautious with suspicious emails	93	self-centered
Everyone's responsibility	89	posture
Do not discuss confidential matters (in public)	88	self-centered
Do not use work email for personal purposes	83	self-centered

Table 8: Statements that are particularly strong

Statement	Consent	Perspective
Measures are explained by supervisors	39	leadership
There are policies for reporting security breaches	46	organization
Information for new employees	51	organization
The information is easy to understand	51	organization
Training for current employees	53	organization

Table 9: Statements that are comparatively less emphatic

The pattern is clear: High scores are found in fundamental security-related behavioral norms and personally accountable expectations. Lower scores are evident in areas where security must be communicated, explained, and made understandable within the day-to-day work environment. Many organizations thus have a solid foundation of discipline, while the ongoing translation of this into leadership, communication, and empowerment remains more challenging.

Note on interpretation

The highly rated statements primarily relate to one's own behavior or personal attitudes; those rated lower more often relate to the organization, leadership, or support structures. Differences should therefore be interpreted not only as strengths or weaknesses in terms of content, but also in light of social desirability, self-attribution, and a more critical assessment of the organizational environment.

3.1.2 In-Depth connections between the domains of security culture

A culture of security cannot be reduced to isolated domains. The analyses reveal recurring patterns across multiple areas of action:

Leadership and perception

Where leadership visibly supports, exemplifies, and prioritizes information security, awareness of information security is also more pronounced. Leadership is therefore not an ancillary factor, but rather a central reference point for how security is integrated into everyday life.

Communication and training

These two areas frequently appear as closely linked areas of development. Communication without learning opportunities often remains abstract; training without a communicative context often has only a limited impact. An integrated approach combining communication, empowerment, and regular learning opportunities is the most sustainable.

Values and attitudes

These two domains form a coherent cultural core. Where security is embraced as a shared value, attitudes toward security-related behavior are typically more positive.

Motivation and problem management

Motivation stems from the practical feasibility of actions and a professional approach to incidents. Employees are more committed when processes are clear in an emergency and when they experience the effectiveness of their actions through direct feedback on their reports. A strong tolerance for mistakes is also crucial: This “psychological security” ensures that lessons can be learned from mistakes, rather than hiding them out of fear of punishment.

Structural integration

Improvements over time are often accompanied by clear responsibilities, processes, and structures. Cultural development becomes sustainable when it is institutionally embedded.

Overall, the findings can be summarized into four areas of development **relevant to practice:**

1. Leadership and perception
2. Communication and empowerment
3. Values and cultural roots
4. Manageability and psychological security

3.1.3 Evidence of a more critical assessment of leadership implementation by team leaders

The importance of leadership is evident not only in the context of domains but also from a hierarchical perspective. Team leaders (Position 2) tend to evaluate the implementation of security guidelines by their direct reports (Position 3) more critically than employees (Position 1) evaluate their team leaders, and than middle or upper management evaluates top leadership. In ten out of twelve cases, Position 2 ranks below Position 3; in seven out of twelve cases, it also ranks below Position 1.

This is relevant in practice because team leaders serve as the link between policy and operational implementation. More critical assessments point to inefficiencies in translating security requirements into day-to-day management practices.

Perspective	Level of management being evaluated	Consent
Position 1	Employees evaluate team leaders	46.1
Position 2	Team leaders evaluate middle/upper management	42.2
Position 3	Middle/upper management evaluates top leadership	50.5

Table 10: Agreement scores for Items in the "Leadership" domain by hierarchical level

3.2 Sector-specific dynamics: When expertise does not automatically lead to cultural maturity

A sector-by-sector analysis puts into perspective the widespread assumption that technology-oriented or information-intensive organizations are automatically more culturally mature. In the industrial sector, 94% of organizations fall between “room for improvement” and “good.” In the knowledge-intensive sector, however, 50% are rated as “insufficient.” At first glance, this seems surprising, since one would expect a high level of security awareness in that sector. The domain scores put this into perspective: The knowledge-intensive sector scores 67 points in the “Knowledge” domain, but this is lower than the service sector’s 75 points and slightly below the industrial sector’s 70 points. The differences are even more pronounced in the cultural and organizational domains: Communication 37, Leadership 33, and Organizational Culture 38.

