Kymatio®

ACTIVATE YOUR HUMAN FIREWALLS

Risk management SaaS focused on the human factor, awareness and training against cyberattacks

White Paper

HUMAN CYBER RISK:

WHAT FACTORS SHOULD YOU MEASURE TO PROTECT YOUR ORGANIZATION?

www.kymatio.com

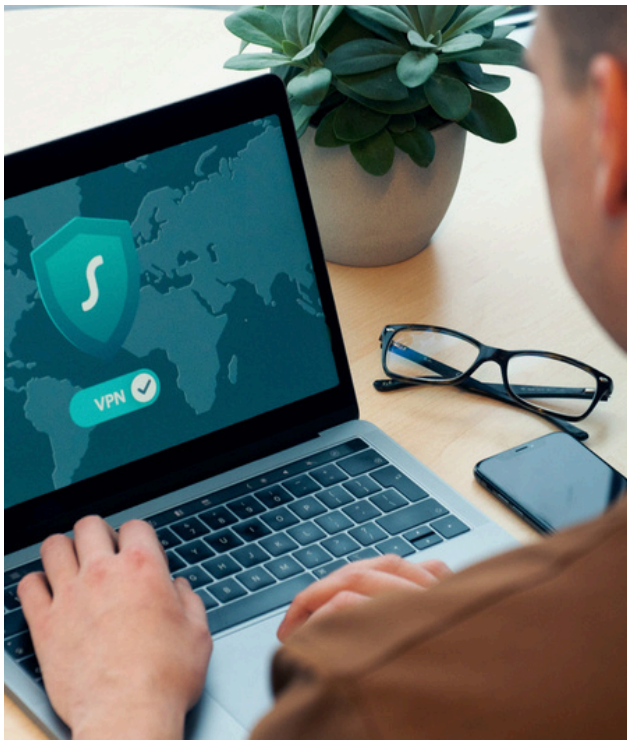
HUMAN CYBER RISK: WHAT FACTORS SHOULD YOU MEASURE TO PROTECT YOUR ORGANIZATION?

Information security is a key aspect for organizations. An incident can have serious consequences, both financially and legally. The average associated cost was $4.35 million in 2022, according to a report by the Ponemon Institute and IBM Security (2022), and for small and medium-sized businesses, it can even lead to the closure of the company.

Organizations are increasingly aware of the need to implement measures aimed at preventing these incidents, focusing their efforts on strengthening their cybersecurity posture.

Of course, there are basic solutions for protecting information from external attacks, such as installing firewalls and antivirus software that filter the data attempting to reach corporate devices.

Along these lines, there are many technological measures that can be implemented to prevent incidents, but to be truly protected, it is essential to pay attention to another factor: **humans.**



Behind every computer, mobile phone, tablet, etc., there is a human being. Like everything, no human being is infallible, so it's possible that actions may occur that lead to an incident. This is what is known as human cyber risk.

FACTORS BEHIND A HUMAN-INFECTED INCIDENT

There are many reasons why an incident of this nature can occur. However, each and every one of them has one thing in common: the disastrous consequences. That's why it's essential to understand what's behind it in order to address it before an incident occurs, managing this type of risk holistically rather than just partially.

LACK OF AWARENESS

The first reason is the most obvious of all: lack of awareness. Often, employees are unaware of their own importance in the organization's security. They may think this is an area that falls under the purview of information security or IT teams, overlooking the role each plays individually. Therefore, developing a cybersecurity culture within the organization is essential.

Other times, even if everyone is aware of the individual role they play in this area, the level of awareness regarding good or bad practices is not high enough. There are several issues to consider, including:

- **Communications: Sending information over the internet is something we do every day, in one way or another. In many cases, the data we wish to send is sensitive, whether personal (such as bank details when making an online purchase) or professional. Knowing how to do it securely is very important to avoid security incidents.**

- Compliance: While organizations typically have a dedicated team for legal tasks related to regulatory compliance, each employee has individual responsibility for the information they handle. However, not everyone is aware of this fact or what their role entails, so this is an area that requires strengthening.

- Data protection: Although many employees understand the importance of the information they handle, not everyone does. It may also be the case that, even though they know they should protect it, they don't know how to do so. Raising awareness about these issues is essential to maintaining security.

