ChatGPT

Kai Roer's Contributions to Cybersecurity

Research and Publications

Books (2010–present): Kai Roer has authored and co-authored several books on leadership and cybersecurity. Notable titles include *The Leader's Workbook* (2010) – an Amazon bestselling leadership guide, *The Cloud Security Rules* (2011) – a primer on cloud technology risks (with contributions from experts like Anton Chuvakin), and *Build a Security Culture* (2015) – a foundational handbook introducing Roer's Security Culture Framework. Most recently, he co-authored *The Security Culture Playbook* (Wiley, 2022) with Perry Carpenter, which provides executives with strategies to measure and improve their "human defense layer". These books are widely regarded as key resources on security culture and human-centric security practices.

Peer-Reviewed Research: In addition to books, Roer has contributed to academic research on security behavior and culture. In 2022 he co-authored *"Phishing Susceptibility Across Industries,"* a study presented at the 16th International Conference on Augmented Cognition (part of HCI International 2022) comparing how different sectors fall prey to phishing. He also partnered with social scientist Prof. Gregor Petrič on a 2022 journal article in *Telematics and Informatics* examining how formal vs. informal organizational norms impact phishing susceptibility. Earlier, Roer and Petrič produced research on credential-sharing behaviors: *"Security Culture and Credential Sharing – How Improved Security Culture Reduces Credential Sharing in Cybersecurity"* (2021), which combined survey and field experiment data to link strong security culture with reduced password sharing. This body of empirical work – often done in collaboration with academic partners – provides scientific validation for security culture concepts.

Industry Reports and Whitepapers: As a researcher-practitioner, Roer has led the creation of industry reports that benchmark human factors in security. He launched an **annual Security Culture Report** series at his company CLTRe in 2017, providing data-driven insights into the "human factor" of security across organizations. For example, the *Security Culture Report 2018* compared security culture scores across 8 countries and 7 languages, revealing significant national differences. After CLTRe's acquisition, Roer (as KnowBe4's research chief) continued this work, producing large-scale Security Culture Reports in 2020, 2021, and 2022 based on data from hundreds of organizations worldwide. These reports introduced the "Security Culture Survey" and its seven-dimension model (Attitudes, Behaviors, Cognition, Communication, Compliance, Norms, Responsibilities), giving organizations concrete metrics to track their security culture. Roer has also published whitepapers translating research to practice – for instance, *"To Measure Security Culture – A Scientific Approach"* (2018), co-authored with Petrič, which outlines methodological steps to quantify security culture in an organization.

Articles and Columns: Beyond formal publications, Roer has written extensively in industry media to spread security culture insights. He was a columnist at *Help Net Security*, where he penned the "Security Startup Confessions" series (2016) sharing lessons from building a security company. He has contributed opinion pieces to outlets like *Infosecurity Magazine* (e.g. *"A Culture of Security, Not of Blame,"* 2017) and is a featured expert in cybersecurity blogs and podcasts. (For example, he's been interviewed by *Cybercrime Magazine* about the evolution of security culture programs.) According to his speaker bios, Roer's writing credits span dozens of print and online publications, and he has served as a guest expert blogger for professional audiences. This mix of books, research papers, industry reports, and articles underscores Roer's role in both advancing academic knowledge and providing practical guidance on cybersecurity culture.

Entrepreneurial Contributions

The Roer Group (1994–2016): Roer's entrepreneurial journey began in the mid-1990s. In 1994 he co-founded *The Roer Group*, a European management consulting firm focused on information security, communication, and leadership development. Through the Roer Group, he spent over a decade advising organizations on strategic leadership and IT security challenges, pioneering the idea that security culture is an integral part of organizational culture. Roer served as founder and CEO, delivering consulting and training in more than 20 countries and organizing events like the Roer Conference on Sustainable Leadership. This early venture established his reputation as an innovative security coach and provided a platform for developing the Security Culture Framework in the 2000s.

CLTRe – "Culture" (2015–2019): In 2015, Kai Roer teamed up with socio-informatics expert Dr. Gregor Petrič to launch *CLTRe AS* (pronounced "Culture"), a Norwegian startup and the world's first SaaS company dedicated to measuring and managing security culture. As CEO and Founder of CLTRe, Roer built a software platform that allowed organizations to survey and score their internal security cultures across the seven dimensions he developed. This innovation gave businesses a concrete "yardstick" for the human factors of security – an ability to pinpoint cultural strengths and weaknesses that was previously missing in the industry. Under Roer's leadership, CLTRe also produced an annual Security Culture Report (noted above) to share industry benchmarks. The company quickly gained global recognition for turning the abstract concept of security culture into a measurable, improvable part of security programs. In mid-2019, CLTRe was acquired by KnowBe4, Inc., the U.S.-based leader in security awareness training. This acquisition validated CLTRe's impact – as Roer noted, in just a few years CLTRe built a brand and product portfolio that attracted a global client base and industry acclaim.