This finding is particularly relevant in practice because it corrects a common misconception: technical expertise is no substitute for cultural guidance. When security is viewed primarily as the responsibility of individual specialists, shared direction, leadership signals, and social integration often remain weaker.

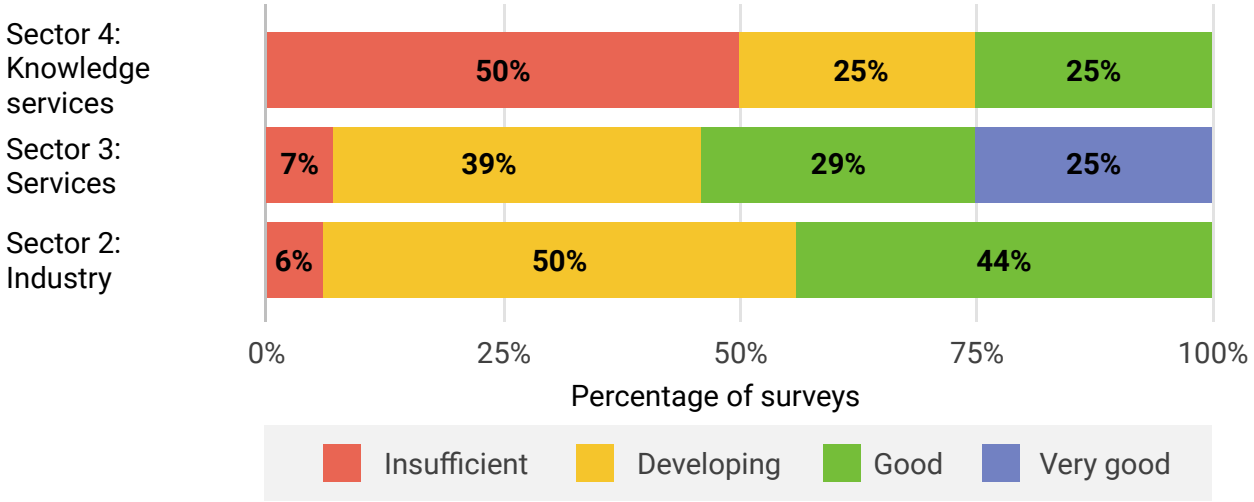


Figure 9: Maturity levels by sector, 2019–2025

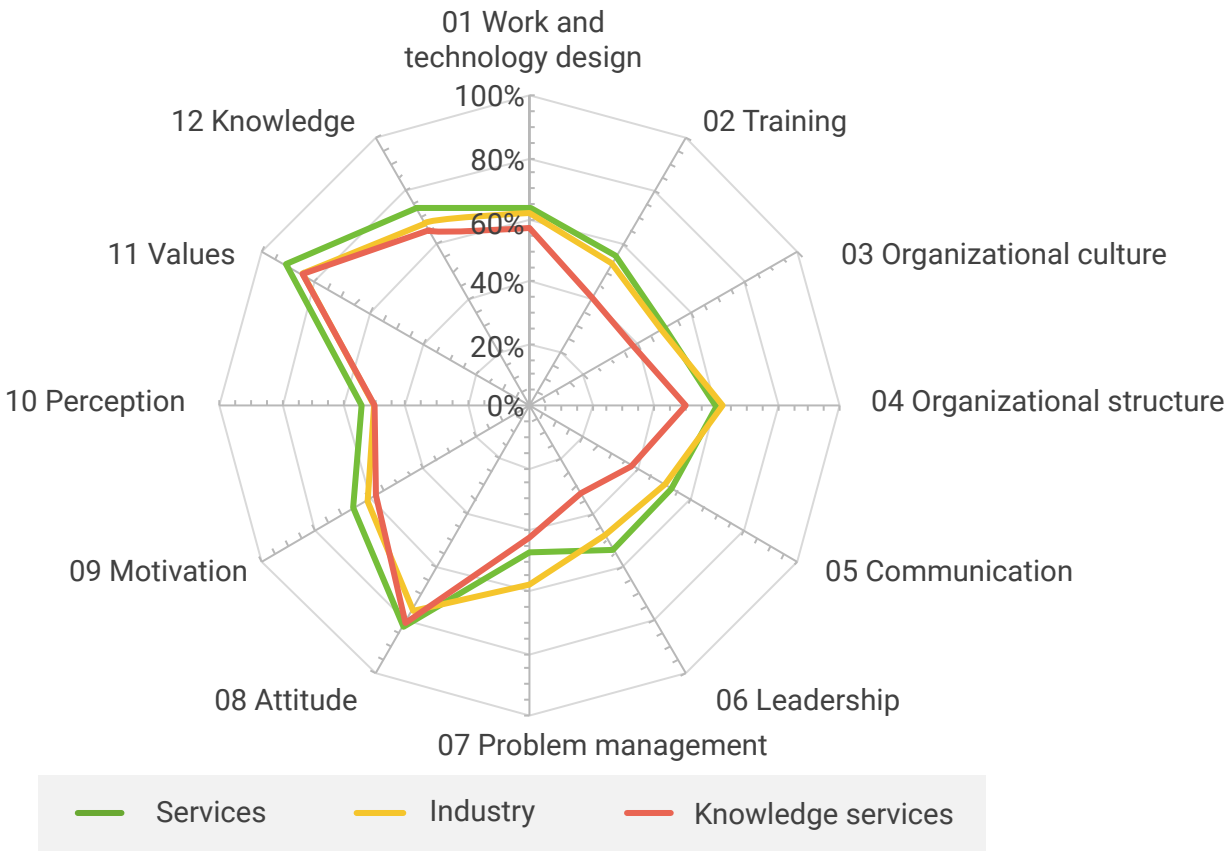


Figure 10: Domain adoption by sector, 2019–2025

Sector 4 is not “weaker,” but rather organized differently in cultural terms

The lower scores in communication and leadership often reflect a specific organizational logic. Drawing on Handy’s (1993) cultural types, such contexts more frequently prioritize individual autonomy and expert status over formal hierarchy. In such structures, central control signals often have less impact. The challenge here is not a lack of knowledge, but rather the collective translation of this knowledge into binding behavioral norms within an expert organization.

3.3 International presence and cultural maturity

The distinction based on multinational status provides another important insight. Multinational organizations are more likely to achieve a high or very high level of security culture than organizations that operate solely at the national level.

This advantage is particularly evident where security culture benefits from clear processes, scalable measures, and consistent implementation—for example, in the design of work processes and technology, communication, and knowledge management. This speaks less to the general superiority of multinational organizations than to the impact of formalized structures. Where security programs are embedded in governance, reporting, and standardization frameworks, security is more likely to be organized systematically rather than on an ad hoc basis.

In practice, it is not multinationality that is decisive, but rather the management logic often associated with it: more binding frameworks, greater pressure to provide evidence, standardized rollouts, and the consistent translation of security requirements into recurring processes. However, cultural excellence does not arise automatically from this. It develops only when these structural prerequisites are brought to life through visible leadership, local integration, and active communication.

