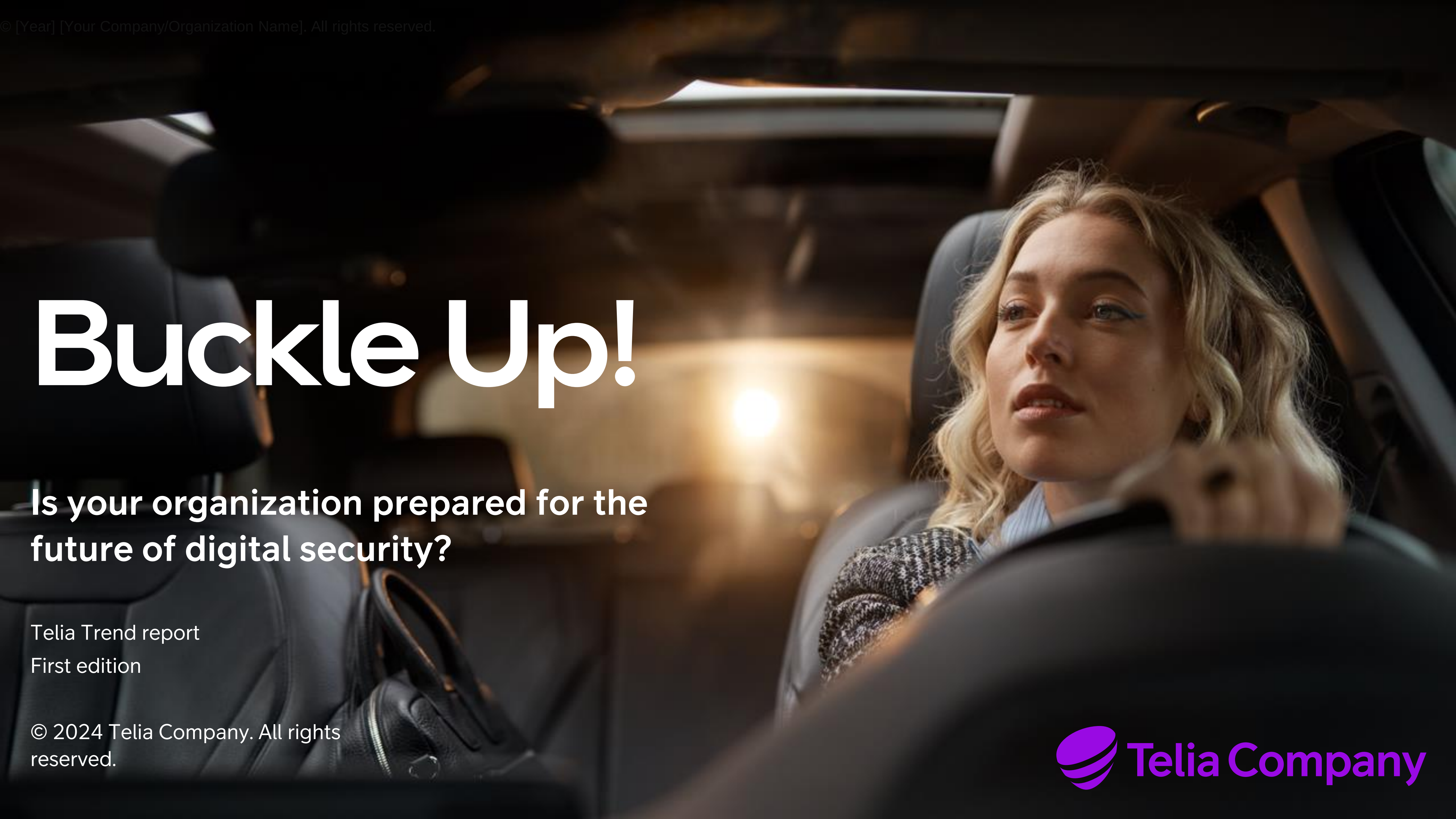
© [Year] [Your Company/Organization Name]. All rights reserved.



Buckle Up!

Is your organization prepared for the future of digital security?

Telia Trend report
First edition

© 2024 Telia Company. All rights reserved.

Telia Company

Contents

1st edition September 2024

“The importance of robust security measures has never been greater”

Patrik Hofbauer
Telia Company President & CEO

A word from our CEO

As our society becomes more connected, it gets increasingly vulnerable to digital threats. Hacker attacks and cyber-crime are escalating by the minute, and many organizations are lagging in digital security.

While some may feel that security is complex and costly, digital resilience actually improves business. It prevents expensive downtime caused by sophisticated cyberattacks and lowers the risk of data breaches that could harm both the company and its employees. In fact, safeguarding people’s data and privacy builds trust, which is especially important in times when data protection is at the top of the agenda. In every sector, everywhere, robust security creates significant advantage. And as digital security becomes increasingly important, it clearly deserves our attention.

As a leader in digital security, we at Telia know what it takes to build resilience. While technology and processes are important, our experience tells us that people are crucial too. Humans are easy to hack, and if you don’t get people onboard with security, it doesn’t matter how much you invest in tools and tech.

This report explores how people’s behaviors and emotions shape the state of digital resilience. By partnering with security experts, customers, and industry leaders, we have gained key insight into some of the challenges organizations face today – and developed hands-on advice on how to overcome them. Now, we want to share these insights to raise awareness, spark conversation and contribute to the constant journey of creating better connected living - together. We hope to inspire organizations everywhere to take action.

02

Setting the stage

The seatbelt of our time

In 1959, the three-point seatbelt was introduced, promising dramatically improved survival rates in car accidents. Despite awareness campaigns and the automobile industry's quick uptake, public adoption lagged. Why? Changing habits is a challenge, even when it’s a matter of our own survival.

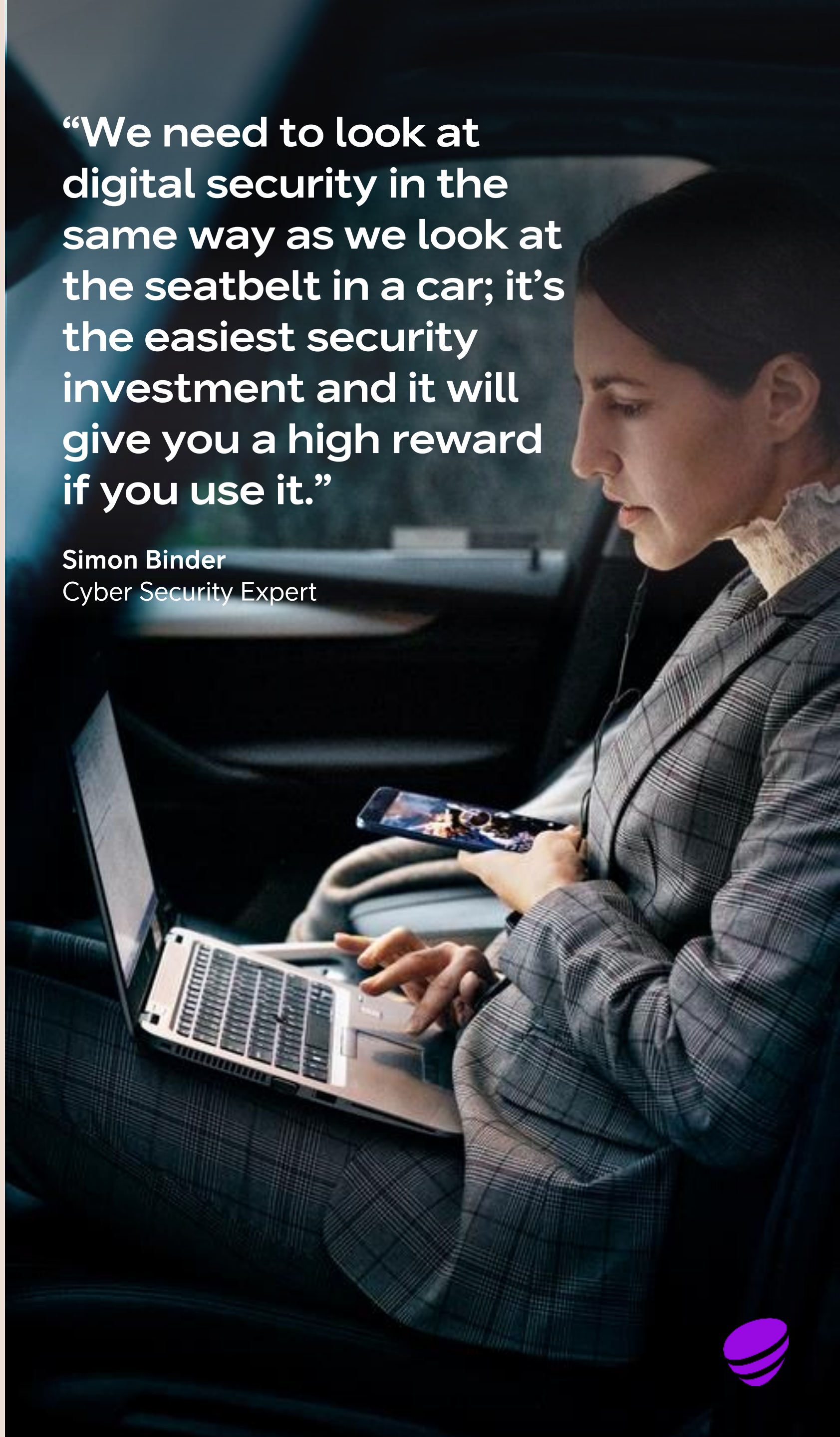
In our fully digital world, we face threats that are a lot more complex and abstract than traffic accidents. But much like with cars and seatbelts, digital security is largely an afterthought. We have been speeding on the digital highways, naively disregarding the risks.

The slow but ultimately widespread public adoption of the seatbelt serves as a powerful reminder of a few elementary truths about innovation, people and security:

- In the highly competitive development and diffusion of a new, hot and often poorly understood technology, security - if existent - is rarely a top concern for anyone involved. Only gradually, when the downsides of the technology are apparent, does security get the attention it deserved all along.
- Even when security measures do exist, there are no guarantees that we will readily embrace them in a way proportional to the risks presented by the technology.
- Security as a concept and practice is often intangible and must be simplified and made concrete for us to take notice, understand, care and act.

