gds Security Summit

Security Insight Summit

Lisbon, 07-08 May 2025

Insight Report from the Main Stage

Contents.

Security Insight 2025

Thriving Amidst Uncertainty – Navigating Europe's Compliance and Resilience Challenges.

The Security Insight Summit in Lisbon brought together senior cyber leaders from across the spectrum of industries to tackle today's most pressing compliance and regulation management challenges – and a lot more besides.

We heard insightful discussions, bold strategies, and industry-shaping ideas on everything from bridging the trust gap to closing the skills gap.

If you missed out or maybe just wanted a refresher, here is a wrap-up of all the key takeaways from the main stage...

Resilience Revolution:
Cyber and Corporate Synergy

Speaker

Dr. Timo Wandhöfer
Group CISO / Head of Information Security & Business Continuity Management, Klöckner & Co. S.E.

Summary

Dr. Timo Wandhöfer's opening keynote centered on resilience in business, society, and the state. He stressed that for security professionals, the most critical starting point is a deep understanding of their own business and its diverse processes. Security challenges should be treated as business issues, not just technical ones. Crucially, demonstrating value beyond just quick recovery, such as increased IT quality and better processes, is vital for gaining stakeholder support.

Key Takeaways

Understand Your Business

The most important starting point for any security professional. Security issues must be addressed as fundamental business problems.

Measure Maturity and Plan

Implement and use frameworks like NIST to assess the current security maturity level. You're aiming for 3 or 4.

Define Roles for Collective Resilience

True organizational resilience relies on clearly defined responsibilities and accountability for every individual.

Demonstrate Value Beyond Technical Recovery

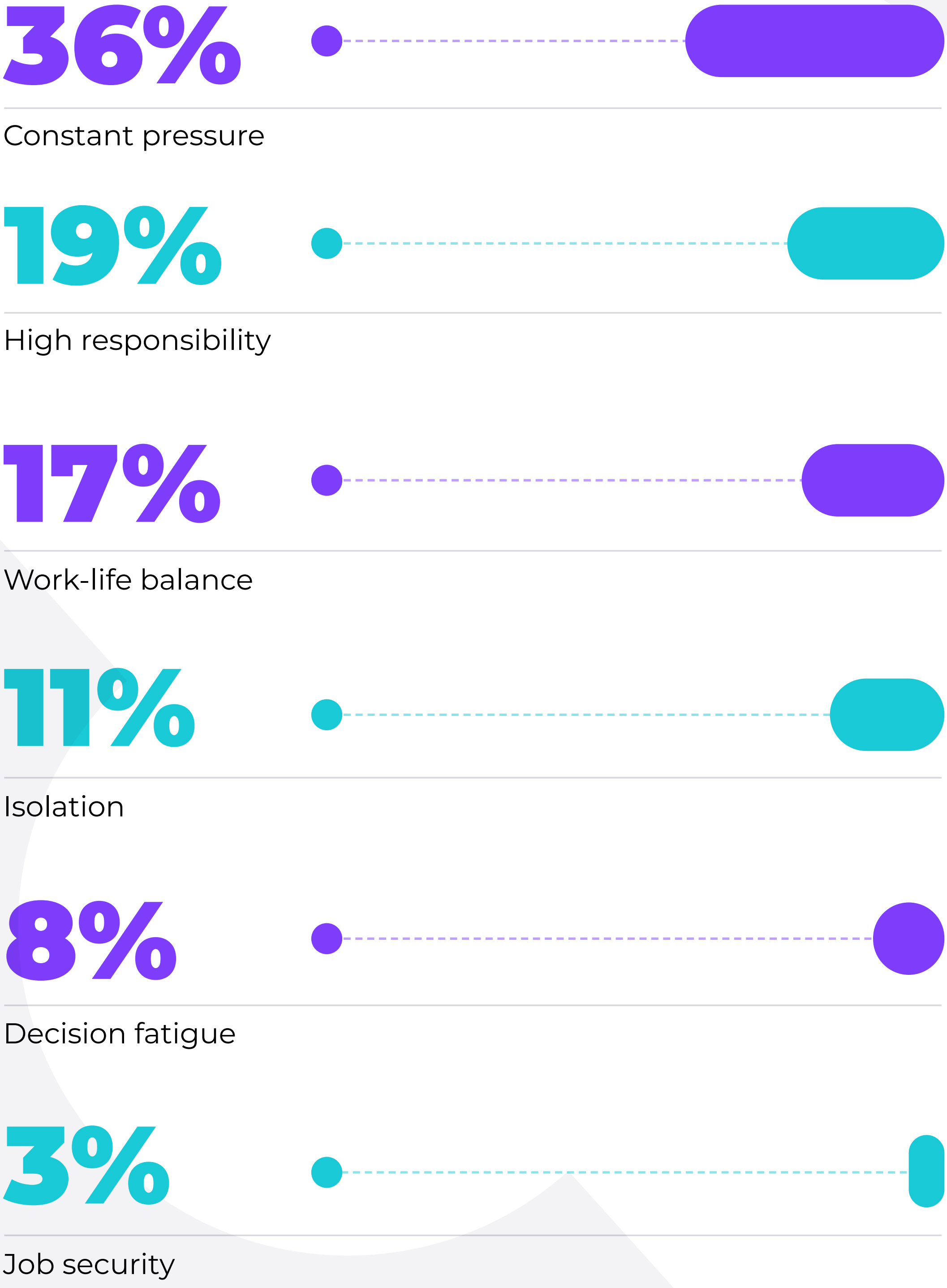
Prove the worth of security efforts by highlighting benefits (such as quantifiable improvements in IT quality) that resonate with stakeholders.