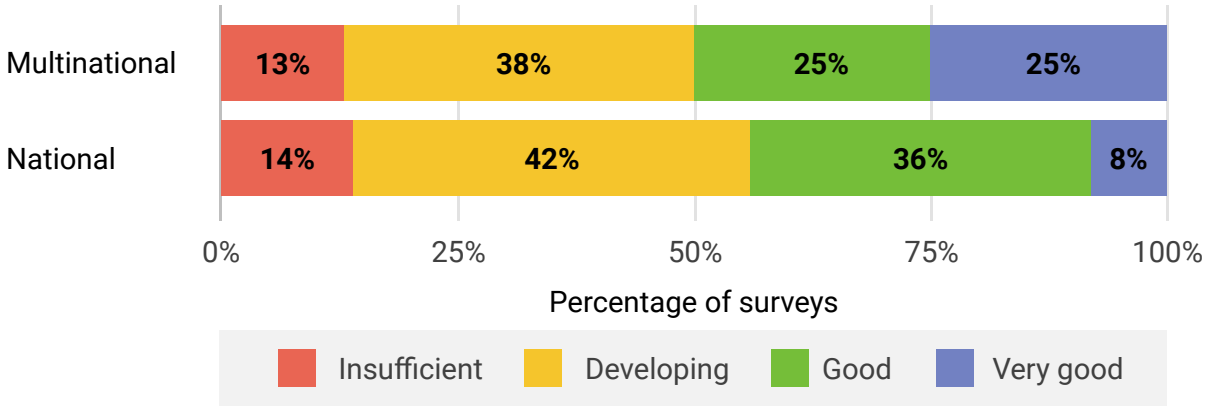


Figure 11: Maturity levels by multi-nationality, 2019–2025

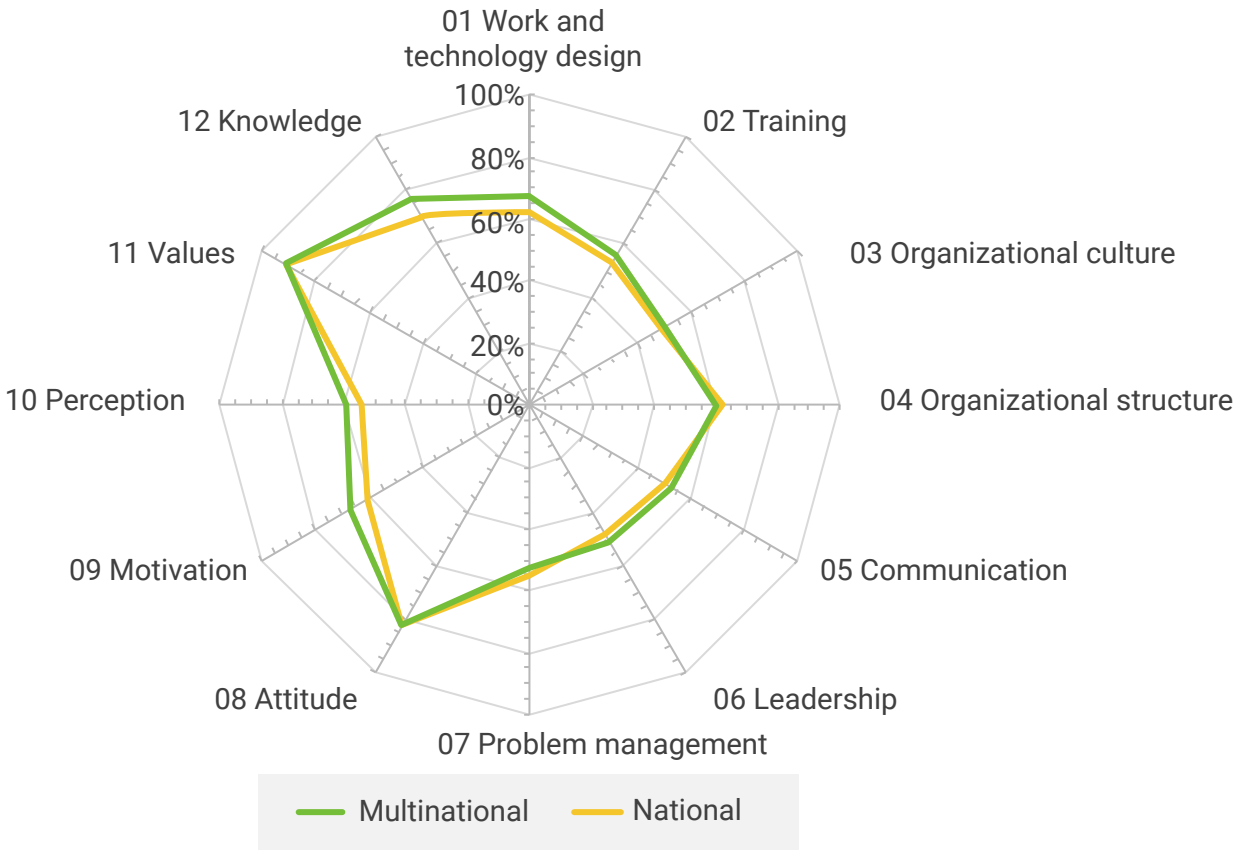


Figure 12: Domain agreement by multi-nationality, 2019–2025

A competitive edge through systems, not geography

The observed lead is primarily due to system logic, not geography. Shared frameworks, standardized routines, and consistent reporting create the conditions under which leadership and communication can be culturally effective.

3.4 The tension between organizational strength and expert autonomy

Sectoral and international comparisons reveal a common area of tension. A comparison between multinational organizations and knowledge-intensive organizations in Sector 4 reveals two distinct logics of cultural maturity. On the one hand, there are organizations that rely heavily on systems, standardization, and formalized processes to manage security. On the other hand, there are contexts in which professional autonomy, expert status, and decentralized problem-solving have a stronger influence on organizational behavior.

Multinational organizations benefit from the systematic rollout, documentation, and standardization of security requirements across all locations. This creates a sense of commitment and makes it easier to translate security goals into routines. Knowledge-intensive expert environments often exhibit a different pattern: Security is a natural part of the field, but it is viewed more as the responsibility of informed individuals than as a shared cultural norm. As a result, communication, leadership by example, and organizational embedding often remain weaker.

In practice, this comparison is revealing:

- Organizations with strong systems run the risk of formalizing security effectively but narrowing their focus too much on compliance and process adherence.
- Organizations driven by experts often possess a high level of technical expertise, but underestimate the importance of shared commitment and clear leadership signals.