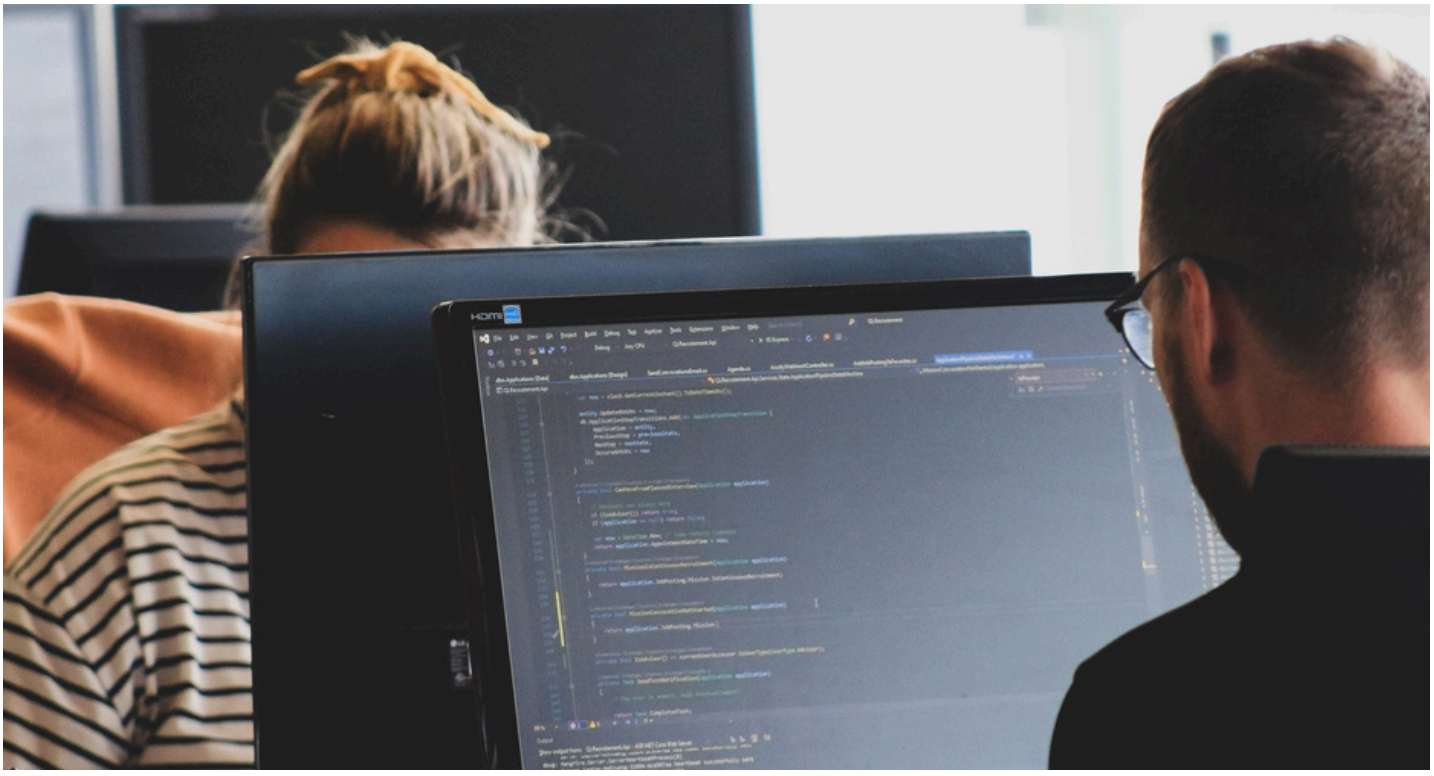
- Malware: One of the main dangers facing any internet user is the proliferation of malicious software. While antivirus and firewalls are capable of filtering out a large number of malicious software, this isn't always possible, among other reasons because, like these defense programs, cybercriminals also update themselves. That's why it's important for employees to know the types of malware they might encounter and how their devices could be infected.

- **Password management: All of our devices and accounts are protected by a password. This is the key to accessing all of our information and the various features we use at our own risk. For this reason, knowing the best practices for protecting our accounts and devices is essential.**

- **Social engineering: This is one of the main attack methods used by cybercriminals today due to its high effectiveness. Hacking people has proven, in many cases, to be more effective than hacking computers and other devices, so it is essential to educate employees about the existence of this practice and the different forms it can take.**

- **Workplace Security: Information security cannot be conceived in isolation, without considering the environment where information-related activities are carried out. Whether in the office, at home, or anywhere else, knowing how to act in each location is something all employees must internalize.**

Maintaining a healthy state of alert is essential to protecting the information we handle, and to do so, it's necessary to address all of these topics not only theoretically but also practically, so that the knowledge acquired can be put into practice.