> **It is most important to know the business. What is the business all about? What are all the different processes? This is where we need to start.**

Dr. Timo Wandhöfer
Group CISO / Head of Information Security & Business Continuity Management, Klöckner & Co. S.E.

Audience Snapshot:

Which of the following gives you the most stress?



36%
Constant pressure

19%
High responsibility

17%
Work-life balance

11%
Isolation

8%
Decision fatigue

3%
Job security

Staying Ahead of EU Cyber Regulations:

A CISO's Compliance Roadmap

Speakers

Sam Rhea
VP, Strategic Advisor & Chief of Staff, Cloudflare

Robin Lennon Bylenga
CISO, VP of AI Security, DWS Group

Stefan Romberg
VP IT, Maxon

Summary

Our opening panel explored the complexities of governance, risk, and compliance and the impact of Artificial Intelligence. A central theme was the rapid pace of change, especially with AI, making it challenging to keep up with evolving regulations. Sam, Robin, and Stefan all emphasized the need for security professionals to be involved early and acknowledge that humans are not just a weakness but must be engaged and understood to navigate these complex challenges effectively.

Key Takeaways

Regulatory Complexity & Pace

The landscape of cybersecurity requirements and regulations is constantly evolving. Compliance a significant challenge for organizations.

AI's Dual Nature and Speed

Significant benefits and substantial risks. AI's adoption and capabilities require early security involvement.

Pervasive Third-Party Risk

Reliance on suppliers and third parties is increasing, leading to widespread third-party breaches. Many organizations still lack understanding and visibility.

Human Factors in Security

Security professionals must better understand human nature and engage people effectively to build a strong security culture.

> **People get a new tool, and they forget about data loss protection. They forget about information classification. They forget about everything that's ingrained in them that they would never do with email. But they found a tool.**

Robin Lennon Bylenga
CISO, VP of AI Security, DWS Group

Building High-Performing Teams with Compassion and Respect: Part One

Speaker

Milos Pesic
CISO, Accelleron

Summary

Milos Pesic's keynote centered on the human element in cybersecurity, emphasizing compassion, trust, and excellence. Milos believes that security is everyone's business, and empowering people makes them the strongest link. Building trust involves open communication, including the team in stakeholder interactions, and investing in their growth. Recovering from incidents requires emotional resilience and collaboration without finger-pointing. Making security engaging, embracing cyber psychology, and utilizing AI are future directions.

Key Takeaways

Cybersecurity is People

The human element is at the core of security. Involving people and connecting security to their personal lives are critical for resilience and effective security practices.

Empower and Invest

High-performing teams are built through support, recognition, and involvement. This investment yields significant returns.

