Building a Human Firewall

The growing use and dependency on technology is a steadily increasing trend. Digitalization is not only changing our everyday life and the way we conduct business, but also the way criminals and nation states go about. Crime is turning into cybercrime and warfare is becoming cyber warfare. This IT-revolution brings many advantages, but also leads to the emergence of new cyber risks. As a result, the threat landscape is changing rapidly, forcing organizations to act and ensure that they are resilient to changes.

The economic costs of cyber-attacks and breaches are extremely high and can lead to both financial damage and considerable reputational damage. In 2019, the annual growth of ransomware attacks amounted to 363%[1] and the total cost of ransomware was estimated at $11.5 billion[2]. For a single data breach, organizations can expect an average cost of $3.9 million[3]. Hence, many organizations are enhancing their cyber resilience capabilities. A great deal of attention is devoted to improving existing security infrastructure via technical solutions such as firewalls and intrusion detection systems. Frequently, however, the human firewall is neglected when protecting organizations against cyber attacks. Most organizations leave cybersecurity responsibilities to their security function and IT department. As a consequence, cybersecurity measures are often designed and implemented with a strong focus on technology and not necessarily in harmony with other business responsibilities such as HR. As a result, a culture of security awareness is lacking in most organizations.

In the current COVID-19 crisis, organizations are increasingly facing challenges in light of new cybersecurity threats that have arisen in the course of this crisis. Organizations are dealing with high reliance on technology, remote working, a high level of uncertainty and deviations in processes as compared to the previous 'business as usual'. This change in 'business as usual' also brings with it a shift in necessary security precautions. Remote working and the use of new technologies present new challenges on the security level. Now more than ever, organizations should strive for the facilitation of the interaction between people, processes and technologies. A set of values in the form of a secure culture program, which allows for the integration of technology and human aspects should be a cornerstone of corporate cybersecurity strategies.

This article highlights the role of human behavior in cybersecurity, followed by a reflection about how to build a 'human firewall' including a quick checklist about working remotely in the face of COVID-19, closing with an outline about how PwC can support in building a secure culture.

The role of human behavior in cybersecurity

Recently, COVID-19 has shed new light on human behavior in cybersecurity. There has been a 667% increase[4] in spear-phishing e-mail attacks related to COVID-19 since the end of February alone. Malicious actors have employed specialized phishing campaigns that prey upon collective fear and misinformation regarding the virus. For example, fraudsters sent E-mails that seemingly originated from legitimate sources with information about the virus. However, the E-mails actually contained embedded links or attachments that enabled the installation of malicious software on the target's device. The damage caused by such malware attacks is severe, especially in times of crisis, as availability of systems is crucial.

Moreover, organizations are increasingly faced with the challenge of adapting their business processes to the crisis. Most importantly, employees are asked to perform their work remotely. This has a significant impact on cybersecurity, as confidential information is now handled within the private space of the employee rather than a controlled office environment. In such conditions, the risks of weak WiFi security, phishing attacks, insecure passwords and insufficient patch management increases. Thus, the security awareness of employees working remotely is paramount.

1 2019 state of malware (Malwarebytes, 2019)
2 Morgan, S., Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021 (Cybercrime magazine, 2018)
3 Cost of a Data Breach Report (IBM, 2019)
4 Boosting cybersecurity immunity: Confronting cybersecurity risks in today's work-from-home world (Cap gemini Research Insitute, 2020)

In addition, attackers make use of the crisis by specifically targeting organizations that play a crucial role in the mitigation of the crisis. For example, cybercriminals focused their efforts on harming hospitals that are responsible for treating COVID-19 patients. The attackers managed to encrypt patient data and demanded high ransoms for decryption of the highly sensitive data. Security awareness is crucial for mitigating such risks, since ransomware attacks are often (partially) enabled by human error.

However, this is not a new trend. Already for years, hackers have exploited the vulnerabilities of human behavior in reaching their target. In 2018, the cinema chain Pathé lost roughly 19 million euros[5] after being targeted by CEO fraud. The attack was executed with a business email compromise scam. In such a scam, the target receives a seemingly legitimate E-mail from a colleague, which is actually sent by a malicious actor to attain sensitive information or financial gains. In this case, the attackers impersonated the board of the French Headquarters, asking Dutch Board members to transfer funds for a highly confidential takeover. The Dutch board members wired the funds to the attackers, causing severe financial damage to the organization.

