EPiC Series in Computing

Volume 107, 2025, Pages 88–97

Proceedings of EUNIS 2025 annual congress in Belfast

EPiC Computing

# A systemic perspective to the Human Firewall Problem (HFP): the AwAKE approach

Giuliano Pozza (C.I.O.), Filippo Colombo (C.I.S.O.), Alberto Frati (Focal point for training - IT department) and Carmelo Andrea Scordino (IAM Product & Information Security Specialist)*

[1]Università Cattolica del Sacro Cuore, Italy

giuliano.pozza@unicatt.it, filippo.colombo@unicatt.it, alberto.frati@unicatt.it, carmeloandrea.scordino@unicatt.it

* **Giuliano Pozza** - is the Chief Information Officer of Università Cattolica del Sacro Cuore, one of the most important private universities in Europe. Previously Giuliano worked as Chief Information Officer (CIO) for San Raffaele Hospital, a top clinical research institution in Italy. He is also the Past President of the Italian Association of Healthcare Information System Professionals (AISIS). Previously, he has been the CIO of Fondazione Don Carlo Gnocchi Onlus and Istituto Clinico Humanitas. The first part of his career was in the consulting firm Accenture, where he worked for healthcare, pharma, telecom and automotive clients. He likes hiking and trekking on the Alps, reading and sometimes writing (www.yottabronto.net).

**Filippo Colombo** - Is the Chief Information Security Officer of Università Cattolica del Sacro Cuore. Previously he was Chief Technical Officer at the same University, for a long time (10 years). Since 2018 as CISO he has responsible for the implementation of the business plan, in the different areas, of cyber risk mitigation measures with a focus on identity management and the evolution of cyber security training. He likes trekking and gardening.

**Alberto Frati** - Graduated in mathematics, with a PhD in computational mathematics, he has taught mathematics and physics and has been an adjunct professor at the Università Cattolica del Sacro Cuore; since 1994 he has been working in the IT Department of the Università Cattolica del Sacro Cuore and currently also holds the role of Focal point for training in the IT department. Passionate about astronomy, physics, music, art ... and mountains.

**Andrea Carmelo Scordino** - Graduated in Telecommunications Engineering. He worked at Accenture in the Digital Identity field, mainly for telco clients, where he learned and consolidated the notions of Identity Governance. After many years in that role, he now works at the Università Cattolica del Sacro Cuore where he can make the most of his experience and increase his skills by working in collaboration with the CISO and horizontally expanding his scope of work with the role of IAM Product & Information Security Specialist.

L. Desnos, R. Vogl, L. Merakos, C. Diaz, J. Mincer-Daszkiewicz and S. Mclellan (eds.), EUNIS 2025 (EPiC Series in Computing, vol. 107), pp. 88–97

**Abstract**

Università Cattolica del Sacro Cuore (UCSC), being a university and part of the Catholic ecosystem, experiences constantly a high level of cyber risk exposure in a complex, multi-cultural and heterogeneous environment. The challenge is to dramatically improve the performance of the "Human Firewall", thus extending the reach of cybersecurity professionals and improving UCSC security posture. The journey started with a first group of "Security Ambassadors", a sort of "volunteer firemen" able to support the professional IT security expert. Along the way, several initiatives to improve Awareness, Abilities, Knowledge and Emotional Engagement (AwAKE approach) were launched, with proved outcomes. Currently, we are working to expand the use of emotional engagement techniques to capture the attention of refractory users. Specifically, spatial computing technologies, AI and simulation/gamification approaches are used to capture the attention and emotions of unapproachable users. The activities carried out pursue the objective indicated by the ACN (Italian National Cybersecurity Agency) regarding training and awareness (ACN 2024).

# 1 Context and challenges

The "Human Firewall" concept (HF) has been around for some time now in the cyber security space (Edegbeme-Beláz, 2020). The term is used to describe people who follow best practices to prevent or report data breaches and suspicious activities. Its value is self-evident, since some studies report that up to 74% of data breaches (Verizon, 2023) involve the human element and other statistics scale up to 95% the role of the human element (IBM, 2022).