Unlike in traffic, the digital threat is deliberate: cybercriminals actively target victims with increasing efficiency and reach. And as we race into the new and unchartered realm of artificial intelligence, we not only need to have the right security solutions in place but also learn how to buckle up.

This is the seatbelt moment of our time.



“We need to look at digital security in the same way as we look at the seatbelt in a car; it’s the easiest security investment and it will give you a high reward if you use it.”

Simon Binder
Cyber Security Expert

03

Methodology

Methodology

The purpose of this report is to outline the future of digital security for organizations. It is based on a mixed research methodology that combines primary, quantitative and qualitative data from multiple sources. The research was done during the spring in 2024.

- **13 in-depth interviews** with security decision makers (e.g. CISO, CIO) at large enterprises and organizations across various industries in Telia's key markets in the Nordics and Baltics
- **9 in-depth interviews** with renowned cyber- and digital security experts, as well as profiled experts at Telia (see right →)
- **Expert roundtables** gathering 15+ cross-functional specialists from the wider Telia organization, including Risk, Strategy, Human Resources, Innovation, Communication and Cybersecurity (see appendix)
- **Data and insights** from leading industry reports and articles
- **Data from Telia's Digital Index 2024** sampling input from 1152 organizations of all sizes. TDI is an annual survey tracking Swedish companies' digital development.

The consulted experts

A special thank you to these experts, who provided valuable, in-depth perspectives and insights to the creation of this report.

Anne Marie Eklund Löwinder

CEO Amelsec and Cyber Security Expert

Mehis Hakkaja

CEO and Owner of Clarified Security OÜ

Åke Holmgren

Head of Cybersecurity, MSB - The Swedish Civil Contingency Agency

Pontus Johnson

Professor KTH and Director of the Center for Cyber Defense and Information Security

Niclas Jalvinger

CISO / CSO, Telia

Michael Mothander

Cyber Security Expert, Telia Cygate

Malin Fransén Kronberg

Head of Security, Telia

Simon Binder

Cyber Security Expert

Mats Mägiste

Security Infrastructure Expert, Telia

04

The current state of digital security

Building security is like running on an ever-accelerating treadmill

91%

of organizations reporting at least one cyber incident or breach during 2022
Source: Deloitte, Global Future Cyber Security 2023

+466%

Increase in DDoS attacks in Sweden in Q1 2024 compared to Q1 2023
Source: Cloudflare DDoS threat report, 2024

Struggling beyond competition

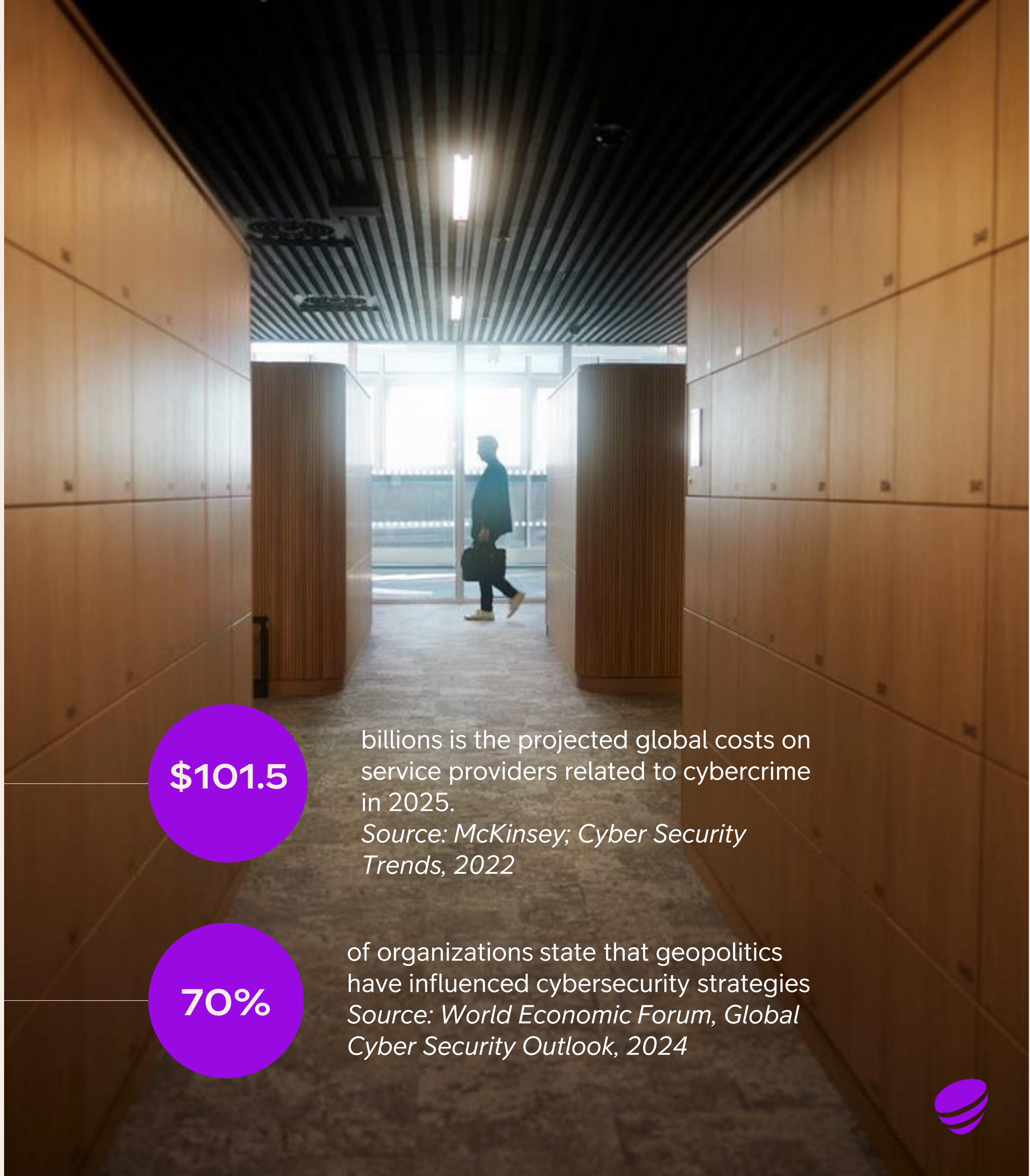
In nature, species engage in a relentless evolutionary arms race against competing species. Adapt or die. For businesses, this arms race has historically been determined by market fitness. Gradually, however, an existential threat has emerged beyond the boundaries and rules of regular competition.

Today, digital threat actors – not unlike invasive species in ecosystems – threaten the survival of companies around the world, big and small, no matter their market competitiveness. Add to this the accelerating pace of change and it's clear that running from extinction will become even more intense in the coming decade.

The arms race analogy provides us with a powerful insight: security, like fitness, is not a destination. There is no *arriving at* security, just continual progress and adaptation. The fact that we wore a seatbelt while driving yesterday doesn't mean we will be properly buckled up today.

“Just assume you will get attacked.”

CISO – Global Hardware Manufacturer



$101.5 billions is the projected global costs on service providers related to cybercrime in 2025.
Source: McKinsey; Cyber Security Trends, 2022

70% of organizations state that geopolitics have influenced cybersecurity strategies
Source: World Economic Forum, Global Cyber Security Outlook, 2024

The security gap in the Nordics-Baltics

Over the past decades, digital transformation has fundamentally reshaped most organizations. Although the Nordic-Baltic region was an early digital adopter, security efforts often lagged. Historically high levels of trust* and previous decades of relative calm have left us vulnerable in a rapidly evolving threat landscape.

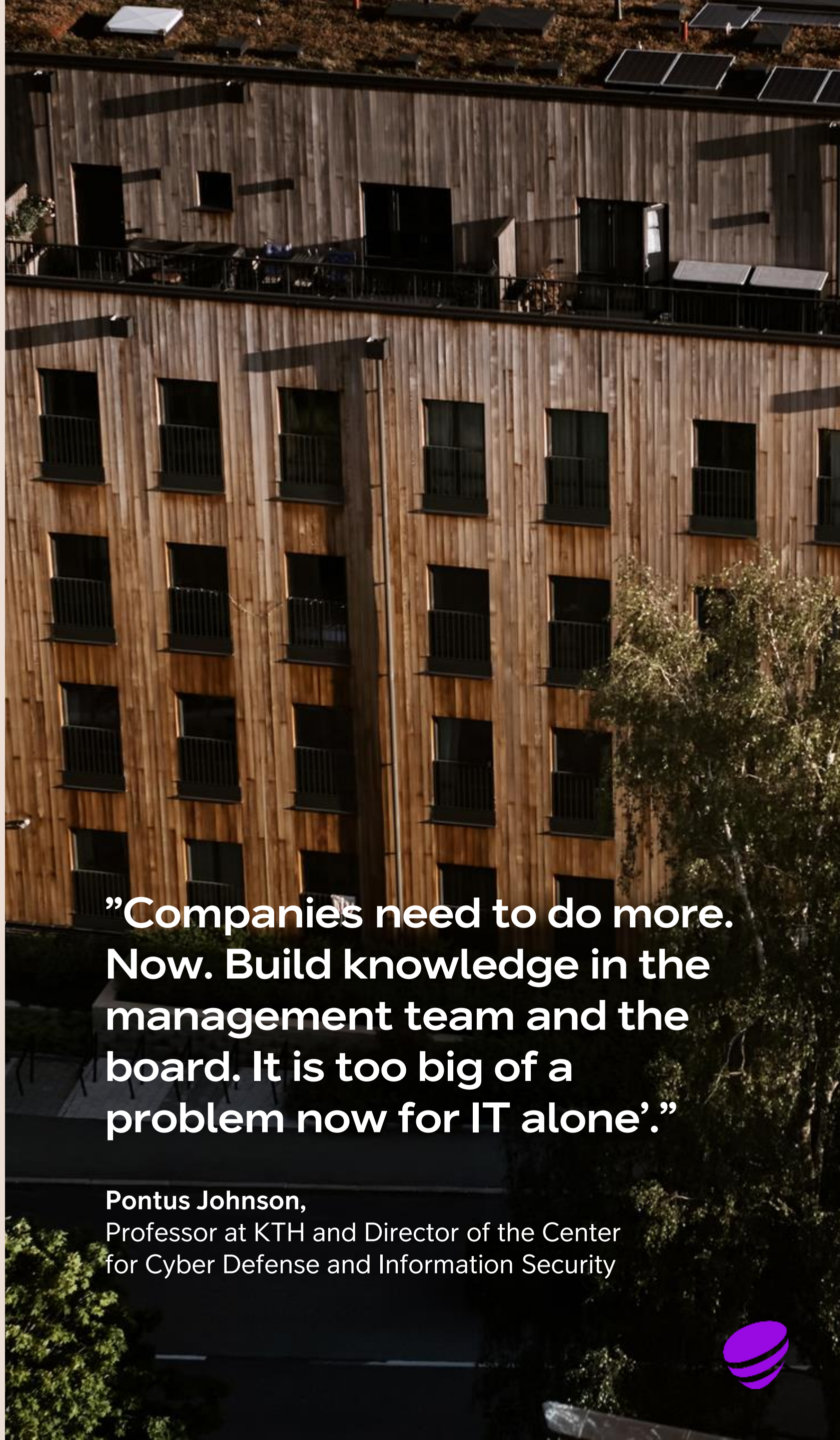
Coupled with our naive past is the power of inertia, not least in larger, more traditional organizations: it takes time to unlearn old habits and cultivate a new security mindset.