Understand the Business

Effective security requires an understanding of processes, recognition of the roles of different departments, and alignment of the security strategy with business goals.

Embrace Change

Overcoming resistance to change involves making security fun and accessible through engaging activities.

> **I do believe that people are the strongest link, but not just because they can be or they need to be, it's because if you involve people, they feel more connected.**

Milos Pesic
CISO, Accelleron

Beyond the Firewall:
The Multidisciplinary Edge
in Cybersecurity

Speaker

Béatrice Cadet
Cyberthreat Intelligence Manager, KLM Royal Dutch Airlines N.V.

Summary

Béatrice Cadet demonstrated that cyber threat actors are already operating in a multidisciplinary manner, leveraging not only technology but also human psychology and the cognitive domain, such as exploiting stress and emotions. Effective defense requires integrating insights from diverse fields such as psychology, marketing, and communications to understand better and engage the human element. Successfully bridging these disciplines requires effort in translating perspectives and building a common understanding.

Key Takeaways

Multidisciplinary Defense

The modern cyber threat landscape is increasingly complex. It requires a multidisciplinary defense strategy that mirrors attacker tactics.

Human Psychology

Understanding human psychology is crucial because attackers actively exploit human vulnerabilities, such as stress, emotional biases, and attentional biases.

Expertise from Everywhere

Incorporating expertise from traditionally non-security fields (such as marketing and communications) is essential for effectively engaging people.

Common Ground

Achieving successful multidisciplinary collaboration involves translating concepts between different professional perspectives and building common ground.

> **In clinical psychology, we always say, if the patient is not motivated, there's no therapy. Because if the person does not understand the problem, you won't be able to go further.**

Béatrice Cadet
Cyberthreat Intelligence Manager, KLM Royal Dutch Airlines N.V.

Her, Me, and the Missing Trust Patch

Speaker

Virginie Coulloudon
Founder, Positive Leadership Coach

Summary

Virginie Coulloudon's dinner keynote focused on using AI to enhance emotional intelligence. This was about the need to protect trust and move from trying to convince others to influencing them, especially when dealing with resistance or fear. A key element is activating curiosity to understand others' perspectives and maps of the world, with AI serving as a "second brain" to analyze communication and help understand what motivates or scares others.

Key Takeaways

Leverage Curiosity to Influence

Instead of trying to convince people, activate curiosity in yourself to understand others, which opens space for collaboration and influence.

Listen More Than You Talk

When communicating, aim to listen for two-thirds of the time and channel your message in the remaining one-third.

Understand Others' "Map of the World"

Focus on understanding others' perspectives, motivations, and fears rather than just presenting your vision or expertise.

Use AI to Enhance Emotional Intelligence

Use AI as a tool to understand others' reactions better and enhance your emotional intelligence.

> **Work with AI for your emotional intelligence. Because, by definition, we are prisoners of our map, our vision**

Virginie Coulloudon
Founder, Positive Leadership Coach

Can AI Enhance Your Cyber Resilience?

Speakers

Valerie Ezinmo
CISO UK & Ireland, L'Oréal

Amir Vashkovar
Head of Philips Data Security, Philips

Vincent Meijer
CISO, ANWB

Summary

Our second panel focused on cybersecurity resilience, defining it as "the ability to adapt, absorb, and anticipate changing circumstances, encompassing technology, regulations, and geopolitical factors."

Valerie, Amir, and Vincent discussed AI's profound impact on ways of working and mindsets, highlighting the crucial balance between enabling AI adoption and implementing necessary controls. While acknowledging practical AI applications like policy chatbots and SOC tools, our panel voiced concern that threat actors might be leveraging AI capabilities more rapidly...

Key Takeaways

Defining Resilience

The ability to adapt, absorb, and anticipate changing circumstances, encompassing technology, regulations, and geopolitical factors.

AI's Transformative Impact

AI is fundamentally changing how people work and think about cybersecurity, requiring a careful balance between fostering innovation and maintaining controls.

Practical AI Applications

AI offers tangible benefits for security operations and compliance, such as automating policy lookups via chatbots or assisting SOC teams with investigations and responses.