With the "Human Firewall Problem" we mean the challenge of building an effective, consistent and sustainable barrier to cyber-attacks by means of security-aware and security-trained employees. If the context and the goals are easy to understand, the implementation is arduous. First, to be successful a HF should have a higher level of effectiveness. Indeed, our objective was to improve dramatically the ability to identify and disarm phishing attacks. Moreover, we needed to be consistent in our ability to react to threats. If being better than average is difficult, being consistent is strenuous. Finally, developing an effective and consistent human firewall is a journey: it requires resources and puts a lot of pressure on the entire organization. You need to be continually alert, motivated and engaged. It is paramount to plan the journey in a way that is sustainable for the organization and the people involved.

# 2 The case: Università Cattolica del Sacro Cuore (UCSC)

UCSC, being a university and part of the Catholic ecosystem, experiences constantly a high level of cyber risk exposure (Nature, 2024) (Greig, 2023) in a complex, multi-cultural and heterogeneous environment. The challenge, in the UC context, is to set up a Human Firewall composed of user clusters with extremely heterogeneous cultures: administrative staff, instructors, students. To test the approach, we started with administrative staff. We pursued a multi-format approach composed of five parallel streams:

- **Creation of the "Security Ambassadors" community:** since one of our pain points was the size of our IT Security team, the first step in our journey has been the set-up of a "volunteer fire department" to extend the reach of the IT security professional team. We targeted 10% of the total number of administrative staff in UCSC and created a specific training and certification path for them. We used AICA ICDL IT Security training and certification program (AICA, 2021) as the primary framework, but the true aim was to set-up a community of practice. The Security Ambassadors attend monthly meetings with the CISO and other IT Professionals to keep their competencies up to date and to foster their motivation. The selection of the candidates combines the evaluation of spontaneous applications with the need for a homogeneous distribution in the different offices and departments. Up to date we have 154 Ambassadors (around 13% of staff) distributed on all organization levels and campuses. Their effectiveness is demonstrated by the statistics on ethical phishing (see Figure 1: Normalized click rate by campaign: ambassadors vs general.), where they consistently outperform other professional clusters.