This security gap poses significant challenges to organizations that suddenly find themselves in a different world, without sufficient preparation and defense to cope with emerging threats. In the words of former FBI Director Robert Mueller, *“There are only two types of companies: those that have been hacked, and those that will be”.*

Today, the state of organizational security is fragmented. An organization's readiness to face threats largely depends on the level of digital security maturity it has been able to develop alongside its digital transformation. Digitally native companies, regardless of size, are naturally better positioned to tackle future challenges.

Only 3%

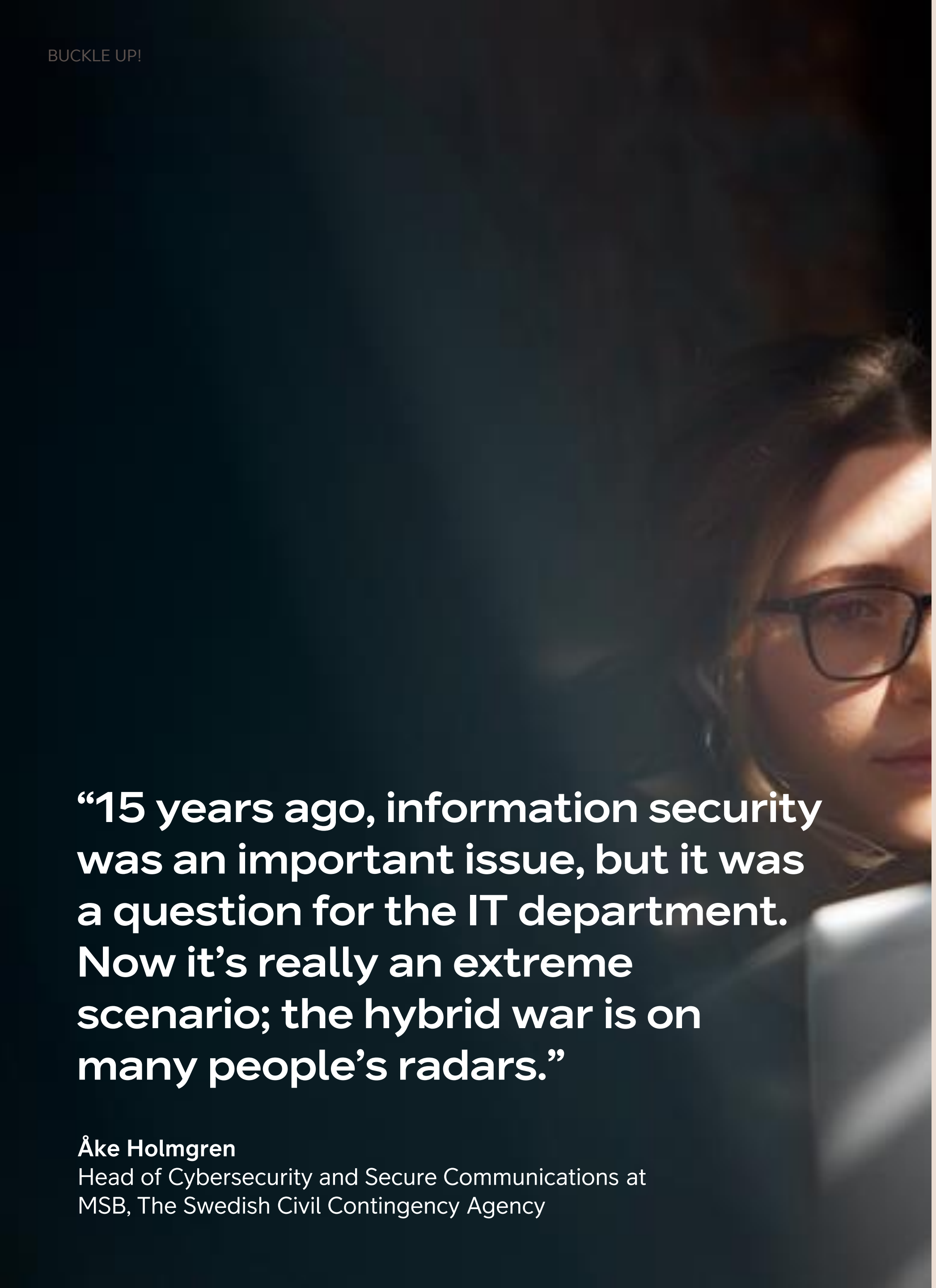
of Swedish governmental agencies live up to cybersecurity demands in 2024
Source: MSB



”Companies need to do more. Now. Build knowledge in the management team and the board. It is too big of a problem now for IT alone’.”

Pontus Johnson,
Professor at KTH and Director of the Center for Cyber Defense and Information Security

*particularly the Nordics: Finland (78%) and Sweden (69%), score among the highest in Europe when it comes to trust in Government. *Source: OECD*



> “15 years ago, information security was an important issue, but it was a question for the IT department. Now it’s really an extreme scenario; the hybrid war is on many people’s radars.”

Åke Holmgren
Head of Cybersecurity and Secure Communications at
MSB, The Swedish Civil Contingency Agency

Anxiety levels are rising

2/3

of enterprise security professionals worry about cyberattacks
Source: Telia Digital Index 2024

Between digital guns-for-hire and state-sponsored cyber terrorists, cybercrime is experiencing unprecedented growth. Increases in scale and scope mean that attacks can cause more damage than ever before. Organizations hit by cyberattacks might find themselves having to manage without critical systems for weeks or even months.

This new reality causes significant unease among security professionals: two in three large companies worry about being attacked, an increase of 10 percentage points since 2023, according to Telia’s Digital Index 2024.

Simon Binder, Cyber Security Expert, notes a shift in enterprise attitudes: *"Enterprise customers are much more aware today and almost paranoid over digital security”.*

Organizations seem to recognize the sense of urgency and invest in robust technology solutions to reduce system vulnerabilities. However, several key challenges need to be addressed moving forward.

> “As long as you can earn lots of money in a very short time with low risk, this will continue.”

Michael Mothander,
Cyber Security Expert, Telia Cygate

Security challenges facing organizations today

01. Balancing security & technology investments

There is a perceived investment trade-off between technology and digital security. The former has a clear, measurable impact on business activities, while the benefits of digital security can seem abstract unless an organization has been directly affected. If the security budget is part of the IT budget, there's a risk that funds will shift towards AI adoption rather than enhancing digital security. Conor McGlynn, Director Group Head of Security Strategy and Transformation at Telia, compares digital security to insurance: *"Security investments won't be perceived as valuable until something happens".*

51%

Is the share of CISOs that project that their overall IT security budgets will stagnate or decrease 2024
Source: Pentera, The State of Pentesting, 2024

02. Preparing for the worst, not just prevention

Many organizations prioritize preventing and detecting incidents over preparing for the worst. Data from the 2024 Telia Digital Index shows that companies have more solutions for identifying, protecting, and detecting threats than for recovering and repairing after an attack. Recent figures from a Cisco survey of 4,700 security professionals show that organizations with incident experience focus more on mitigating losses and maintaining business continuity.

71%

Share of organizations that believe they don't have solutions in place for service recovery after an attack
Source: Telia Digital Index 2024

03. Attracting security talent and building know-how

The skills gap is real: enterprises struggle to attract and retain IT professionals, especially security experts. Small- and medium-sized companies often lack security know-how entirely, relying on third-party vendors and partners. This shortage of experts poses a significant challenge, particularly in the short term.

3.4M

Current global estimated cybersecurity skills gap
Source: Allianz, Cyber security trends, 2023

04. Scattered digital security efforts – no overview

Digitalization often occurs in isolated teams in an organization, leading to scattered digital security efforts. Without a holistic unified strategy, digital security is often an afterthought rather than an enabler of business operations.

15%

of organizations have reached the highest level of maturity (4), where cyber security is a prioritized perspective within all operations.
Source: Radar Cyber Maturity Index 2024.

Wait a Minute!