KnowBe4 and Research Leadership (2019–2023): After the acquisition, Roer joined KnowBe4's executive team, where he served as **Chief Research Officer** from 2019 to 2023. In this role he integrated CLTRe's capabilities into KnowBe4's platform and founded the **KnowBe4 Research** division [1]. Roer led a team of researchers focused on "bridging the gap between theory and practice" in cybersecurity – partnering with academia, analyzing KnowBe4's vast training and phishing data, and publishing findings to improve security behavior worldwide. Under his guidance, KnowBe4 Research released new editions of the Security Culture Report (covering hundreds of thousands of employees) and whitepapers on topics like security behavior and risk metrics. Roer's tenure helped KnowBe4 evolve beyond training into an evidence-driven thought leader on human risk. By 2023, after ensuring a strong research culture at KnowBe4, Roer decided to return to hands-on entrepreneurship.

Praxis Security Labs (2023–present): In 2023, Kai Roer co-founded *Praxis Security Labs*, where he currently serves as CEO. Praxis is a new venture building a SaaS "human risk management" platform, aiming to unify data about human behavior and security (e.g. training scores, phishing test results, cultural metrics) to improve organizational cyber resilience. The company's approach reflects Roer's multidisciplinary philosophy – the team includes experts in statistics and psychology (some of whom collaborated with Roer on prior research) to develop advanced analytics on human factors. At Praxis, Roer is again driving innovation at the nexus of cybersecurity and behavioral science, this time applying lessons learned over decades to create tools that *operationalize* security culture management for enterprises. Though early-stage, Praxis has been positioned as an "unfair advantage" for organizations seeking to reduce human cyber risk, and Roer's industry standing lends credibility to this ambitious startup.

Other Ventures and Roles: Throughout his career, Roer's entrepreneurial spirit led him to spearhead numerous initiatives. He has founded companies, authored startups' business plans, and mentored emerging security entrepreneurs. For example, as a side venture he created *Security Culture TV*, a

monthly video podcast started in the 2010s to discuss human-centric security trends. Additionally, Roer has been active in standardization and non-profit projects (detailed below) that, while not companies, exhibit his drive to build communities and frameworks from the ground up. From the mid-1990s onward, every venture Roer has touched – whether a consulting firm, product startup, or corporate research lab – has reinforced his overarching mission to strengthen security through better understanding of people and culture.

Public Speaking and Media Appearances

For over 25 years, Kai Roer has been an energetic public speaker, keynote presenter, and media commentator on security, culture, and leadership. **Since the 1990s,** he has appeared at countless events worldwide (over 40 countries on 4 continents). Below is a selection of his speaking engagements and media appearances, illustrating the breadth of his outreach:

- **International Leadership Forums (1990s–2000s):** Roer honed his public speaking in the late 90s through early 2000s as a trainer with Junior Chamber International (JCI). He delivered workshops on leadership and personal development across Europe, earning recognition such as *International Training Fellow* status in JCI. Notably, he spoke at the **JCI World Congress** in 2009 (Hammamet, Tunisia), 2010 (Osaka, Japan), and 2011 (Brussels, Belgium), inspiring global audiences on topics of leadership and security culture. He also addressed the **JCI European Conference 2011** in Tarragona, Spain, and led JCI-sponsored public speaking courses in locations like Stockholm, Porto, and Reykjavik in this period. These early appearances established Roer's reputation as an engaging, motivational speaker capable of connecting with diverse audiences.

- **Cybersecurity Conferences (2010s):** As Roer's focus shifted to information security, he became a sought-after speaker at security industry conferences. In **2014**, as president of the Cloud Security Alliance (CSA) Norway Chapter, he began hosting chapter meetings on topics like mobile security, often to sold-out audiences in Oslo. He has since delivered keynotes and sessions at major events such as the **RSA Conference** and regional cybersecurity summits. For example, at **RSA Conference Asia Pacific 2017**, Roer presented "How Measuring Security Culture is Different from Counting Employees," sharing his pioneering metrics approach with an international crowd of security professionals [2]. He has also headlined events like the **CISO 360 Congress** (virtual in 2020), where he spoke as an "award-winning specialist on security culture and behaviors" and shared insights from his research. Roer's talks often blend data and storytelling – he explains the psychology of cyber threats in relatable terms, leaving audiences with practical steps to build a strong security culture.