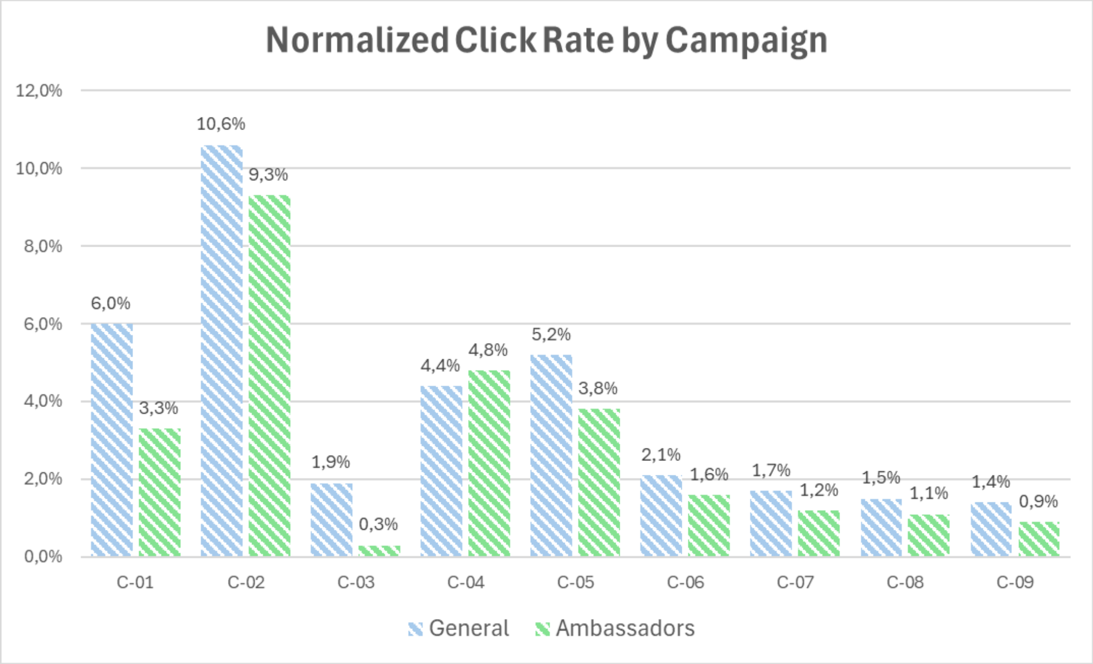


**Figure 1: Normalized click rate by campaign: ambassadors vs general. C-n are the phishing campaigns.**

- **From awareness to knowledge to ability:** the “Security Ambassadors” strategy was extremely successful and effective, but it does have a fundamental flaw: it is difficult to scale up. We needed a more “industrialized” and sustainable approach to cybersecurity training to reach a larger population. In 2023 we activated the Cyber Guru platform (Cyber Guru, 2024) which provides several interesting functionalities:

  - A three-year course called “Cyber School” to improve awareness and knowledge of the fundamentals of cyber security. At the end of each short learning module (5-7 minutes) a test will verify the competence of the learner.

  - Adaptive ethical phishing: monthly campaigns using up to ten concurrent. We run the first campaign before the activation of the learning modules, and we continued to test organizational resilience with the following campaigns. The campaigns are adaptive, since the level of difficulty was not constant, but was automatically adapted based on the historical performance of the users. The results are extremely interesting, with a constant grow of the normalized reliability score[†] from campaign 3, after the activation of the e-learning platform (Figure 2: Normalized reliability score (users vs ambassadors). C-n are the phishing campaigns.):

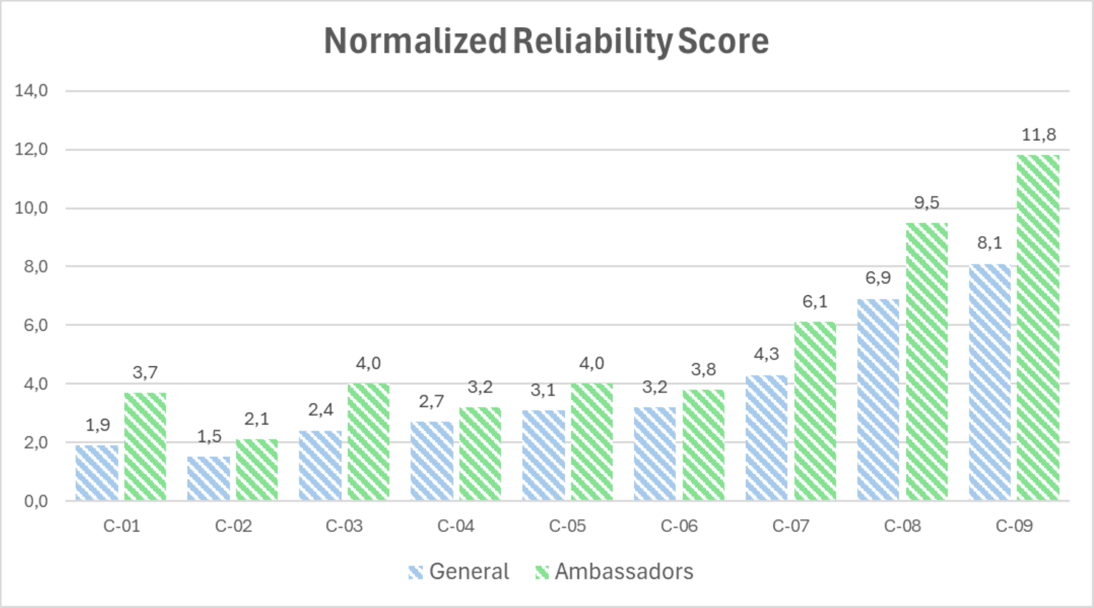
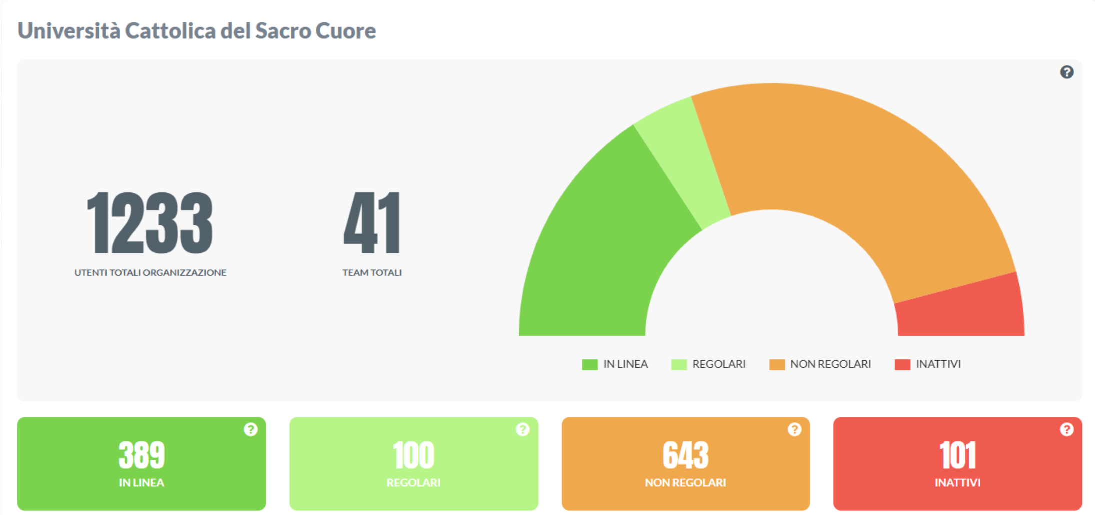