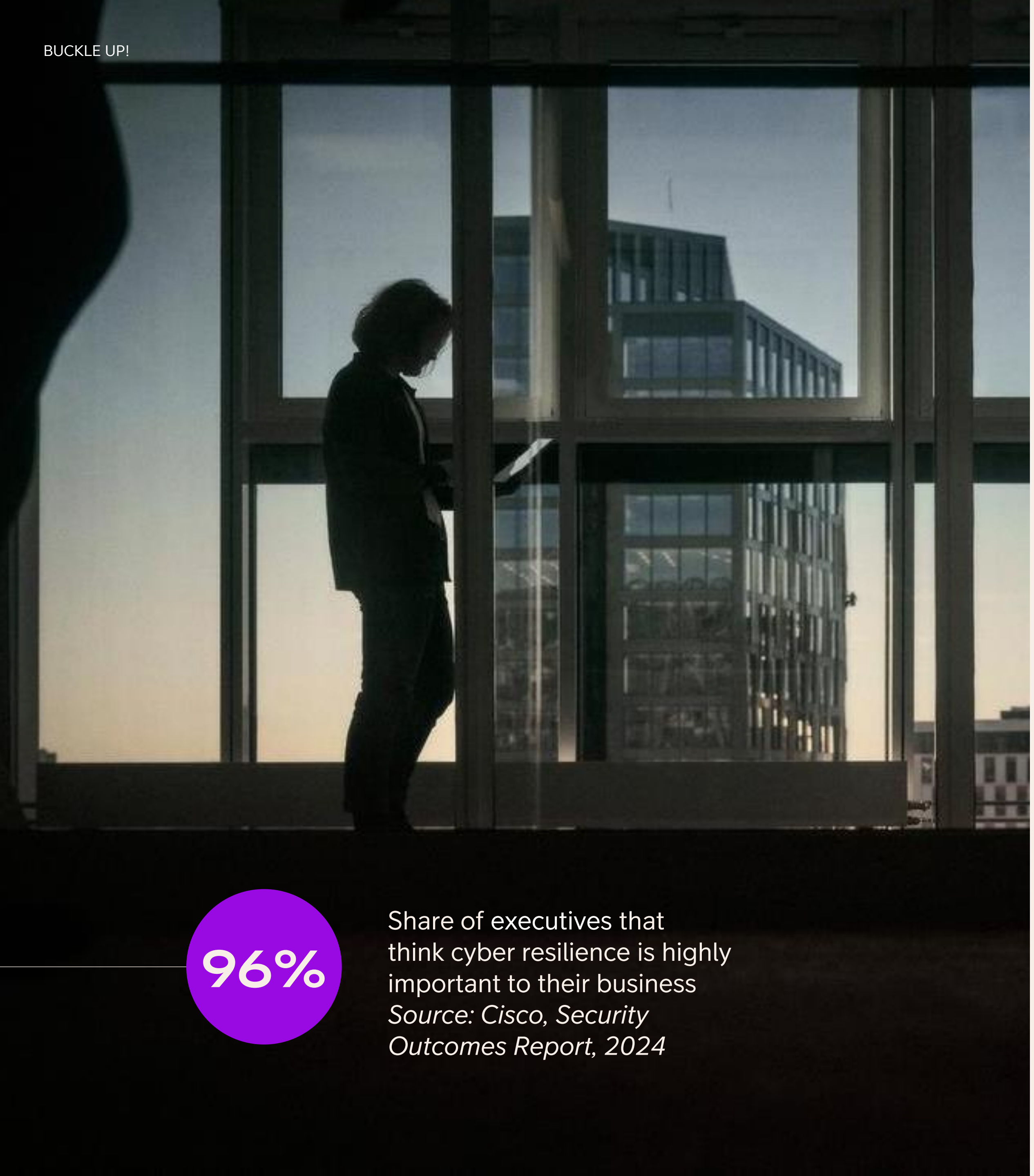
You might have noticed something missing from this breakdown: people. For now, hold that thought. First, let's briefly look at what it is organizations are trying to achieve by improving security. As the treadmill metaphor thought us, only the resilient will survive. So, what exactly is digital resilience?

“It's not so unlikely that there will be higher demands on safety, especially with new EU regulations. Serious organizations will seek to do business with those who have good enough security.”

Åke Holmgren
Head of Cybersecurity and Secure Communications
at MSB, The Swedish Civil Contingency Agency

05

Building digital resilience



96%

Share of executives that think cyber resilience is highly important to their business
Source: Cisco, Security Outcomes Report, 2024

“If by chance an attack succeeds, we are able to react, expose the attacker and recover with minimal impact.”

CISO - Nordic Dairy Enterprise

Follow the NIST framework to build resilience

1/5

Share of organizations segmented as having "high cyber maturity" *Source: Deloitte, Global Future of Cyber Survey 2023*

37%

of organizations are confident they can remain resilient through a worst-case cyberattack. *Source: Cisco, Security Outcomes Report, 2024*

Making continuous improvements easy

Building digital resilience requires structured work and dedicated resources. Luckily, there are established ways to help get started.

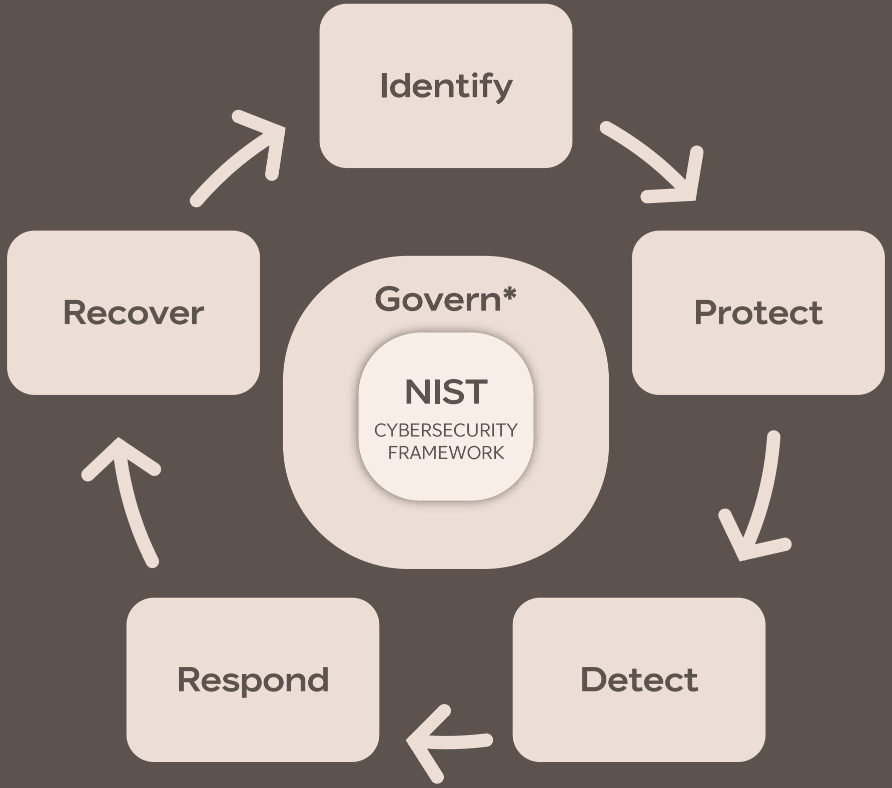
The widely accepted NIST Cybersecurity framework defines cyber resilience as *"the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources".*

First, this definition implies that organizations need to focus their security efforts not only on protecting and mitigating attacks, but also being able to recover, learn from and adapt to events that do happen to them, or others.

Second, it implies that the process of building and maintaining resilience is a continuously ongoing process – you are never done.

Take actions steps by step.

As Simon Binder, Cyber Security Expert says: *"I see it as any sport; you don't start with the most advanced things straight away. You start with building up a strong body, a strong mind, a strong foundation to stand on. If you build the best base, you'll be able to accelerate later and compete."*



*During 2024, 'Govern' will be added as the sixth component of the framework. For more information, visit *nist.gov/cyberframework*

“We have so many users which means a big risk of someone opening an email or clicking on a code. In the past, it was more embarrassing admitting you got a virus. But it is good that you learn from it - then you can apply it in other ways. What lessons can be learned and strengthen your environment?”

Head of IT and Security, Public sector

Collaboration and transparency builds power

Partnerships are your best bet

Organizations are exposed to looming threats. Our research points in one clear direction; going forward, no organization will be able to handle security alone. The shortage of skilled security professionals, as well as the increasingly interlinked ecosystems of partners and supply chains organizations operate in, cause vulnerabilities. Partnerships and collaborations will therefore be key to succeed – whether it's strengthening security together with vendors, outsourcing security work, or sharing learnings and intel with industry peers.

Transparency builds trust

Everybody knows there is a huge debate about data privacy. Protecting data is important to build trust. The momentum of incoming EU regulation, combined with increasing demands from the public and customers, suggests that more transparency and openness will be needed going forward. Experts agree; transparency and accountability can make a difference, especially when building trust with customers, the media, and other key stakeholders.

Finding the security balance

It can be helpful to look at resilience as balancing the dynamic between people, processes and technology. And that brings us to the biggest challenge and opportunity in building a resilient organization: people.

94%

of consumers would be more loyal to brands that practice transparency
Source: Forbes

"A weak setup in the US could affect a factory in Belgium or Sweden, and a malware infection in China will spread quickly elsewhere unless we act."

CISO – Global Vehicle Manufacturer

06

The hackable human

#2

Low security maturity among employees is ranked as the second biggest barrier to maintaining sufficient security levels, after restricted budgets and resources.
Source: Radar, Cybersäkerhet 2024

“AI is to cyber threats what nuclear is to warfare.”

Håkan Kvarnström,
Head of Governance, Risk and Compliance at Telia

The missing component: people are the prime target for future attacks

The simple but useful People, Process, Technology (PPT) framework lets us examine how the three key components of any organization interact and what micro and macro patterns that emerge as a result.

Historically, investments in digital security have mainly been allocated towards two of the three areas: technology and processes. One obvious reason for this is their tangibility: things and ways of working are simple; people and culture are complex.

Leaders may have hoped the "people part" would naturally fall into place once the other elements were in order. Unfortunately, it didn't.

An overwhelming majority of attacks target people and not even the most sophisticated technology can prevent people from becoming victims. Any organization looking to get the most out of their digital security investments must address this critical fact. So, let's explore what makes people the prime targets for future attacks.

98%

of cyber-attacks rely on social engineering *Source: Splunk, State of Security 2024*

52%

of leaders believe their employees lack the necessary cybersecurity knowledge *Source: Fortinet, Cybersecurity skills gap 2022*

> “It’s easier to hack a human than a computer”

Anne-Marie Eklund Löwinder (Amel), CEO and Cyber Security Expert

Three factors putting people at risk

01.
Rapid AI adoption is both a blessing and a curse

We're witnessing another big shift in technology use as organizations explore AI tools to boost efficiency, eliminate tedious tasks, and spark creativity. So far, so good. But there's a catch: employees' often immature use of AI tools poses significant security risks and creates a playground for cybercriminals.

Simple actions like copying and pasting text into a public AI model can expose sensitive information. Feeding these models with confidential data is irreversible, yet the risk seems distant to the average employee. While some enterprises proceed with extreme caution, others lack guidelines, leaving employees to navigate AI on their own.