In both cases, greater maturity is achieved only when formal requirements or individual expert knowledge are transformed into a shared, communicatively conveyed, and leadership-supported security culture.

3.5 From knowledge transfer to organizational awareness

A consistent pattern emerges across all maturity levels: High scores in knowledge and security-related attitudes are not sufficient to achieve cultural excellence. Even at the “insufficient” level, attitudes and values are comparatively high. Although knowledge also increases across the maturity levels, it does not sufficiently explain the difference between “solid” and “very high” maturity.

The real difference is more pronounced in those areas where security is visibly communicated, exemplified by leadership, and embedded in day-to-day organizational life. Therefore, the transition from “room for improvement” to “good” or “very good” depends less on expanding the scope of content and more on the quality of its organizational integration—particularly in communication, leadership by example, problem management, and the design of work processes and technology.

In practice, however, this does not mean that training is becoming less important. It remains an essential foundational tool for building knowledge, raising awareness, and ensuring minimum standards. Once a certain level of maturity has been reached, however, further progress is rarely achieved through more content alone, but more often through visible leadership attention, credible role models, a learning-oriented approach to incidents, and better integration into work processes.

The maturity lever: Attention reinforces what training prepares us for

In many organizations, knowledge and core values are already at a considerable level. The next step in maturity therefore often does not come from additional content alone, but rather from making security more visible in everyday life: when leadership discusses security, incidents are used as learning opportunities, and safe behaviors are embedded in processes and routines. Awareness does not replace training; it enhances its cultural effectiveness.