- **Recent Engagements (2020s):** Roer continues to appear on the global stage. In December 2023, he served as a moderator at the **Black Hat Europe 2023 Executive Summit** in London, leading CISO panel discussions on human-centric security strategy. He is a regular presenter at **KnowBe4's KB4-CON** and other industry events, frequently invited to discuss the findings of the latest Security Culture Reports. Even during the COVID era, Roer adapted by giving virtual keynotes and webinars, ensuring the message of security culture reached organizations adapting to remote work risks. His engaging style – often incorporating humor, real-world anecdotes, and audience interaction – consistently earns high praise. (As one conference organizer noted: "Absolutely excellent! The quality of the presentations and ideas shared were first class".)

- **Media Interviews and Commentary:** Beyond conferences, Kai Roer is a familiar name in media coverage of cybersecurity's human aspect. He has appeared on radio and television to discuss topics like social engineering and corporate risk culture. Norwegian news outlets and tech programs have interviewed him on how human behavior affects security (for instance, explaining major phishing incidents on national TV). Internationally, Roer has been featured in print media – he has provided expert commentary to magazines and newspapers on security awareness trends. In 2020, *Cybercrime Magazine* profiled Roer in a podcast interview, where he traced the history of CLTRe and the importance of measuring security culture. He has also guested on podcasts such as the *InfoSec Security Influencers* series, discussing human factors in cybersecurity. In written media, Roer's insights have been quoted in outlets like *Infosecurity Magazine*, *Help Net Security*, and *CSO Online* on topics ranging from avoiding a cybersecurity "blame culture" to effectively communicating security to executives. Notably, Roer was a columnist for *Help Net Security*, where his "Security startup confessions" articles provided candid advice to entrepreneurs in the security field.

- **Audience Impact:** Many of Roer's speaking engagements have targeted large and influential audiences. At the 2015 CSA EMEA Congress, where he received an award, he spoke to an audience of industry peers and cloud security leaders. His keynote at RSA APJ reached hundreds of delegates and was later made available online due to popular demand. Even his webinars can draw thousands of registrants given KnowBe4's global customer base. Roer's ability to engage audiences of all sizes – from intimate workshops of 20 people to conference halls of 500+ – stems from his focus on interaction and clear messaging. He often polls audiences or uses live examples to illustrate how culture changes can reduce risk, making his sessions memorable and actionable. The impact of his public speaking is evident in the uptake of concepts like the "7 dimensions of security culture" by organizations worldwide, many introduced to these ideas through Roer's talks.

In summary, Roer has spent decades on the speaker circuit championing the human element of cybersecurity. Whether keynoting a major conference, moderating a CISO panel, or giving a media interview, he consistently raises awareness that improving security culture is vital in thwarting cyber threats. His enthusiasm and clarity have made him an influential public educator in the cybersecurity community.

Industry Influence and Collaboration

Security Culture Framework and Standards: One of Roer's most significant contributions is the development of the *Security Culture Framework (SCF)* in 2010 and its influence on industry standards. He created the SCF as a free, open-source methodology to help organizations build and sustain a robust security culture. In practice, this framework provides a step-by-step process – from assessing culture, to implementing targeted interventions, to measuring outcomes – that organizations around the world have adopted. Roer freely shared the SCF with the community, and it quickly gained traction. Notably, the **European Union Agency for Cybersecurity (ENISA)** incorporated Roer's framework into its own guidelines: ENISA's 2015 *"Cybersecurity Culture in Organizations"* report explicitly cites that its recommended 8-step implementation framework is *"grounded on the Security Culture Framework developed by Kai Roer,"* adapted with input from European practitioners. In other words, Roer's work directly informed EU-level best practices for cybersecurity culture programs. This cross-pollination exemplifies how Roer's ideas have shaped policy: by gifting SCF to the open-source community, he enabled governments and large enterprises to build upon a proven model rather than starting from scratch. Today, the concept of "security culture" as a measurable program is increasingly embedded in standards (for example, ISO and NIST have begun addressing organizational security culture), a trend Roer helped initiate through early advocacy and sharing of the SCF.