34%

of organizations lack a complete generative AI strategy
Source: Splunk, Cybersecurity skills gap 2022

43%

of security practitioners think AI can benefit defenders more than attackers (up from 17% in 8 months)
Source: Splunk, Cybersecurity skills gap 2022

02.
Attacks are becoming hyper-automated (and our response too)

Phishing emails still account for a large portion of data breaches. With AI, anyone can target thousands of companies at once and even personalize attacks for each employee. As deepfakes become more sophisticated, distinguishing between real and fake becomes nearly impossible.

Criminals exploit our emotions using "dark psychology," triggering our autopilot mode, or 'System 1' as defined by Nobel laureate Daniel Kahneman. This system is reflexive and emotional, unlike the more deliberate 'System 2', which requires cognitive effort. We expect a lot from employees—agility, tech adoption, and work-life balance—which makes slipping up almost inevitable under stress or urgency.

$4.8M

Average cost for organizations breached through phishing
Source: IBM, https://www.ibm.com/topics/phishing, 2024

03.
Our lives are being infiltrated like never before

Hybrid work has blurred the lines between personal and professional life, introducing new digital security risks. Employees share personal and sensitive information daily. Leaders are encouraged to be transparent, which are great news for criminals. With access to our hobbies, preferences, and whereabouts, "social engineering" in the age of AI is scarier than ever. Deepfakes are becoming so convincing that they may soon challenge our perception of reality.

So, what can we do?

No human is an island, and employees don't act in isolation. Organizations have a huge task in providing the right conditions for security to flourish. We must therefore now turn to the focal point of our argument: culture as the enabler of resilience.

46%

Share of IT professionals that report an increase in social engineering attacks directly targeting individuals
Source: LastPass, Combating Social Engineering in 2024.

“As an organization, you should be very careful not to blame those who have done wrong. It’s a management question; they have not put the right conditions in the hands of people.”

Åke Holmgren
Head of Cybersecurity and Secure Communications
at MSB, The Swedish Civil Contingency Agency

CASE STUDY

WSY Group's Laurynas Prikockis Catering to people first

> **"It's crucial that the team handling the incident are prepared from a psychological perspective. We must understand that employees are vulnerable."**

Laurynas Prikockis is the CIO of Western Shipyard Group. Earlier this year, the enterprise experienced a significant cybersecurity incident involving a phishing attack that compromised an employee's credentials, leading to unauthorized access to sensitive information.

The investigation revealed that the phishing email exploited weaknesses in the company's MFA (Multi-factor authentication) implementation, and that the attack could have been mitigated with better employee training and awareness.

Laurynas, who also has an MBA that includes Psychology, shares learnings from how he and the team handled the incident putting people first.

Employee-centric incident response

When the breach happened, the security team at WSY were able to respond quickly. Initial measures included resetting passwords and securing affected accounts.

More importantly, significant emphasis was put on the well-being of the affected employee who was promptly contacted and informed about the breach. WSY also provided psychological support to help manage the stress associated with the incident.

Multi-factor authentication was reinforced across all platforms. The security team conducted a thorough investigation to identify any additional vulnerabilities and took steps to fortify their systems against similar attacks.

Transparency throughout

Transparent communication was maintained to ensure the employee understood the situation and the steps being taken to mitigate the impact.

Laurynas and the security team worked closely with the employee to restore their confidence and provide necessary training to prevent future incidents.

The incident was reported to the National Cyber Security Office and other relevant governmental bodies to comply with data protection regulations. The company's response plan also included notifying stakeholders and the public, ensuring transparency about the incident and the measures being taken.

Conclusion

The incident highlighted the importance of a holistic approach that balances technical measures with employee support. By focusing on the well-being of the person responsible for the breach, the company not only managed to contain the incident effectively but also fostered a culture of trust and resilience. Additional cybersecurity training sessions were conducted for all employees to enhance their ability to recognize and respond to phishing attempts.

The case demonstrates that human-centric cybersecurity practices are vital in managing and recovering from security incidents.

Date of Incident: Feb 2 2024
Type of Attack: Phishing
Attack Vector: A Black Hat hacker deceiving the employee into revealing login credentials for social accounts and corporate email

Don't miss Laurynas' lessons learned!

WSY and Laurynas' checklist
Lessons learned

Three key lessons to learn from when shaping a people-centric approach to security

01

Employee well-being

Prioritizing the affected employee's mental health and confidence was crucial. It ensured that the employee remained a valued part of the team and helped in rebuilding trust within the organization.

02

Enhanced training

Continuous education and training programs were established to keep employees updated on the latest cybersecurity threats and best practices.

03

Strengthened protocols

The incident prompted a review and enhancement of existing security protocols, including the implementation of more robust MFA solutions and regular security audits.

07

Culture as the security enabler

“Culture is the collective and aggregated behavior of the people. We need storytelling, training, information, and discussions.”

Håkan Kvarnström
Head of Governance, Risk and Compliance Telia

> ” Our people and experience are key – anyone can buy ingredients for a pasta Carbonara but not everyone's got the skills to make a good one. The same goes for cybersecurity.

Sam Rabar
Cyber Security Expert, Telia

How culture can be a security enabler

73%

of employees say being involved in the company culture keeps them engaged
Source: Seenit, The State of Employee Engagement, 2023

72%

of leaders say that culture helps successful change initiatives happen
Source: PWC, Global Culture Survey 2021

Phishing emails, updating passwords, and letting people into the office building are all part of everyday work life. But how do you build a solid security culture?

Before diving in, let’s define culture as the shared values, attitudes, beliefs, and behaviors of a group. In short, culture lives in the hearts, minds, and hands of its members.

Leadership is key to changing hearts and minds

Changing culture is tricky. Many leaders naturally try to shift what employees value and believe. It sounds simple: define the desired culture, communicate it, and wait for change.

But science shows us that this approach rarely works. Why? Because values are slow to change and deeply ingrained. Even if we manage to shift attitudes and beliefs, there's still the infamous gap between knowing and doing. Think about health: we know exercise is good, but often fail to follow through. Changing only thoughts rarely leads to changing actions.

Actions speak louder than words

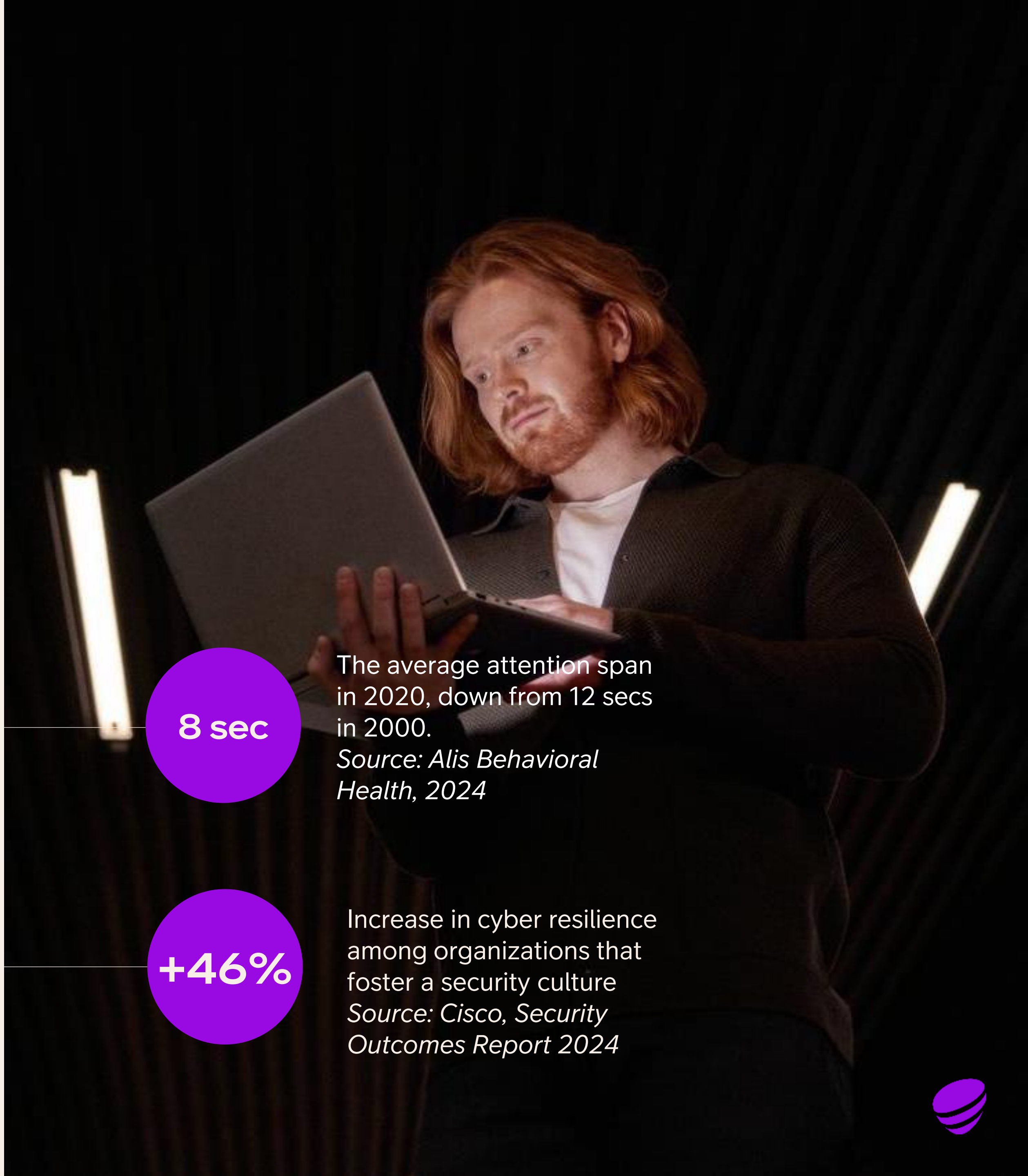
Here’s the good news: targeting behaviors and decisions is the most effective way to change culture. Notable academic studies clearly indicate that leaders should focus on getting employees to act differently first. Over time, the adoption of new behaviors will shape new attitudes, beliefs and values. A new culture emerges, driven by practicing rather than preaching.