**Figure 2: Normalized reliability score (users vs ambassadors). C-n are the phishing campaigns.**

- Gamification: the1233 users (as of February 2025) are grouped in 41 teams, in competition with each other. Every team has a score based on the ability and the knowledge accumulated on the platform and measured via on-line tests and on the timeliness of course completion. Periodic reports with the first three teams classified and the position of the team of the specific user are distributed to all team members, fostering competition to improve the team's ranking.
- Web series: to increase the emotional impact of the knowledge acquired, the learning platform includes a web series with a docu-film approach with compelling storytelling. Each episode explores a lifelike situation and explains how to avoid or mitigate risk.
- Performance monitoring: a comprehensive dashboard empowers information security managers with precious insights about user engagement and security posture of UCSC. Specifically (see Figure 3: User engagement dashboard: the green users are following the training timely. The red ones are inactive.) we can see (as of February 2025) that 91,8% of the users are active on the platform following (more or less regularly) online lessons.

[†] Normalized Reliability Score (NRS) is a proprietary algorithm provided by the Cyberguru platform. It weights the difficulty level of the phishing campaign in order to evaluate the user and the user clusters. For example, a "strong user" is defined as a user who clicks on malicious links one phishing campaign every five (or less).



Università Cattolica del Sacro Cuore

1233 UTENTI TOTALI ORGANIZZAZIONE

41 TEAM TOTALI

389 IN LINEA

100 REGOLARI

643 NON REGOLARI

101 INATTIVI

**Figure 3: User engagement dashboard: the green users are following the training timely. The red ones are inactive.**

The continuous phishing campaigns, with new template emails, are a strong stimulus for reinforced learning and, together with the training materials, develop specific skills and abilities in dealing with phishing attacks and with incident escalation and reporting.

- **Targeted actions:** the insights gained from the platform triggered several critical targeted actions. In fact, some of the phishing campaigns showed a worrisome weakness in System Administrators and in Management clusters (Directors). The criticality of these two clusters is evident, leading to specific classroom-based training for the System Administrators. Since intensive in-presence training for the managers was not feasible, several fact-based meetings with the Directors were organized to discuss the evidence from the phishing campaigns. The subsequent campaigns showed an improvement in the reliability of both the clusters.