Early Engagement Over Policing

Security teams are more effective when they are engaged with the business from the initial stages of projects.

> **AI is not just influencing technology or advancing our tools and stuff like that. It impacts the way of working, the mindset of the people.**

Valerie Ezinmo
CISO UK & Ireland, L'Oréal

Building High-Performing Teams with Compassion and Respect: Part two

Speaker

Milos Pesic
CISO, Accelleron

Summary

In his second presentation, Milos continued his critical discussion on building high-performing cybersecurity teams by emphasizing the importance of putting humans at the center. Build bridges with every division by openly communicating what the security team is doing and what they aim for, encouraging others to ask questions. Curiosity and kindness are essential for fostering collaboration and getting people to help. And acknowledging that you are not the smartest person in the room allows for better team performance.

Key Takeaways

Put Humans in the Middle

Putting humans at the center and empowering your team members is fundamental to building a high-performing cybersecurity function.

Build Bridges

Building collaborative bridges with other business divisions by communicating openly and inviting questions helps integrate security into the wider organization.

Foster a Culture of Curiosity

Fostering a culture of curiosity, kindness, and mutual acknowledgment encourages collaboration and overcomes potential resistance from others.

Embrace Humility

Successfully leading change involves convincing your team by sharing a clear long-term vision and embracing humility, recognizing that others also have valuable knowledge.

> **It took me probably around 15 years to learn that I’m not the smartest person in the room. Ever since I’ve embraced that, magic happens.**

Milos Pesic
CISO, Accelleron

Future Focus:
Unlocking Maximum Value from Cybersecurity Investments

Speakers

Anthony Ayanleke
Head of Cybersecurity, MUFG

Sree Kesanakurthi
CISO, ARC Europe Group

Summary

Anthony Ayanleke and Sree Kesanakurthi examined the challenge of cybersecurity investment and how to effectively convey its value to leadership. They emphasized the need to prioritize investments by linking them to business risks, utilizing data such as risk quantification, and providing real-life examples.

A central theme was the importance of balancing technical defenses with human factors, including training and establishing trust with stakeholders, such as the board and finance teams, to secure buy-in and maximize impact.

Key Takeaways

Justifying Investment

Securing necessary cybersecurity investments is challenging and requires articulating purpose and actual value.

Risk-Based Prioritization

Prioritizing investments should be driven by identified risks and their corresponding treatment plans, striking a balance between quick wins and long-term roadmaps.

Speaking the Board's Language

Gaining board buy-in requires using clear figures, quantifying risk, and providing real-life examples, including competitor breaches.

Building Trust and Accountability

Presenting a risk acceptance form can be a powerful motivator when faced with resistance.

> **If you can help the board visualize what could go wrong, then it's a much easier discussion to have**
>
> **Anthony Ayanleke**
> Head of Cybersecurity, MUFG

Closing the Cybersecurity Skills Gap

Happy Employees, Secure Future

Speaker

Vincent Meijer
CISO, ANWB

Summary

Our workshop session focused on the critical challenges related to the cybersecurity skills gap and building motivated, high-performing teams.

We discussed the need to improve team retention and morale by addressing the shortage of hands-on experience and practical skills, as well as enhancing training. We also touched upon insider risk, noting that frustrated employees who feel unable to make a difference are more likely to leave. Are you prepared for this risk?

Key Takeaways

Address the Practical Skills Gap

There is a significant shortage of hands-on experience and practical skills in the cybersecurity field.

Prioritize Team Retention and Morale

Improving how teams are trained, motivated, and kept happy is crucial for retention and reducing turnover in the industry.

Embrace and Facilitate Diversity

Actively seeking talent from diverse backgrounds is vital to enriching perspectives and closing the skills gap, but requires effort to bridge understanding.

Mitigate Frustration and Insider Risk

When teams feel stuck or unable to make a difference, it leads to frustration that can result in losing talent and potentially increases insider risk.