4. The roadmap to cultural maturity: Strategic recommendations for 2026–2030

The roadmap to cultural maturity

Data spanning two decades shows that there is no one-size-fits-all solution for a strong security culture. Which measures yield the greatest benefits depends on the organization's level of maturity and its organizational logic. Nevertheless, it is possible to identify robust development paths.

1 Path 1: Laying the foundation

from Insufficient to Developing

Organizations at this level often already have some knowledge of security in specific areas, but have not yet managed to reliably incorporate it into their day-to-day operations. Security is viewed more as an additional burden than as a source of support. The first step in their development, therefore, is primarily to reduce friction and make it easier to integrate secure behaviors into their day-to-day operations.

- **Focus:** Work and technology design, supported by clear, straightforward communication
- **Measures:** Reducing cognitive load through single sign-on, password managers, intuitive ways to report phishing, clear standard processes, and easy-to-understand guidance at the moment of action
- **Goal:** To make security a matter of course—shifting it from an individual burden to an organizational priority

2 Path 2: Closing the "attention gap"

from Developing to Good

This is the largest group in the dataset. Basic compliance is generally in place, but security too often remains confined to the line of business and does not receive enough visibility in day-to-day management. The next step in maturity arises less from additional content than from its tangible integration into communication, leadership, and day-to-day management.

- **Focus:** Setting an example and communication
- **Measures:** Regular security updates during town hall meetings and line-of-business sessions, brief management updates, integration of security into existing leadership routines, and visible references to incidents and lessons learned rather than isolated awareness campaigns
- **Goal:** To bring security out of the IT niche and into general management communication and day-to-day business operations

3 Path 3: Breaking through the “glass ceiling”

from **Good** **to** **Very good**

Organizations at this level have achieved basic stability. The remaining gap to cultural excellence lies less in additional sets of rules than in the quality of their social embeddedness. A learning-oriented culture of error, credible leadership, and motivation that goes beyond mere fulfillment of duties are crucial.

- **Focus:** Problem management, motivation, and cultural adaptability
- **Measures:** Establishing a positive reporting culture, systematically using near-misses as learning opportunities, security champion networks, team-based reflection sessions, and visible recognition of desired behavior
- **Goal:** To embed security as part of organizational identity, collective learning, and professional pride

4 Path 4: The strategy for expert cultures

Special feature of Sector 4

For knowledge-intensive professional organizations, Paths 1 through 3 are only fully effective if they are adapted to the organizations’ specific organizational logic. A high degree of professional autonomy and a strong expert culture can support security culture, but often make centralized control and traditional top-down communication more difficult.

- **Focus:** Decentralized implementation, peer-to-peer communication, and professional legitimacy
- **Measures:** Engaging recognized subject-matter experts, translating security requirements into the language of each profession, team-oriented discussion formats, communities of practice, and standards that are perceived as a mark of quality rather than as external bureaucracy
- **Goal:** Position security as an expression of professional excellence rather than as an administrative obstacle

Which development path is right for your organization?

The roadmap is not a standard linear program. The key factor is which bottleneck is currently the greatest constraint on further development:

- If uncertainty or circumvention arises from high levels of everyday friction, the focus is on simplification and technical safeguards.
- If basic compliance is already in place, visible leadership attention becomes the key driver.
- If the organization is already taking a proactive approach, its learning culture, motivation, and credible leadership will determine the next step in its development.
- In expert-driven cultures, all measures must also be professionally sound and have decentralized legitimacy.

5. Final thoughts: Actively shaping the Culture Code

An analysis of 20 years of Security Awareness Radar data makes it clear: The **Security Culture Code** is not a static set of rules, but a dynamic management model. The analysis of two decades demonstrates a significant level of professionalization across the board, but also highlights the glass ceiling to cultural excellence.