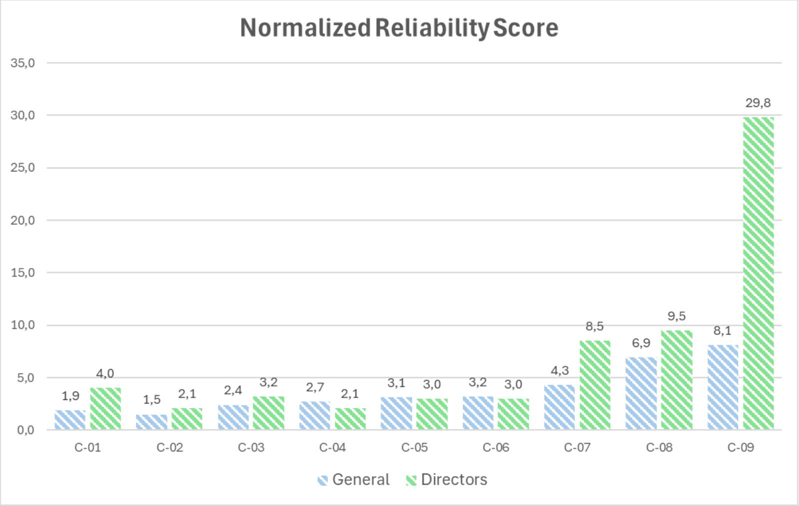


**Figure 4: Normalized reliability score (users vs Directors). C-n are the phishing campaigns.**

- **Passive communication and information radiators** (Agile Alliance, 2024)**:** another mean way to spread awareness is to use passive communication strategies. The use of cybersecurity infographics (two campaigns for year) as placemats in lunchrooms and the use of posters in common spaces (information radiators) allowed to improve the awareness of all users about "Minimum Security Measures" (password complexity, use of mobile device, Public wifi risks, etc).

# Mobile device

*You consider yourself an experienced user of mobile technologies. You have your own smartphone with which you navigate the Internet and use several apps to get updates for local services, weather, etc., and to find additional services, e.g., locating the best restaurant in the local area.*

BE AWARE.
CYBER SECURITY IS
A SHARED RESPONSIBILITY!

✓ Lock your device when not in use
✓ Connect only to secure Wi-Fi networks
✓ Scrutinize permission requests when using or installing applications

EDUCATIONAL CAMPAIGN POSTERS: KEEP UPDATING · TRAINING AND CULTURE · PRIVACY · LOCK YOUR DEVICE. ONE DAY ACTIVITIES. · MOBILE DEVICE

enisa
*European Union Agency for Network and Information Security*
*www.enisa.europa.eu | @ENISA_EU | #ENISA | #CyberSecMonth*
*For more information* ***info@enisa.europa.eu***

EDUCatt
Ente per il Diritto allo Studio Universitario dell'Università Cattolica

UNIVERSITÀ CATTOLICA del Sacro Cuore

**Figure 5: Lunchrooms placemats**

- **Emotional engagement:** during 2023 we started working on emotional engagement (EE). There are several studies underlying the importance of emotional engagement to increase cybersecurity (Wiederhold). We are aware that the topic needs a more structured approach but following the agile mindset we believed in the opportunity to experiment in a sort of MVP (Minimum Viable Product) on EE. In November 2023 we held a security incident and disaster recovery simulation involving the General Manager and all the manager-level staff. Simulating a life-like disaster situation, with the organization under attack by a treacherous group of cybercriminals, gave us a powerful chance to learn-by-doing with full emotional engagement of all the managers involved.

A few days later, we organized a workshop to speed up the adoption of the eLearning platform with a non-conventional format. The title of the workshop was: "CISO's coup d'etat". The narrative started with the C.I.S.O. announcing the impossibility of the C.I.O. to be physically present and announcing a video conference with him. Next, a deep fake of the C.I.O. started with a reasonable discussion about multi-factor authentication, escalating progressively towards an aberrant and paradoxical 5-factor authentication to prevent finger cutting or eyeball stealing. At the climax, the real C.I.O. entered the scene unmasking the C.I.S.O.'s attempt to impose absurd security rules. Unconventional as it is, the workshop had a strong emotional impact on the 800 plus participants and by word of mouth it rapidly spread to other employees, raising of 54% the number of "high fidelity users"[‡] and reducing by 14% the number of inactive users on the eLearning platform in the 3 weeks after the event.

Both events had a long tail of discussion and sharing of ideas, which was the desired outcome. This was a confirm that the hypothesis behind the intuition was valid: emotional engagement is a powerful tool in spreading awareness and in stimulating participation to other activities.