Professional Community Leadership: Roer has a long history of volunteering and leading within cybersecurity professional organizations. Since 2012, he has been an active member of the **Cloud Security Alliance (CSA)**, serving as founding President of the CSA Norway Chapter. In this role, he organized local events, fostered knowledge exchange among security professionals, and contributed to CSA's global initiatives. Roer's dedication to the community was recognized with the **Ron Knode Service Award** in 2015 – CSA's annual award honoring outstanding volunteer contributions worldwide. In the award citation, CSA noted Roer's passion for volunteerism and his work in spreading best practices for cloud and information security. He continues to be involved with CSA internationally, often speaking at CSA conferences and advising on security culture matters. Additionally, Roer is a Fellow of the **National Cybersecurity Institute** (NCI) in Washington, D.C., which is a think-tank and training body – this fellowship recognizes his expertise in cybersecurity education and allows him to collaborate with other experts on research and policy advocacy.

Beyond CSA and NCI, Roer has collaborated with numerous industry groups. He was (per an RSA Conference bio) a **columnist for Infosecurity Magazine** and an expert panelist in various security forums, indicating his role in shaping industry discussions. He has lent his expertise to the *Honeynet Project* community as well, focusing on the human factors of cyber attacks. Through such roles, Roer contributes to developing frameworks and recommendations that organizations use to manage human risk.

Academic and Corporate Collaborations: Roer's work exemplifies a bridge between academia and industry. He has partnered with university researchers to bring scientific rigor to cybersecurity practice. For example, his collaboration with Prof. Petrič (University of Ljubljana) not only produced research papers but also improved CLTRe's methodology by incorporating social science techniques (survey design, statistical modeling of culture). Another collaborator, Dr. Thea Mannix (PhD in psychology), worked with Roer on the 2022 phishing susceptibility study, blending neuroscience insights with security data. Roer has served as a *guest lecturer at multiple universities* – including BI Norwegian Business School and University of Oslo – where he teaches about security culture and risk communication. Through these academic engagements, he influences curricula and inspires the next generation of cybersecurity professionals to consider human and cultural aspects, not just technical ones.

On the corporate side, Roer frequently advises Fortune 1000 companies and government agencies. He has worked closely with CISOs and management teams to implement culture programs. In some cases, he's been brought in as an external consultant to diagnose an organization's security culture using his metrics and recommend improvements (for instance, through The Roer Group and later via KnowBe4's services). His company Praxis Security Labs is currently running a *Design Partner Program* with organizations, collaborating directly with industry partners to refine new human-risk management tools. Such partnerships ensure that his solutions are aligned with real-world needs and that collaborating organizations stay at the cutting edge of security culture management.

Roer has also been involved in **international policy dialogues** on cybersecurity awareness. As a recognized expert, he has contributed to panels and workshops by bodies like ENISA (as mentioned) and the EU's cyber agencies, offering guidance on how to incorporate cultural indicators into national cybersecurity assessments. His membership in professional councils (e.g., as noted in his Black Hat Exec Summit bio, he sits on or advises industry boards) allows him to champion the human factor in strategic security discussions.

Influence on Industry Mindset: Perhaps Roer's greatest industry impact has been normative – influencing how security leaders think about security culture. When he began evangelizing "security culture" over a decade ago, many saw security awareness training as a checkbox compliance activity.

Roer's research and advocacy shifted the dialogue towards treating security culture as a *measurable, improvable component* of security strategy. Terms and concepts he helped popularize (like the seven dimensions of security culture, or the notion of a "security culture maturity model") are now common vocabulary in the field. Global companies in sectors from banking to manufacturing have adopted culture metrics similar to CLTRe's, demonstrating the ripple effect of Roer's work. Moreover, Roer's collaboration with other thought leaders – e.g. co-authoring *The Security Culture Playbook* with Perry Carpenter – has further disseminated his approach to a broad executive audience, influencing decision-makers beyond the security team. In summary, through open collaboration, thought leadership, and volunteer service, Kai Roer has significantly shaped the industry's frameworks and best practices related to the human element of cybersecurity.

Overall Impact and Influence Summary

Human-Focused Cybersecurity Pioneer: Kai Roer is widely regarded as a leading authority on security culture and the human factors of cybersecurity. Over his career, he has fundamentally reframed how organizations approach security by emphasizing that technology alone is insufficient – the behaviors, beliefs, and culture of people are the "missing piece" in effective cyber defense. Roer's impact is evident in the vocabulary and priorities of today's security programs: terms like "security culture", "human firewall", and "measuring security behaviors" have entered the mainstream in large part due to his advocacy and empirical work. By providing a practical framework and metrics, he gave security leaders tools to treat culture as a core pillar of security (alongside technology and policy), rather than an abstract concept. This has enabled executives to benchmark their organizations' security culture and drive improvements with the same seriousness as they address technical vulnerabilities.