Leading by example

A crucial component to influencing how employees act differently is leadership: when leaders say that security is top priority but don’t act accordingly, employees will quite naturally follow suit.

> “A security culture is marked by awareness and how it affects me on a daily basis; whether it's walking through a door or opening an email.”

Head of IT and Security – Tech Company



8 sec

The average attention span in 2020, down from 12 secs in 2000.
Source: Alis Behavioral Health, 2024

+46%

Increase in cyber resilience among organizations that foster a security culture
Source: Cisco, Security Outcomes Report 2024

“10 years ago, I didn’t discuss security with leadership, it was more IT service and stability. ‘That’s for IT to handle, it just has to work’. Now it’s much more a topic on the leadership level. Security is a business pillar; we talk about security culture and awareness.”

Head of IT and security, Financial services company

CASE STUDY

Arla Foods' Thomas Zuliani
The importance of security culture

> "You have the technology, the people and the processes. But none of them work unless you have a security culture established throughout the organization"

Arla Foods, a dairy giant with some 21,000 employees, had not had a dedicated CISO or a proper cybersecurity department for a decade before Thomas Zuliani's appointment. This had created a significant backlog of security issues that needed addressing.

Under Zuliani's leadership, the cybersecurity team rapidly expanded from 2 to 12 members to tackle these challenges and comply with new European regulations.

One significant challenge was changing the mindset of an organization that had not prioritized cybersecurity for years. Overcoming this required persistent efforts in education, engagement, and demonstrating the value of proactive security measures.

The Role of Culture in Cybersecurity

Zuliani highlights that the success of any cybersecurity program relies critically on the culture of the organization, pinpointing three key areas:

1. Top management involvement:

The involvement of top management is crucial. Zuliani points out that a CEO who prioritizes cybersecurity can drive the organization towards higher maturity levels in security practices. Conversely, if top management is indifferent, achieving the same level of maturity becomes significantly harder.

2. Proactive mindset:

A proactive approach to cybersecurity is essential. Zuliani explains that many organizations only respond to cybersecurity after a major incident. However, at Arla, there was a deliberate effort to address security proactively. This helps in mitigating risks before they turn into significant problems.

3. The human factor:

Humans are both the weakest link and the greatest asset in cybersecurity. Despite investing millions in technology, a vast majority of successful cyberattacks exploit human vulnerabilities, such as phishing and social engineering. Hence, transforming employees into alert defenders of the organization is vital.

Conclusion

Zuliani's leadership illustrates that a resilient digital security strategy extends beyond technology and processes. It requires a pervasive culture of security awareness and proactive engagement from all organizational levels, especially top management. By fostering a culture where every employee understands their role in digital security, organizations can significantly enhance their resilience.

This approach not only mitigates risks but also transforms potential vulnerabilities into strengths, creating a human firewall that complements technological defenses.

10

New members recruited to the cybersecurity team by Thomas in his first year as CISO at Arla Foods, growing the team from 2 to 12.

→ Don't miss Thomas' culture checklist!

Arla Foods and Thomas’ checklist
Cultivating security

Four ways that organizations can facilitate conditions for resilient security culture to grow and blossom.

“If the CEO is not propagating the culture we want to have, it’s going to be a lot more difficult to achieve cyber maturity.”

01

Awareness & training

Arla conducts phishing simulations and mandatory training sessions to keep employees knowledgeable and alert about potential threats. The sessions are designed to be engaging and relevant to employees' everyday tasks.

02

Engagement activities

Zuliani advocates for creative engagement strategies such as cybersecurity month activities, guest speakers, and town halls. These activities not only educate but also motivate employees to take cybersecurity seriously.

03

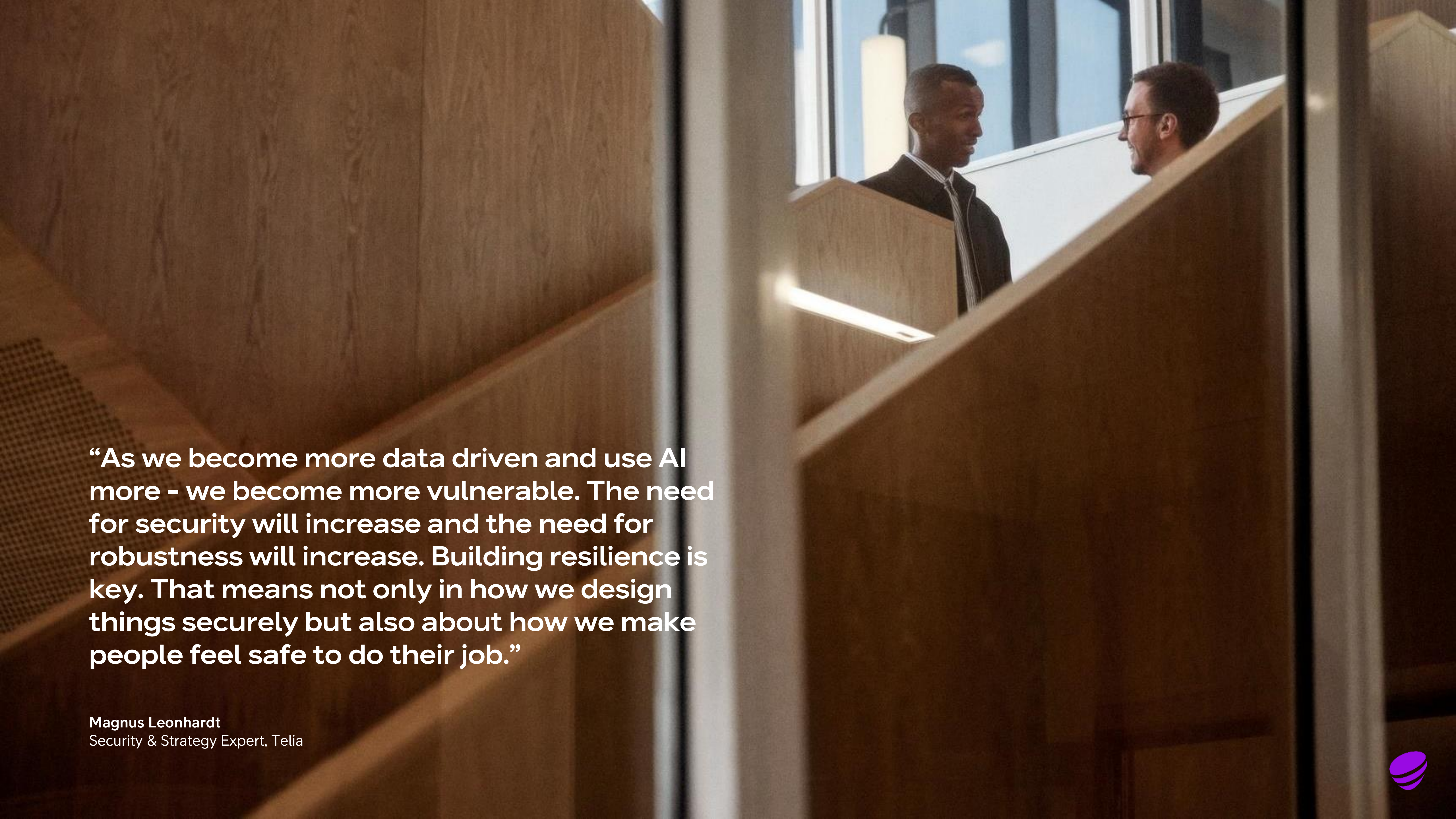
Carrot over stick

Instead of the punitive style, Zuliani prefers a soft approach that encourages collaboration and shared responsibility. This involves delegating security responsibilities to employees, fostering a sense of ownership and vigilance.

04

Strategic integration

Cybersecurity goals are integrated into the overall mission and vision of the company. For instance, ensuring the reliability and integrity of data aligns with the company’s mission of sustainability and quality in dairy production.



“As we become more data driven and use AI more - we become more vulnerable. The need for security will increase and the need for robustness will increase. Building resilience is key. That means not only in how we design things securely but also about how we make people feel safe to do their job.”

Magnus Leonhardt
Security & Strategy Expert, Telia

08

How to build a security culture: the big five

“A security mindset is the foundation of resilience; it empowers individuals to recognize risks and take proactive actions to protect not just themselves, but the entire organization and the society we serve.”

Malin Fransén Kronberg
Head of Security, Telia

The recipe for digital resilience: Building the big five of security culture

We have identified five patterns that mature security organizations tend to have in common. These traits all contribute to developing a resilient culture of security by empowering individuals to actively participate, learn and grow.

01
Ps
Psychological safety

02
Mp
Mild paranoia

03
Zf
Zero friction

04
Dp
Diverse perspectives

05
Cl
Continuous learning

> **“Security culture means being able to speak about it. No one should get blamed for admitting anything.”**

Michael Mothander
Cyber Security Expert, Telia Cygate

01. Psychological safety

Traditionally, many organizations have experienced a culture of silence and shame surrounding digital security. Individuals have been afraid to make and admit to mistakes, and organizations have stayed silent in the wake of being attacked.

Resilient organizations have a blameless and shameless policy: employees are not afraid to make mistakes and feel safe to report them if they do happen. There are no threats of repercussions when mistakes are made. Specially trained experts are first responders and offer support to vulnerable employees who have been targeted and exploited by threat actors.

A key component to psychological safety is transparency: they communicate honestly with employees and stakeholders when incidents occur. This in turn builds mutual trust as employees feel safe to share themselves.

Measuring psychological safety among employees

*Questionnaire developed by Harvard professor Amy Edmondson**

1. If you make a mistake on this team, it is not held against you
2. Team members can bring up problems and tough issues
3. Team members accept others for being different
4. It is safe to take a risk on this team
5. It isn’t difficult to ask other team members for help
6. No one would deliberately act to undermine my efforts
7. My unique skills and talents are valued and utilized

**Test your team at fearlessorganizationscan.com*

02. Mild paranoia

Perhaps due to the abstract and often indirect nature of cyberattacks, people in general have been way too trusting. This lack of alertness has invited threat actors to take advantage.

Resilient organizations have managed to concretize and highlight risks to enable company-wide alertness. They have done this without going too far in the direction of panic or resignation. In the words of Niclas Jalvinger, CISO/CSO at Telia, the key term here is *mild paranoia*, a heightened risk awareness coupled with common sense.