The key insight: The next stage of maturity does not fail due to a lack of knowledge, but rather because of the visibility and manageability of security in everyday life. The necessary knowledge is usually in place; the difference lies in the social and organizational dimensions: in leadership setting an example, the consistency of communication, and the quality of problem management.

This results in a sophisticated control logic:

- Security culture develops differently depending on the organizational context.
- A higher level of maturity is achieved only when leadership, communication, and empowerment are integrated into the system.
- Progress does not result from isolated projects, but rather from targeted efforts to create the conditions under which safe behavior becomes a consistent part of everyday life.

For decision-makers, measuring the level of maturity is not an end in itself, but rather a starting point. Those who integrate the **Security Culture Code** into their strategy develop a resilience that goes far beyond simply checking off compliance checklists. Security thus becomes an integral part of how organizations manage accountability, collaboration, and future-readiness.

Practical check: Three implications for the awareness strategy

Measure maturity regularly and make progress visible

Maturity assessments should be repeated at appropriate intervals and, whenever possible, integrated with existing risk or governance processes. This allows for the earlier detection of stagnation, plateau effects, or new vulnerabilities, enabling more targeted corrective actions.

Using leadership as a cultural amplifier

The findings suggest that differences in leadership by example and communication are particularly relevant at higher levels of maturity. Security should therefore be visibly incorporated into leadership routines, management communication, and cross-functional priority-setting—not just in training programs.

Use benchmarking as a guide, not as an end in itself

Comparing oneself to similar organizations or sectors can help provide a more realistic assessment of one's own level of development. However, what matters most is not one's ranking, but rather which bottleneck is currently the greatest constraint on one's own maturity development and which measure promises the greatest progress under the given circumstances.

6 Methodological interpretation of the results

TREESOLUTION

88
Surveys

100k
Participants

4.5M
Individual responses

20
Years

The results are based on 88 organization-wide surveys conducted by the Security Awareness Radar (SAR) between 2004 and 2025. The data set includes over 100,000 participants and approximately 4.5 million individual responses.

The goal of the analysis is not to demonstrate universally valid causal relationships, but rather to provide a data-driven classification of recurring patterns, typical developmental trajectories, and practice-relevant differences between organizational contexts. The report is thus an empirically grounded practice report, not a comprehensive impact study.

6.1 Data source and analysis focus

With the exception of the case studies, the analyses are conducted at the aggregated organizational level. The focus is on mean values and distribution patterns across organizations, not on individual profiles.

For the case studies in Chapter 2, the entire period from 2004 to 2025 was used. Only organization-specific anchor items were considered—that is, only those questions that appeared in identical form at all measurement points for a given case.

For the in-depth analysis in Chapter 3, the focus is on the 2019–2025 time cluster, comprising 52 surveys, as this period best reflects today's organizational, technological, and regulatory conditions.

In addition to the descriptive analyses, correlations between the domains were analyzed in depth—across organizations and longitudinally. The goal was to reveal recurring patterns and identify those domains that particularly frequently occur in conjunction with positive developments in other areas. These results do not constitute strict proof of causality, but rather data-driven indications of stable and practice-relevant correlations.

For the hierarchy-related analysis, only those 34 surveys were considered in which ratings for all three hierarchy positions under consideration could be unambiguously assigned.

The sectoral classification follows the expanded sector theory. The dataset includes organizations from the **industrial sector (Sector 2)**, the traditional **service sector (Sector 3)**, and the knowledge-intensive quaternary sector **(Sector 4)**. There were no cases in the primary sector.

6.2 Derivation of the maturity levels

Classification is performed using a four-level maturity model based on the SAI, which is derived from agreement scores across twelve domains of security culture.