Strategic Thinker and Author: As a best-selling author and researcher, Roer has disseminated his ideas globally. His books and reports have been read by thousands of professionals and cited in academic literature, influencing both practice and research. *Build a Security Culture* (2015) remains a go-to handbook for building awareness programs that truly influence behavior. *The Security Culture Playbook* (2022) now guides executives on integrating culture into risk management, reflecting Roer's ability to address both practitioner and board-level audiences. Through these writings, he has equipped organizations with strategies to transform their security cultures from reactive "blame and compliance" models to proactive, risk-aware, and inclusive environments. The long-term benefit is a more sustainable security posture: Roer's approach helps reduce incidents (like phishing breaches) by tackling root causes in human behavior, not just symptoms. Industry surveys (e.g. a Forrester study cited in Roer's work) show that an overwhelming majority of security leaders now recognize a strong security culture as critical to their security program – a testament to the awareness Roer helped build.

Mentorship and Community Impact: Beyond his direct work, Roer has inspired many others in the field. He is known for being generous with his time in mentoring upcoming professionals, whether through formal roles (like training young leaders in JCI or advising startups) or informally guiding colleagues. His volunteer leadership in CSA and other groups has built local and global communities that continue to evangelize better security practices. The Ron Knode Award he received underscores how his "energy and incredible generosity" have benefited the community. Furthermore, Roer's emphasis on volunteerism (he often says that contributing to the community is as important as business success) has encouraged a culture of knowledge-sharing in cybersecurity. Many practitioners who have heard Roer speak or read his work have adopted his mindset and gone on to lead security culture initiatives in their own organizations, multiplying his impact.

Bridging Theory and Practice: A hallmark of Roer's influence is his ability to bridge disciplines – he combines insights from psychology, sociology, and communications with deep cybersecurity expertise.

This interdisciplinary approach was ahead of its time and is now becoming standard as organizations realize cybersecurity is as much about people as technology. Roer has collaborated with academic researchers to ensure that security culture interventions are evidence-based, and conversely, he has brought practical questions from industry into academic research. The result is a richer understanding of topics like why employees fall for scams or how organizational norms affect security outcomes. Few in the industry have the credibility to speak to both a technical security audience and a social science audience – Roer does, and he's managed to get these groups speaking to each other. His work on measuring culture has even sparked new research directions (for example, studies on cultural predictors of phishing susceptibility cite Roer's initial reports).

Global Cultural Change Agent: Ultimately, Kai Roer's impact can be seen in the gradual shift of organizational cultures worldwide. Through his company's tools and his evangelism, thousands of employees (from bank tellers to software engineers to executives) have become more aware of security in their daily job behaviors. By introducing concepts like positive reinforcement, openness, and "security as a shared responsibility" into corporate cultures, Roer has helped replace the old "blame and shame" approach with one of continuous improvement and learning. Companies that have implemented his methods report not only better compliance, but also more *engaged* employees who actively contribute to security (for instance, by reporting incidents or following policies more diligently). In a field often focused on technical innovation, Roer's contribution has been a human innovation – showing that empowering people is the real key to managing cyber risk. This perspective is now influencing high-level strategy: boards of directors and C-suite leaders, who traditionally only asked about firewalls and audits, are asking their CISOs, "How do we know if we have a good security culture?" – a question straight out of Roer's playbook.

In summary, Kai Roer's professional journey has made a profound mark on cybersecurity by elevating the importance of human behavior and culture. Through research, entrepreneurship, public speaking, and collaboration, he has injected the human dimension into the heart of cybersecurity strategies globally. His work on security culture and risk culture has transformed it from an academic concept into an actionable, strategic practice for organizations of all sizes. The ripple effects of his contributions – more secure behaviors, better-informed leadership, and a culture of shared cyber responsibility – continue to enhance the security of countless organizations in an era of ever-evolving threats. As a thought leader and change agent, Roer has ensured that people are recognized not as "the weakest link," but as essential defenders in the cybersecurity chain.

---

1 Build a Security Culture: IT Governance Publishing: 9781849287166: Amazon.com: Books
https://www.amazon.com/Build-Security-Culture-Governance-Publishing/dp/1849287163

2 Measuring security culture is different from counting employees | PDF
https://www.slideshare.net/slideshow/measuring-security-culture-is-different-from-counting-employees/78337936