Related to psychological safety: overreporting is always better than underreporting. The only threat that can be avoided is the threat that is detected.

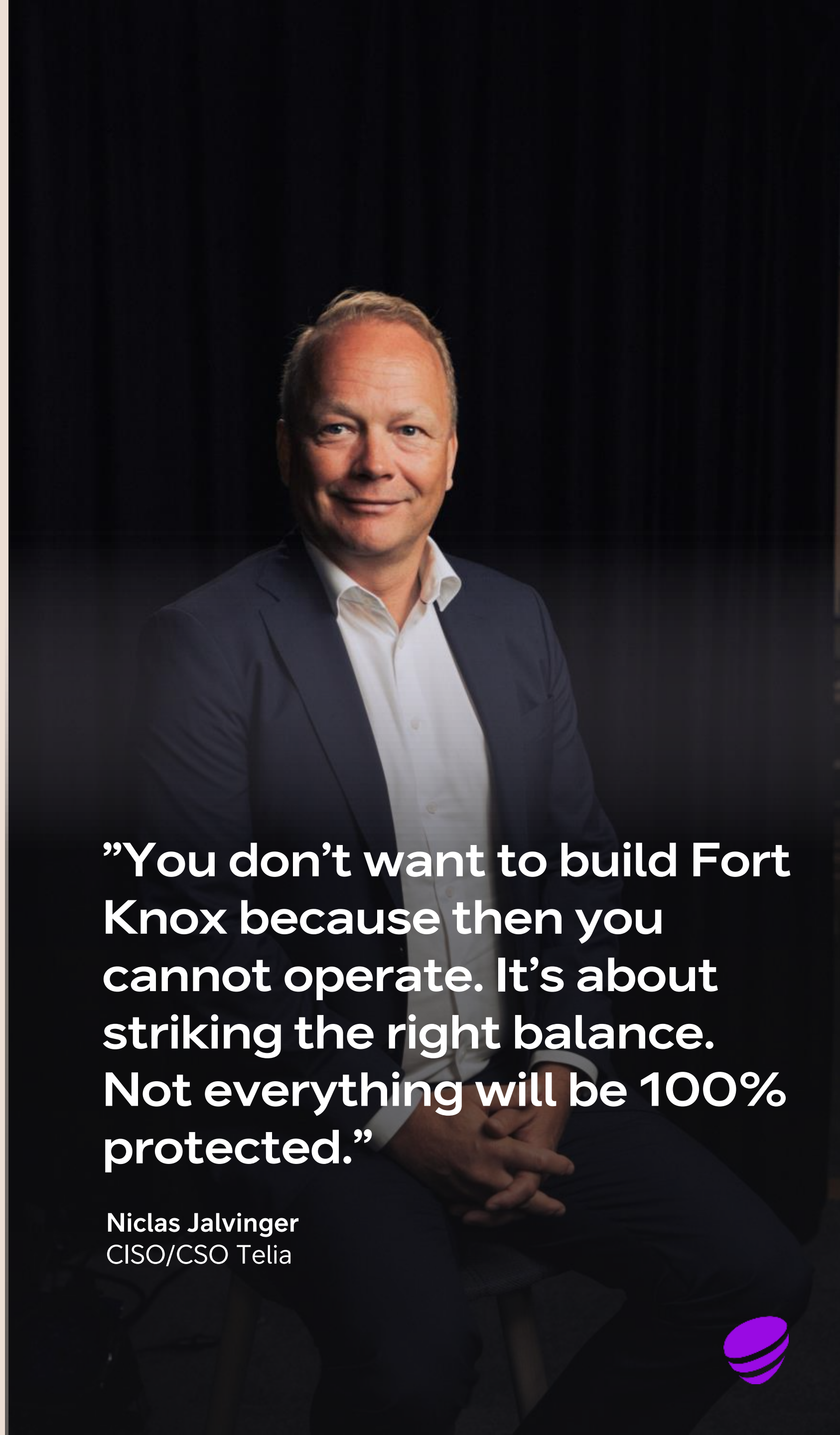
Niclas Jalvinger's top 3

Telia's CISO/CSO shares his tips on building a security-infused culture

1. **Walk the talk**
Leaders can't stand on the barricades and talk about security without living it themselves. It starts at the top.

2. **Listen more, talk less**
Never assume you know more than the employees. There is a lot to learn by just listening instead of talking.

3. **Think like a criminal**
Encourage employees to come up with ways criminals might attack the company to boost awareness.



> ”You don't want to build Fort Knox because then you cannot operate. It's about striking the right balance. Not everything will be 100% protected.”

Niclas Jalvinger
CISO/CSO Telia

> “Company security policies should be written for everyone to comprehend, not for security experts.”
>
> **Sam Rabar**
> Cyber Security Expert, Telia

03. Zero friction

As we have seen, organizations that depend on employees carrying a heavy cognitive load to do their job are setting themselves up to fail.

Resilient organizations don’t work against human nature, but rather tailor their security efforts in line with it. As much as possible, they incorporate security technology and processes into existing behaviors and workflows instead of forcing new ways of working on employees. The key is appealing to what matters to people: finding ways to align individual and organizational incentives.

The many acronyms and abbreviations used in digital security makes the topic both opaque and excluding. Resilient organizations reduce friction by using simple and unambiguous security language to minimize mental effort and avoid the risk of misunderstanding. And importantly, they understand that there is no one-size-fits-all in security: messages need to be tailored to different audiences to boost engagement and retention.

Another friction point is unclear paths of communication: not knowing what to do and whom to reach out to when threats emerge. Resilient organizations establish clear protocols to simplify and encourage reporting.

3 friction reducers

Three ways that resilient organizations work with - not against - human nature

1

Call in the experts
Team up with experts on human behavior and psychology to define how lasting change is best achieved.

2

Simplify language
Collaborate with communication department to find a common language around digital security everyone understands.

3

Appeal to self-interest
People support what they create. Focus on what motivates people in their daily work to lower the threshold.

04. Diverse perspectives

Digital security has traditionally been a male-dominated, homogenous field: many professionals share similar backgrounds, experiences, knowledge and cultural references. This poses the very real threat of inattentional blindness, which occurs when individuals fail to detect unexpected stimuli in plain sight.

A famous experiment had 24 radiologists examine a series of lung x-rays to search for lumps. A gorilla, 48 times larger than the average lump, was inserted in the last x-ray. 83% of radiologists didn't see the gorilla.

Resilient organizations involve employees in security, taking advantage of the fact that diverse perspectives increase the chance of threat detection and avoidance. They look outside of traditional venues and invite new skills to the table: behavioral scientists, hackers and ex-military may all contribute to shaping the security expertise of the future.

3 tips for a new outlook

Collected tips and tricks for broadened perspectives.

1

Acknowledge your biases
Teams with similar backgrounds and perspectives risk overlooking crucial security factors. Identify potential biases and bring in new perspectives.

2

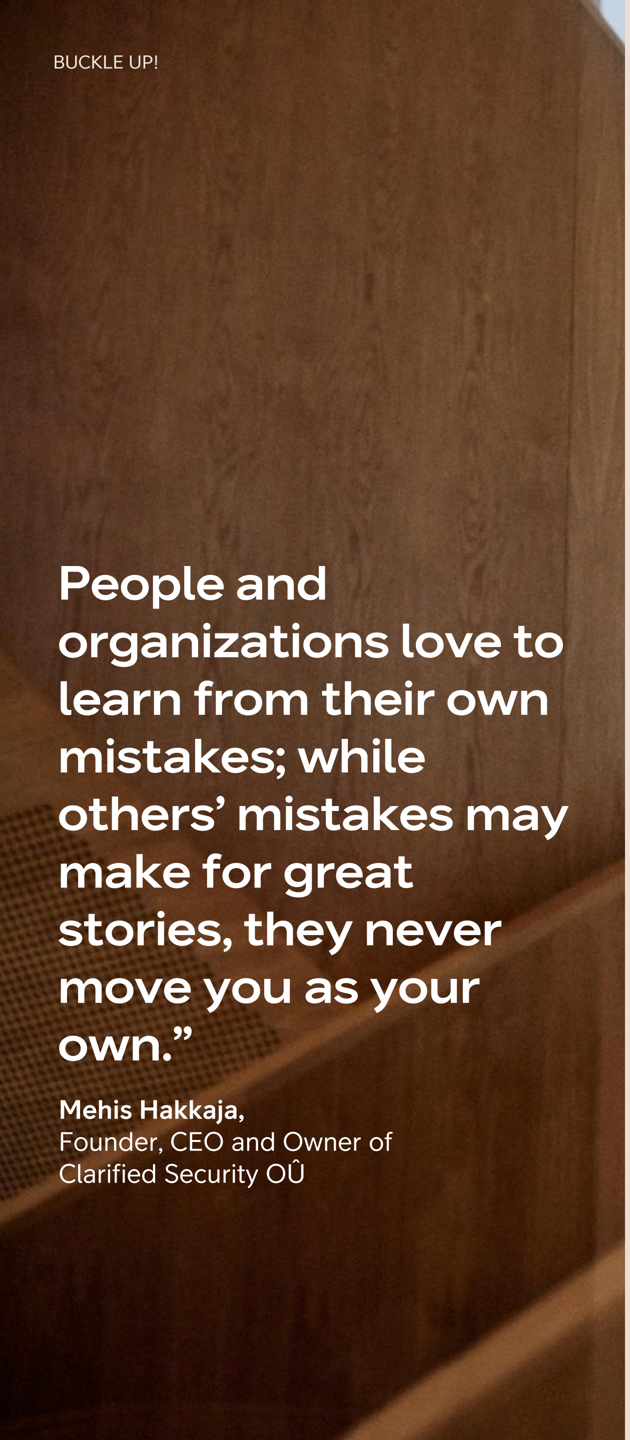
Diversify the security skillset
Criminals move fast. Challenge traditions by bringing in new skills – behavioral experts, analysts and process leaders are mentioned as top skills for future-proofing your team.

3

Find new friends
Create structured collaborations among key stakeholders and departments internally around digital security – from HR, Communications and Legal to top management.