> **A lot of theoretical advice just doesn’t fit the operational reality, and that’s why there’s still a huge gap**

Vincent Meijer
Vice President, Talent Acquisition, Daikin Comfort

Digital Transformation Unleashed:

Securing the Future, Budgeting Smartly, Staying Compliant

Speaker

Juan Manuel Muñoz Perales

Corporate Assistant Director, Security in Strategic Digital Initiatives, MAPFRE

Summary

Our closing keynote speaker, Juan Manuel Muñoz Perales, focused on evolving security approaches to align with modern business needs – shifting from a traditional, centralized security model to a product security approach, embedding security within development teams, and focusing on individual products. Ultimately, this transformation aims to improve time to market, compliance, and business understanding by embedding security earlier in processes.

Key Takeaways

Shift to Product Security

Create dedicated roles (security transformation leaders) who understand both the business and IT aspects of specific products.

Measure and Demonstrate Value

Security personnel focused on product security must have a deep understanding of the business value and processes related to their assigned products.

Business Understanding is Crucial

Prioritize significant risks and critical vulnerabilities on dashboards to maintain the attention of business stakeholders, rather than overwhelm them with minor issues.

Focus on Key Risks for Business Buy-in

Prioritize significant risks and critical vulnerabilities on dashboards to maintain the attention of business stakeholders, rather than overwhelm them with minor issues.

> **We are not regretting our traditional security approach. We are not getting rid of it. We are simply evolving our organization, our approach, trying to be more focused on what we call product security**

Juan Manuel Muñoz Perales

Corporate Assistant Director, Security in Strategic Digital Initiatives, MAPFRE

Beyond the Challenges

Speakers

Nnambi Ozonma
Information Security Officer, UK & Nordic Regions, Bilfinger

Amir Vashkovar
Head of Philips Data Security, Philips

Summary

Anthony Ayanleke and Sree Kesanakurthi examined the challenge of cybersecurity investment and how to effectively convey its value to leadership.

They emphasized the need to prioritize investments by linking them to business risks, utilizing data such as risk quantification, and providing real-life examples.

A central theme was the importance of balancing technical defenses with human factors, including training and establishing trust with stakeholders, such as the board and finance teams, to secure buy-in and maximize impact.

Key Takeaways

Third-Party Risk is a Universal Challenge

It impacts every organization, demands a thorough understanding of suppliers, and necessitates a continuous, planned approach instead of merely using a tool.

Understanding is Fundamental to Managing Third-Party Risk

Identifying and understanding internal assets, particularly people ("your people and the people you're working with") is a critical starting point.

AI Adoption FOMO

Many feel pressure to leverage generative AI heavily, yet the reality is that most organizations are still exploring. Learning from others is beneficial.

Human Intelligence and Ethics Must Guide AI Use

Despite the capabilities of AI, organizations must not abandon human judgment, ethical considerations, business standards, and privacy standards.

> **We all feel a little bit of FOMO. We all think that everyone is doing magic and leveraging a lot of AI. And yet, when you start asking people, most of us are just still in the very early stages.**

Amir Vashkovar
Head of Philips Data Security, Philips

People, process, technology... And business alignment.

Our Security Insight Summit community covered a wide range of topics. With security these days, there is so much to discuss, which highlights the elevated importance of our profession in the modern business landscape.

We explored the human element in cybersecurity – the importance of compassion, trust, and respect for building effective teams and fostering resilience. Addressing major incidents requires emotional resilience and global collaboration with no time to point fingers.

We discussed the rapidly evolving landscape of AI, its risks and opportunities, including its potential use to enhance emotional intelligence.

While perennial themes, such as complex governance, risk, and compliance, and managing third-party risk, were given a thorough examination. The latest thinking was applied and shared liberally.

The most important takeaway?
There are two. Security is everyone's business, and engaging people by connecting security to their lives makes them the strongest link. And to be truly effective, security must align with business objectives, demonstrate value through metrics, and be engaging.

Stay tuned

Our content doesn't end here – look out for more blogs, interviews, and footage from the summit, and be sure to check out our calendar of upcoming events.

We look forward to seeing how you apply these insights to advance your organization and navigate uncharted waters.

See you next time!

gds

Register your interest here

Security Insight is a GDS Summit. GDS Group is the data-driven executive engagement company. Our mission is to empower our executive and partner communities. Accelerating their growth through transformative relationships and actionable insight.