In July 2015 the Pentagon suffered from a cyber-attack which affected 4000 military and civilian personnel. The attack was conducted by Russian hackers who used automated social engineering techniques to gain information from employees' social media accounts and then used that information to conduct a spear phishing attack. The attack was not comprised of a phishing attack in the form of an old typo-ridden email, but a highly sophisticated phishing attack which appeared to be an authentic message. The attackers created Twitter accounts operated by robots, which invited users to click on malicious links that were attached to posts. The posts contained promotions for family-friendly vacation packages for the summer. Due to human negligence or simple errors, many people fell victim. This attack showed that attackers constantly find new ways of working. While organizations often train their employees on caution related to opening email attachments, attackers are quick to find new measures to successfully conduct attacks[6] . This example shows that attacks change frequently and that an up-to-date secure culture is inevitable for organizations.

Similarly, a large-scale data breach at Yahoo was caused through targeting human error in 2014 already. The Russian state security service gained access to Yahoo's network, and most likely the information and emails from 500 million people. Through sending out a spear-phishing email the attackers targeted several people, and upon the first click, the data breach occurred. The attackers installed a backdoor in order to retain access to the user database and extract it from Yahoo's network[7].

> **Already for years, hackers have exploited the vulnerabilities of human behavior in reaching their target.**

As the examples show, cyberattacks have been occurring for years already, but ways they are conducted are continuously evolving over time. Although cyber-attacks occur for a multitude of reasons, the human factor in the escalation or success of an attack has surged. A report by Shred-it confirms that 47% of today's data breaches are caused by human error[8]. Organizations are slowly starting to wake up to the fact that one of the biggest vulnerabilities in their armor against cyberattacks is their own employees. Hence, it goes without saying that next to focusing cybersecurity programs on designing better technologies, a major aspect of security – the human factor – is being neglected.

Security technologies such as firewalls help protect data assets and computer systems against unauthorized entry. However, through social engineering techniques, malicious attackers are able to breach organizational security via human interactions[9]. Although almost every attack is computer-related, people still control computers and are therefore ultimately accountable. While most organizations invest in the latest security software to protect themselves, they fail to realize that cybersecurity is not only about technology. The majority of data breaches within organization are in fact the result of human actors. The reason why human actors are often responsible for the success of cyberattacks is multifold. First and foremost, people do not take personal accountability for security. People tend to remove themselves from the risk rather than admitting to it. Mostly, this negligence is owed to a combination of security fatigue and a lack of awareness. Owing to this, most security awareness trainings are not effective. After people attend a training session, 50% of the information is usually forgotten within an hour[10] . This is mainly due to the fact that basic awareness training exercises neither engage employees nor instill a security mindset. In other words, there is a lack of integration between security awareness trainings and people's day to day tasks. Awareness without understanding the impact and relevance is dangerous as it can create a culture of risk seeking. Hence, applicability is necessary for an effective retention of the knowledge.

5 'Ceo-fraude' kost Pathé ruim 19 miljoen euro (Accountant, 2018)
6 Frenkel, S., Hackers Hide Cyberattacks in Social Media Posts (New York Times, 2017)
7 Williams, M., Inside the Russian hack of Yahoo: How they did it (CSO, 2017)
8 Data Protection Report (Shred-it, 2019)
9 Ghafir, I., Saleem, J. et al., Security threats to critical infrastructure: the human factor (Springer, 2018)
10 Kohn, A., Brain Science: The forgetting curve – the dirty secret of corporate training (LearningSolutions, 2014)

A paradigm shift concerning the ecosystem of cybersecurity is necessary. The classical technical focus of cybersecurity does not pay sufficient attention to the semantics of the interaction between people and information technology. In essence, an overarching framework of thinking and acting upon security awareness is lacking in most organizations. They should however realize that cybersecurity is a responsibility of all employees, as in the end, an organization is only as strong as its weakest link.