The scores are based on an agreement-based scoring system at the level of individual questions. Response categories are converted into numerical values; strong agreement receives the highest score, while “somewhat agree” responses receive correspondingly lower sub-scores. Domain scores are derived from the average of the corresponding individual questions and form thematic profiles. The Security Awareness Indicator (SAI) is calculated separately as an aggregated total score based on all included individual questions, not as an average of the domain scores. This allows for a consistent representation of thematic strengths and weaknesses at the domain level, as well as the overall state of the security culture.

The four stages of maturity serve as a framework for guidance:

- **Level 1 – Insufficient:** Significant weaknesses in key areas
- **Level 2 – Developing:** basic awareness exists, but implementation is inconsistent
- **Level 3 – Good:** Security is firmly embedded in key areas of the organization and is clearly visible
- **Level 4 – Very good:** A high level of cultural maturity, with strong integration into leadership, communication, and daily routines

The thresholds were defined based on theory and further validated empirically using the distribution of organizational scores. They align well with observable clusters in the dataset.

6.3 Significance and limitations

The strength of the dataset lies in its long-term nature, its scale, and its close connection to organizational practice. This makes it possible to identify trends over two decades and to trace typical patterns across different organizational forms.

At the same time, the results should be interpreted with the caution appropriate for practical reports. The analyses describe correlations and differences between groups but do not allow for the unequivocal attribution of individual causes. Differences between sectors or organizational forms should therefore not be interpreted as rigid typologies, but rather as indications of different starting points and management logics.

Furthermore, individual subgroups vary in size, and the composition of the sample has changed over the years. The report therefore deliberately focuses on robust patterns and consistent differences, rather than on maximizing the statistical differentiation of each subgroup.

6.4 Reference to the in-depth methodological foundation

The more comprehensive methodological foundation and the detailed elaboration of the case studies are not the subject of this practical report but are presented in the corresponding foundational and in-depth studies (Schlienger, 2003, 2006; Keller, 2026).

It is essential for understanding this report to note that the underlying measurement logic has been methodologically validated and refined over several years. This paper builds on this foundation but deliberately focuses on the practice-oriented interpretation of the results and their strategic significance for organizations.

7 References

Handy, C. (1993). Understanding Organizations. Penguin Books.

Keller, D. (2026): Multiple Case Studies of the Security Awareness Radar—Development, Validation, and Question Selection. Master's thesis as part of the MAS in Business Psychology. Zurich: Kalaidos University of Applied Sciences Switzerland.

Schlienger, T. (2006): Informationssicherheitskultur in Theorie und Praxis – Analyse und Förderung sozio-kultureller Faktoren der Informationssicherheit in Organisationen. Doctoral dissertation, University of Freiburg (Switzerland), iimt University Press.

Schlienger, T. & Teufel, S. (2003): Information Security Culture – From Analysis to Change. In: Eloff, J., Venter, H., Labuschagne, L. & Eloff, M. (Eds.): Information Security South Africa – Proceedings of ISSA 2003, 3rd Annual Information Security South Africa Conference, 9-11 July 2003, Sandton Convention Center, Johannesburg, South Africa. ISSA: 183-195.

Additional practical resources

TreeSolution Security Awareness AG (o. J.): Measuring security culture and tracking changes. Available online at: TreeSolution, retrieved on April 7, 2026.

About TreeSolution

At TreeSolution, we are convinced that effective information security is a matter of organizational culture. To ensure that security is effective where it is needed, we view technology, processes, and people as an inseparable whole. Even the most advanced systems remain ineffective if the people who operate them lack the necessary awareness, the appropriate knowledge, and a well-established security culture.

What sets TreeSolution apart is the operational grounding of our solutions: We base our work on real data, clear facts, and two decades of systematic research. Our focus on the human dimension of information security makes us the leading partner in decoding and developing your security culture.

TreeSolution Security Awareness AG
Boesch 23
6331 Huenenberg
Schweiz

Phone: +41 58 510 98 00
Email: info@treesolution.com
Website: www.treesolution.com

Legal notices

TREESOLUTION
SECURITY AWARENESS SINCE 2005