WELLBEING

Of course, without awareness, there remains a huge gap to fill in order to prevent cybercriminals from entering the scene and prevent errors. However, this isn't the only factor to consider.

The next point to address is one that has traditionally been assigned to the Human Resources department: employee well-being. And while it's true that this area of the organization is the most involved, it also directly affects Information Security.

It's obvious that the well-being of all employees in an organization should be a top priority for management simply because they are people; however, maintaining safety is yet another reason to add to the list.

This close relationship exists for several reasons. For an employee who is dissatisfied with their organization, their interest in what might happen there beyond what directly affects them is diminished. Most likely, their thoughts aren't focused on information security, but rather on the deadlines they have to meet and the lack of time to do so, the pressure they receive from their managers, or any other aspect that is causing this discomfort. This increases the likelihood of negligence resulting in an incident. At the same time, the likelihood of intentional incidents also increases, a possibility we shouldn't ignore.

Burnout syndrome deserves special mention. Recognized by the World Health Organization (WHO) as an occupational disease, it consists of three dimensions: emotional exhaustion, depersonalization, and a low perception of self-realization (Maslach and Jackson, 1981). According to the WHO (1994):

> Physical burnout is evidenced by lack of energy, chronic fatigue, weakness, tiredness, increased susceptibility to illness, frequent headaches, nausea, muscle tension, backaches, various somatic complaints, and sleep disturbances. Emotional burnout can involve feelings of depression, helplessness, hopelessness, increased tension and conflict at home, increased negative affective states (e.g., anger, impatience, and irritability), and decreased positive states (e.g., kindness, consideration, courtesy).
>
> Burnout can involve dissatisfaction and negative attitudes toward oneself, one's job, and life in general. Finally, an increase in work withdrawal behaviors (e.g., absenteeism and turnover) has also been observed. (p. 1)

In a 2021 study conducted by Global Web Index and Asana with more than 10,500 participants from seven countries, it was found that 67% of employees at medium-sized organizations and 53% at small businesses had experienced burnout. There's no shortage of reasons to say that these figures are, to say the least, alarming.

Working on avoiding this syndrome and on the general well-being of employees will not only make the work environment a happier place for everyone, but will also bring about an increase in productivity (Wright and Cropanzano, 1997, 2000), a reduction in turnover and its associated costs (Wright and Bonett, 2007; Cascio, 2003 in Page and Vella-Brodrick, 2009) and, what concerns us in this document, a decrease in the probability of information security incidents.

INDIVIDUAL DIFFERENCES

Closely related to the previous point is the third factor to consider: the differences each employee has at an individual level. These differences go beyond knowledge of regulations and protocols; they have to do with our way of being and how we relate to the world around us.

Two people can react completely differently to the same situation. Therefore, it can be deduced that their relationship with cybersecurity also differs.

Our personality largely determines how we act in different environments. For example, some people trust others very easily, while others are more reserved and take longer to open up. Another example would be the emotionality each person brings to each situation: some people are able to remain calm even in extremely adverse situations, while others are more prone to feeling stress, anger, and other emotions easily (Costa and McCrae, 1985).

At first glance, this may not seem very related to information security, but nothing could be further from the truth. Those people who tend to trust others might share information or engage in bad practices (such as sharing passwords) because they think their interlocutor doesn't have bad intentions. Similarly, a relaxed person, who tends to view life from a more relaxed and relaxed perspective, might not give security the importance it deserves, paying little attention and having thoughts like "this won't happen to me" or "these procedures are excessive." At the other end of the continuum, we find people who get stressed easily. In these cases, when there is a heavy workload, it is common to prioritize completing tasks over security, and this stress can also facilitate errors that lead to an incident.

Each person has their own predispositions, and knowing what they are will allow them to pay attention to aspects that would otherwise go unnoticed.

This is especially relevant when we talk about social engineering. People's motivations vary, and while some are driven by the pursuit of benefits, others are driven by the avoidance of negative consequences (Gray, 1981). Thus, we may correctly detect one type of attack but not others. Knowing where we may be most vulnerable is very important to remain alert at all times.

HOW TO INTEGRATE THIS INTO A RISK MANAGEMENT PROGRAM?