> ”A key issue is the tonality that exists in the cybersecurity industry. It's a very male and macho world.”

Anne-Marie Eklund Löwinder (Amel),
CEO and Cyber Security Expert



> **People and organizations love to learn from their own mistakes; while others' mistakes may make for great stories, they never move you as your own."**
>
> **Mehis Hakkaja,**
> Founder, CEO and Owner of
> Clarified Security OÛ

05. Continuous learning

Many organizations fail to recognize the importance of allowing employees to devote time and resources to upskilling, making them brittle in the face of rapid change.

Resilient organizations equip their employees with knowledge and tools but also encourage curiosity and continuous exploration. In line with striving for zero friction, they carefully design and carry out educational efforts to be snackable, memorable and actionable.

They employ behavioral science techniques such as micro habits to minimize energy costs and maximize effects. Employees aren't burdened by more information or instruction than is needed to act securely in the specific organizational context.

When incidents occur, they view them as opportunities to learn and grow. Continuous learning by doing - adaptation - is a key feature of resilience and a tangible way to build organizational knowledge capital.

Finally, resilient organizations compete in business but cooperate in security. Sharing lessons learned across industries builds overall system resilience and contributes to a safer organizational environment for all.

3 learning boosters

Three tips for gaining employee attention and engagement

1

Reporting routines
Make sure employees are equipped with the right tools and processes for learning and reporting; easy to understand, and use.

2

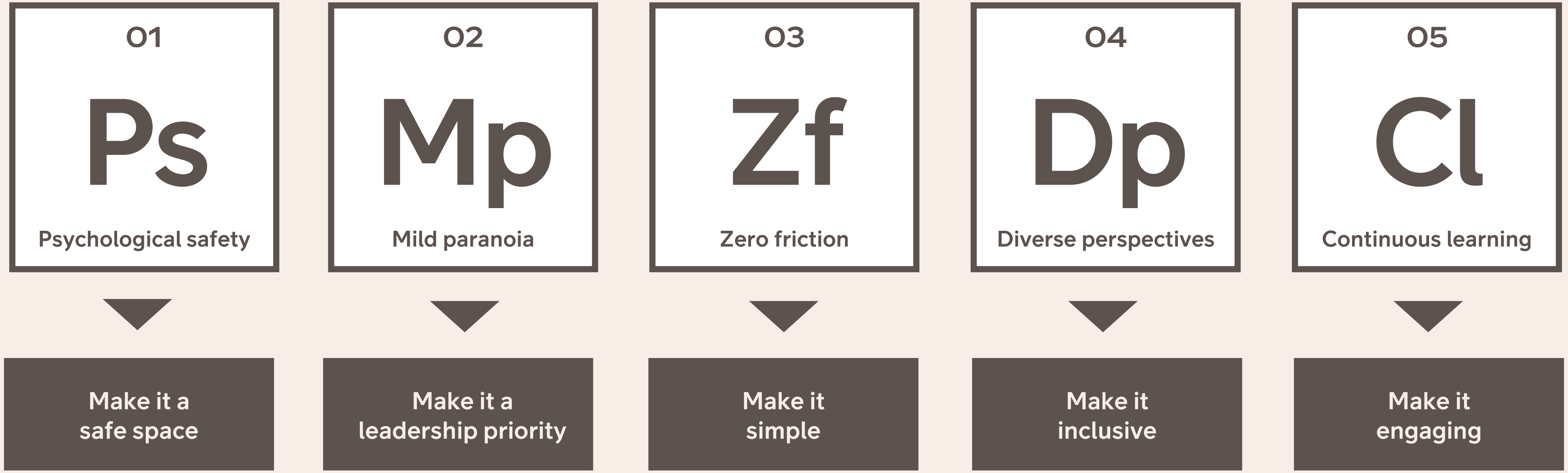
Learn with others
View real incidents as opportunities to discuss, collaborate, share learnings and adapt. Consider teaming up with external organizations and partners.

3

Make learning engaging
Use real cases and examples to inspire (and spook). Experiment with new and engaging formats such as gamification, podcasts or guest speakers.

The recipe for digital resilience: Five actions to take

Changing habits takes time – even when it's a matter of our own survival. It's clear that providing the right safety tools and processes is not enough, you need to get people on board to adopt them too. These are 5 actions to take to build a resilient security culture.



01 Ps Psychological safety – Make it a safe space

02 Mp Mild paranoia – Make it a leadership priority

03 Zf Zero friction – Make it simple

04 Dp Diverse perspectives – Make it inclusive

05 Cl Continuous learning – Make it engaging

09

Conclusions

Stronger together

As we navigate this increasingly volatile digital age, resilience is our most vital asset. Just like the seatbelt transformed car safety, an active digital security culture can safeguard our organizations against ever-evolving threats. By actively considering risks and fostering a culture of continuous learning and adaptability, we can turn vulnerabilities into strengths.

The future belongs to those who are prepared for it. Let's embrace these principles to build a secure foundation based on partnership and transparency. Only then can we confidently stride into a safer, smarter tomorrow.

No one can solve this on their own, so let’s join forces! Together, we can transform challenges into opportunities and ensure that our digital highways are as safe as they are fast.

If you wish to continue the discussion or learn more, please reach out to us at Telia in your local market.

Appendix

Contributors to the report

Telia contributors	Role	Organization
Aurimas Žlibinas	Head of Enterprise	Telia Lithuania
Kristjan Kukk	Head of B2B	Telia Estonia
Conor McGlynn	Head of Security Strategy and Transformation	Telia Company
Håkan Kvarnström	Head of Governance, Risk and Compliance	Telia Company
Ida La Spisa	CIO	Telia Sweden
Jon Christian Hillestad	Head of Enterprise	Telia Norway
Kristofer Ågren	Head of Product, Division X	Telia Company
Magnus Leonhardt	Head of Strategy & Innovation	Telia Sweden
Malin Fransén Kronberg	Head of Security	Telia Sweden
Mats Mägiste	Security Infrastructure Expert	Telia Sweden
Michael Mothander	Cyber Security Expert	Telia Cygate
Minna Vyyrylainen	Head of Business Networking	Telia Company
Nicholas Rundbom	Head of Communications B2B	Telia Sweden
Nicklas Olofsson	Culture and growth	Telia Company
Niclas Jalvinger	Group CISO / CSO	Telia Company
Ola Rembe	Head of Brand, Communications & Sustainability	Telia Company
Olli Pirttijärvi	Head of B2B	Telia Finland
Patrik Holmqvist	COO	Telia Cygate
Pontus Eklöf	Senior Sales Specialist	Telia Company
Sam Rabar	Cyber Security Expert	Telia Company
Sigrid Reijnst	Head of Employer Brand	Telia Company
Simon Binder	Cyber Security Expert	Telia Cygate[1]
Thomas Johansson	Global Business Strategy	Telia Company
Tobias Larsson	Head of B2B Sweden	Telia Sweden
Tomas Eklind	Portfolio Manager	Telia Company
Vinicius Joaquim Camargo	Division X	Telia Company
Zackaria Bennani	Portfolio Manager	Telia Cygate

Report project team	Role	Organization
Emelie Aidehag	Head of Insight & Foresight	Telia Company
Magnus Fahlgren	Brand Insight Manager	Telia Company
Suzanne Tellström	Brand Management	Telia Company

External Experts	Role
Anne Marie Eklund Löwinder	CEO and Founder Amelsec, renowned Cyber Security Expert and former Crypto Officer
Mehis Hakkaja	Founder, CEO and Owner of Clarified Security OÛ
Pontus Johnson	Professor KTH and Director of the Center for Cyber Defense and Information Security
Åke Holmgren	Head of Cybersecurity and Secure Communications at MSB, The Swedish Civil Contingency Agency

Research agency team	Role
Alexis Bolonassos	Research Strategist at Augur
Jenny Franzén Lycke	Foresight Director at Augur

[1] At the time of the creation of the report

References

Albarracin, D. et. al. (2024). Determinants of behavior and their efficacy as targets of behavioral change interventions

Alis Behavioral Health (2024) https://www.alisbh.com/blog/ average-human-attention-span-statistics-and-facts

Allianz Commercial. (2023). *Cyber security trends 2023.*

Barreto, H. (2024). *The secret to creating brand loyalty. Forbes*

Brooks, C. (2023). *Cybersecurity Trends & Statistics for 2023; What You Need To Know. Forbes.*

Cisco. (2024). *Security Outcomes Report Vol. 3. Achieving Security Resilience.*

Click. (2024). *A no bullshit paper: A manifesto for Effortless Culture Change.*

Deloitte. (2022). *Global Future of Cyber Survey 2023. Building long-term value by putting cyber at the heart of the business.*

European Parliamentary Research Service. (2023). *The NIS2 Directive. A high common level of cybersecurity in the EU*

Farnam Street (2021) *The Great Mental Models Volume 2: Physics, Chemistry, and Biology*

Fortanix. (2023). *Preparing for post-quantum cryptography. Mapping your organization's data security strategy to the effects of quantum computing*

Fortinet (2022). *Cybersecurity skills gap.*

Gartner. (2023). *Gartner Identifies the Top Cybersecurity Trends for 2023.* [press release]

Heino, M et. al. (2024) *From a false sense of safety to resilience under uncertainty.*

IBM (2024) https://www.ibm.com/topics/phishing

LastPass (2024). *Combating Social Engineering in 2024.*

International Telecommunication Union. (2021).

McKinsey & Company. (2022). *Cybersecurity trends: Looking over the horizon.*

Pentera (2024) *The State of Pentesting 2024*

PWC (2021), *Global Culture Survey.*

Radar. (2024). *Cybersäkerhet 2024. Från verksamhet till ekosystem.*

Seenit (2023). *The State of Employee Engagement.*

Sentor. (2021). *ISO 27001. En introduktion till standarden.*

Snowflake. (2024). *Data + AI predictions 2024..*

Splunk (2024). *State of Security 2024: The Race to Harness AI*

SVT (2024), *Allvarliga brister i svenska myndigheters cybersäkerhet*

Telenor. (2024). *Digital Security 2023. It gets serious.*

Telia (2024) *Telia Digital Index (2024).*

World Economic Forum. (2024). *The Global Risks Report 2024.*

World Economic Forum. (2024). *Global Cybersecurity Oulook 2024.*