[‡] Users that completed all the prescribed training on-time.

Encouraged by the feedback, in October 2024 we experimented with a physical Cyber Escape room. We planned for around 100 administrative staff to be part of the experience; we ended up with 133 participants (and we closed the booking because we saturated the facility). The outcomes were promising: 94% of the participants declared that the experience had very interesting learning content and 97% rated the experience as highly engaging. In May 2025 we will launch for all the amin staff in UCSC the Cyber escape room in Virtual reality, together with our partner Coderblock. The platform is currently in beta testing phase and used as a learning tool in one master in UCSC. The teaser of the experience "VR Learning Experience - Escape Room" is available on YouTube: https://www.youtube.com/watch?v=T4ZvI4dhLN8 . The platform is currently being evolved to incorporate AI capability to empower NPC (Non playing Characters) with the ability to interact with the player.

Entrare nei vostri sistemi è stato molto facile_

CyberCat is under atta

**Figure 6: Cyber escape room in Virtual Reality**

To measure the results of the last three years of work on the human firewall competencies, in the second half of 2024 we assessed the digital competencies of administrative staff (886 respondents on 1213 submitted questionnaires). The results were encouraging. If the general assessment on digital competencies resulted in 64% of people with passing grades, the assessment on cybersecurity competencies scored 86% of passing grades.

It is worthwhile to underline that the effort described so far is deeply embedded in the Strategic Plan 2023-2025 of UCSC (Università Cattolica del Sacro Cuore).

The strategic plan ensures the financing, the top management commitment and the governance framework, three invaluable key success factors.

# 3 Rationalizing UCSC experience: the AwAKE approach

Our journey started from a weakness (limited number of IT professionals) which turned out to be a powerful stimulus to look for new and creative answers to our problems. We started with the "security ambassadors' community", later we discovered that the experience was successful but not easily scalable, so we activated a cyber-awareness and training platform, with eLearning pills, adaptive ethical phishing campaign and a web-series. At this point, thanks mainly to the dashboard provided by the solution, we discovered that we needed to address two urgent vulnerabilities: the System Administrators and the Managers. The last step moved us toward emotional engagement, to involve the "cold" employees and to reinforce learning for the others.
In a more or less conscious way, we worked on 4 pillars:

- **Aw**areness: the very first goal we set to ourselves was to create awareness in our colleagues and in our organization about the relevance of cybersecurity. This is in a way a leit motive in all that we did. Cyber-awareness is a kind of "mindfulness" that helps us to live in a complex and sometimes dangerous environment with the necessary level of alert.
- **A**bilities: the second goal was to equip our colleagues with a minimum set of abilities, such as how to deal with a phishing e-mail or with an incident response procedure. Abilities are more complex than skills (Indiana State University) and refer to "present demonstrable capacity to apply several knowledge and skills". Our goal, even before developing specific skills or knowledge, was to teach people how to act and react to threats.
- **K**nowledge: knowledge is of course important, but, counterintuitively, we focused our efforts on this pillar *after* we had the feeling that a minimum level of awareness and abilities were widespread. Of course, with a positive reinforcement cycle, more knowledge led to more awareness and abilities. We think that focus too much on knowledge in the early stages could be dangerous, and that more knowledge comes easy as soon as awareness and basic abilities are introduced in the community.
- **E**motional Engagement: the power of emotional engagement was apparent to us after the "CISO's coup d'etat" event. The +54% in high fidelity users and the -14% in the inactive users in the three weeks following the event were clearly correlated to the emotional engagement we were able to deliver. In the following months, the high-fidelity users tended to settle down a little, while the inactive users continued to decrease.
Aware of the importance of emotional involvement, two new experiences have been developed: a physical escape room carried out in October 2024 (European Cybersecurity Month; ENISA 2024) and a virtual reality escape room, currently ongoing.

We called the approach "Aw.A.K.E.", as a way to remind ourselves the enlightenment we experienced.