Building a human firewall

Culture extends beyond awareness. In order to build a secure culture, the unique culture of an organization must be understood by looking at the overall culture(s), strategies and policies within the organization. A mutual understanding between senior management, cybersecurity professionals and employees with roles and responsibilities related to defending cybercrime is undeniably required[11]. Even though senior management sets the tone, a secure culture must be formed with employees rather than being imposed upon them. Senior management is merely responsible for investment decisions, and for modeling the roles related to secure culture within the organization. Forming and implementation on the other hand is an organization-wide task.

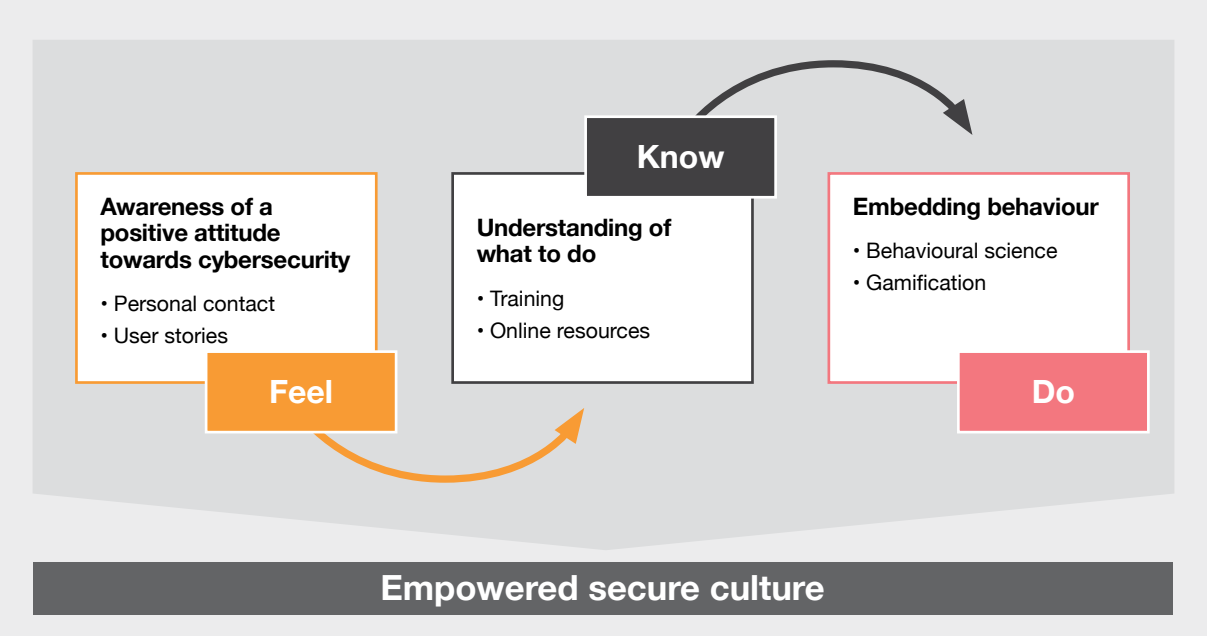
The different stages of achieving a secure culture are threefold. As outlined in figure 1 it is essential to first establish a feeling of secure culture in order to create awareness and a positive attitude towards cybersecurity in general. Through sharing user stories of data breaches, and protecting of sensitive data, employees' awareness to the importance of cybersecurity is facilitated. Next to standard security awareness trainings, specialized secure culture programs should be set up that take into account the new developments in the area of secure culture. Finally, through engaging employees, the knowledge will remain present in their minds. Gamification measures are very popular here, as they engage participants and therefore usually increase motivation and learning outcomes[12].

Home office security checklist

During the COVID-19 crisis, many organizations have implemented a home working strategy. This checklist helps end-users to improve the resilience of their home office.