Having put all these relevant factors on the table, it is clear that the current approach to risk management is not sufficient.

First, it is necessary to integrate the human element into it and go beyond the technological solutions that, until now, have been considered sufficient.

Of course, more and more organizations are choosing to go a step further and introduce awareness programs into their security master plan. However, these programs often fall short of the real needs for truly effective workforce empowerment.

In most cases, this is due to the approach to awareness. Typically, long annual or semiannual courses are offered to all employees equally. Due to their nature, they become tedious and ineffective, not to mention that they only cover the first point discussed in this document.

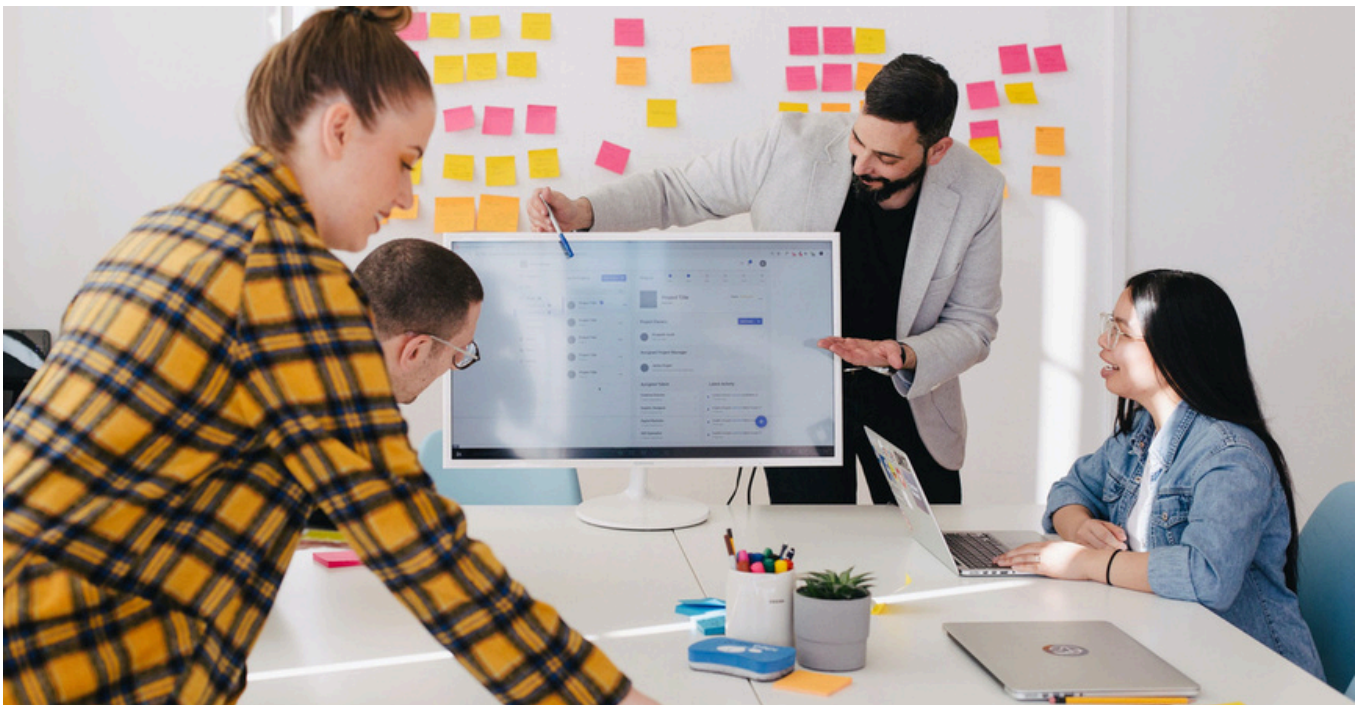
To successfully manage risk associated with the human factor, all the aspects explained above must be considered holistically, something that is often not the case. Good management involves the following points:

- **Periodic awareness raising through theoretical sessions in the different areas of information security.**

- Put this knowledge into practice through attack simulations that allow you to see how employees would behave in a real-life scenario.