Of course, what we described is just the first part of the journey. We have several high priority tasks in front of us, linked to critical outcomes. Specifically:

- We need to continue focusing on managers and system administrators, since they are a powerful resource and a vulnerability as well. We will probably stress more the "emotional engagement" approach.
- We are engaging in the first cohort of instructors and researchers, and we will probably need to fine tune the approach and the tools we use.
- We are designing similar pathways for the students.

- We want to extend the use of information radiators: monitors in lunchrooms, cafeterias and libraries will show cyber-pills, transforming waiting moments (queues or administrative activities) into moments of awareness, in charge of Fondazione EDUCatt.
- Communication: a specific communication plan, on cybersecurity and digital innovation, is part of the Strategic Plan of UCSC 2023-2025 (Università Cattolica del Sacro Cuore). The plan is focused on administrative staff and faculties, but it addresses students as well.
- Collaboration: as mentioned before, UCSC security team co-worked with Fondazione EDUCatt and Gemelli Hospital (both parents company of UCSC) about passive communication strategies, and in close connection with CODAU Digital Transformation group about brainstorming and awareness technique improvement.

<

# 4 Conclusions

As described, our idea of cyber defense is based on a first line of resistance: people. This does not mean that we do not believe in tools, policies, procedures, standards and technical infrastructure. We are conscious that tools, policies, procedures, standards and technical infrastructure are foundational, and we are using a wide variety of them: from Security Performance Management to Endpoint Protection and Respond, from firewall to SOC, from SIEM to AI-powered Users and Entity Behavior Analytics tools, but we do believe that without people engagement even the strongest castle can easily fall. You do not need thousands of men to conquer it, it is enough one insider opening the gates…

The threats landscape is constantly changing, as clearly demonstrated by new AI-powered cyber-attacks. The security posture of any organization must constantly be re-evaluated and improved to keep up with the speed of change. In any case, we do believe that our Human Firewall, powered by tools, policies, procedures, standards and technical infrastructure, is probably the best investment we have made so far to increase our cyber-resilience.

# Bibliography

ACN – National Cybersecurity Agency. (2024). *Training and awareness*: https://www.acn.gov.it/portale/en/formazione-consapevolezza

Agile Alliance. (2024, February 29). *Information Radiators*. Retrieved from Agile Alliance: https://www.agilealliance.org/glossary/information-radiators/

AICA. (2021, May 21). *ICDL Security*. Retrieved from AICANET: https://www.aicanet.it/-/icdl-it-security-ecco-come-ottenere-la-certificazione

CybEE (2024). *Empowering the Human Firewall*: https://www.unicatt.it/cybee

Cyber Guru. (2024, February 25). *Cyber Guru Awareness*. Retrieved from Cyber Guru: https://www.cyberguru.it/en/cyber-guru-awareness-cyber-guru-for-cyber-security/#

Edegbeme-Beláz, A. (2020). THE HUMAN FIREWALL - the human side of cybersecurity. *ResearchGate*.

ENISA (2024). *European Cybersecurity Month*: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/european-cybersecurity-month

Greig, J. (2023, May 2). *Cybercrime groups find a new target: religious institutions*. Retrieved from The Record: https://therecord.media/cybercrime-groups-find-new-target-churches

IBM. (2022, 1 1). *IBM Cyber Security Intelligence Index Report.* IBM. Retrieved February 25, 2024, from www.aig.com.

Indiana State University. (n.d.). *What are KSA.* Retrieved from Indiana State University: https://www.indstate.edu/business/sites/business.indstate.edu/files/Docs/What-are-KSAs.pdf

Nature. (2024, February 7). Cyberattacks on knowledge institutions are increasing: what can be done? *Nature*, -. doi: https://doi.org/10.1038/d41586-024-00323-1

Università Cattolica del Sacro Cuore. (2024, February 29). *Piano Strategico 2023-2025.* Retrieved from UCSC: https://www.unicatt.it/uc/assicurazione-UCSC_Piano%20strategico%202023-2025.pdf

Verizon. (2023). *2023 Data Breach Investigations Report.* Verizon.

Wiederhold, B. K. (n.d.). Increasing Cybersecurity Through Emotional Engagement. *PUBMED*. doi:10.1089/cyber.2021.29224.editorial