- **Obtaining metrics. One of the major problems with current awareness is that there is no data available to determine whether it is having the desired effect or not. Having metrics that provide this information will allow us not only to track the evolution of the risk, but also to adjust strategies as needed.**

- **Measuring employee well-being. As explained above, well-being is not separate from safety; quite the opposite. Knowing how employees are feeling and working to improve this aspect will have a very positive impact on both the workforce and the organization.**



- **Personalize the experience and awareness program to each individual's needs. This will require an automated tool, so there's no need to invest excessive time in developing different personalized itineraries.**

- **Make it fun. To encourage employees to participate and take advantage of all the program has to offer, it's necessary to introduce a gamification component.**

While these points are a brief summary of the issues to consider, in this whitepaper we explain in more detail why current awareness approaches don't work and what the best approach is.

CONCLUSION

Managing risk associated with the human factor remains one of the main challenges for organizations. Unless it is addressed comprehensively, as is currently the case, they will be doomed to continue to expose themselves and, in the most unfortunate cases, suffer security incidents.

It's clear that this isn't an easy task for security teams. It's a complex and, as a result, time-consuming task. That's why it's necessary to have a tool that automates this process to go one step further in protecting organizations' information.

ABOUT KYMATIO®

Kymatio® is a SaaS solution that automates employee awareness and alertness assessment in an unattended and personalized manner, while providing a human-related risk management tool with metrics, time-based evolution, and action plans.

Using neuropsychology and cybersecurity as the foundation of its technology, Kymatio® AI interacts with people, offering personalized awareness tailored to their needs, maintaining their alertness, and strengthening areas where they may be most vulnerable.

This awareness program offers awareness pills that strengthen employees in the areas they truly need, including multimedia content that helps with content retention. This is achieved through periodic evaluations that employees complete while interacting with the platform.

At the same time, it provides organizations with real-time visibility into human risk based on various metrics such as awareness level, roles and access to information, well-being level, response to phishing attack simulations, and monitoring of employee credentials exposure online.

To learn more, contact us at contact@kymatio.com or schedule a meeting

ABOUT THE AUTHOR

ANDREA ZAMORANO

Cyberpsychology Manager at Kymatio®, she researches the human side of cybersecurity and develops the algorithms necessary for the platform to accurately measure the factors involved, allowing it to assess risk and present personalized recommendations based on each individual's needs. She also teaches at the UAM School of Economic Intelligence (La_SEI) as an expert in indirect personality profiling. She is a psychologist by training, having studied at the Autonomous University of Madrid, and subsequently graduated from the Master's in Economic Intelligence and International Relations from La_SEI. She also holds a degree in Organization and Human Resources from the Autonomous University of Madrid.

LITERATURE

Cascio, W. F. (2003). Managing human resource: Productivity, quality of work life, profits. New York: McGraw-Hill.

Costa, P. T., & McCrae, R. R. (1985). The NEO personality inventory. Odessa, FL: Psychological Assessment Resources.

Global Web Index, Asana (2021). ANATOMY OF WORK SPECIAL REPORT: Keeping employees engaged in a burned-out world. Recuperado de: https://asana.com/es/resources/anatomy-of-work-summary

Gray, J. A. (1981). A critique of Eysenck's theory of personality. In Eysenck H. J., A model for personality (pp. 246-276). Springer, Berlin, Heidelberg.

Maslach, C., & Jackson, S. E. (1981). The measurement of experienced burnout. Journal of organizational behavior, 2(2), 99-113.

Page, K. M., & Vella-Brodrick, D. A. (2009). The 'what','why'and 'how'of employee well-being: A new model. Social indicators research, 90, 441-458.

Ponemon Institute, IBM Security (2022). 2022 Cost of a Data Breach Report. Retrieved from: https://www.ibm.com/es-es/reports/data-breach

World Health Organization. (1994). Guidelines for the primary prevention of mental, neurological and psychosocial disorders. 5. Staff burnout (No. WHO/MNH/MND/94.21. Unpublished). World Health Organization.

Wright, T. A., & Bonett, D. G. (2007). Job satisfaction and psychological well-being as nonadditive predictors of workplace turnover. Journal of Management, 33, 141–160.

Wright, T. A., & Cropanzano, R. (1997, August). WELL-BEING, SATISFACTION AND JOB PERFORMANCE: ANOTHER LOOK AT THE HAPPY/PRODUCTIVE WORKER THESIS. In Academy of Management Proceedings (Vol. 1997, No. 1, pp. 364-368). Briarcliff Manor, NY 10510: Academy of Management.

Wright, T. A., & Cropanzano, R. (2000). Psychological well-being and job satisfaction as predictors of job performance. Journal of Occupational Health Psychology, 5, 84–94.