1. Be wary of **unusual, unexpected or urgent requests** by phone, email or text message
2. Only enter your **credentials** on trusted, verified websites
3. Update your software and devices promptly
4. Pay special attention to the **security of your router**
5. Use **strong and unique passwords** or a **password manager**
6. Don't let the people you live with use your **work devices**

Figure 1 – Stages of achieving an embedded cybersecurity culture



11 Cyber security culture in organisations (European Union Agency for Network and Information Security, 2017)
12 Giertsen, E. G. B., Bartnes, M. et al., Gamification of information security awareness and training (Researchgate, 2017)

Leadership action

- Tone from the top
- Role modelling
- Consistency and cohesiveness of leadership

People practises

- On boarding
- Promotions
- Training and development

Organisational structure

- Geography
- Roles and Responsibilities
- Policies and controls

Communication

- Two way communication
- Escalation and resolution channels
- Symbols and stories

Performance management and reward

- Performance measures
- Consequence management
- Recognation schemes

External environment

- Regulation
- Customer management
- Third party vendors and service providers

The outcome of these three steps is an empowered secure culture. Instead of attaining security awareness, the steps, when tailored to organizational needs and implemented appropriately, allow secure culture to become part of the corporate culture within organizations.

Developing a strong secure culture is not a one-off activity, but is rather an ongoing process which needs to be continuously nurtured if it is to become embedded within the wider organization's culture[13]. A cybersecurity culture should involve employees from all levels: ranging from senior management to the IT department to human resources. In order to maximize efficiency, a secure culture should be an iterative process which is continuously nurtured and eventually embedded within the wider organization's culture.

When designing a roadmap in order to bring an organization's secure culture level to a higher maturity, the key behavioural reinforces should be understood in order to determine implementation actions. Those key behavioural reinforcers are factors impacting the employee's attitude and behavior towards security. When understanding the reinforcers, specific actions can be defined. Below the six key behavioral reinforcers are given, including a subset of impacting factors.

> Essentially, organizations should opt for a holistic approach to change, integrating all parts of organizational culture when undergoing a secure culture change.

A secure culture transformation is complex and requires a change in values and beliefs, an alteration in behavior, and a reshaping of the underlying assumptions regarding cybersecurity. However, achieving a culture change takes time: it may take 6-12 months to gain momentum and another 2 years or more before you reach a stage of comfortable maturity and continuous improvement[14]. In order to keep track of the progress of a secure culture program, tangible metrics must be set up for assessment. Although it is challenging to measure culture, metrics concerning the number of unlocked desktops, phishing reports and lost PCs for example, allow for insight and a measurement of the effectiveness of the inherent secure culture within an organization.

When integrating a secure culture into an organization, a change in organizational culture is taking place. It is widely believed that secure culture is a technical issue. In reality however, secure culture is a leadership issue and should be treated as a cultural change. More so, a change in secure culture should be integrated into organizational culture. According to a survey on culture and change management by the Katzenbach Center, only around half of organizational transformation initiatives accomplish and sustain their goals[15]. Experience has shown that a lack of alignment between organizational culture and intended secure culture is often the main reason for failure. Implementing tight secure culture measures in an otherwise loosely controlled organization will most likely not lead to a successful outcome[16]. Essentially, organizations should opt for a holistic approach to change, integrating all parts of organizational culture when undergoing a secure culture change.

13 Cyber security culture in organisations (European Union Agency for Network and Information Security, 2017)
14 Cyber security culture in organisations (European Union Agency for Network and Information Security, 2017)
15 Aguirre, D., von Post, R. & Alpern, M., Culture's role in enabling organizational change (Strategy&, 2013)
16 Ruighaver, A. B. & Maynard, S. B., Organizational Security Culture: More than just an End-User Phenomenon (Springer, 2006)

Even though secure culture is still a developing concept, it has been successfully implemented at many organizations. At Uber for instance, specific secure culture programs are catered to regional, departmental and cultural differences. Owing to the rather young workforce at Uber, the organization has focused on gamification, competition and incentives to encourage participation in its secure culture program. Furthermore, Uber demonstrates a good example of a holistic approach to secure culture. The organization incorporated security into its corporate culture from the start, making it a core part of the company's mission[17]. At SAP a secure culture is also instilled. Next to mandatory trainings sessions, gamification is very popular at SAP. By means of a virtual escape room, employees have to solve security puzzles. Likewise, hacking competitions are organized with the goal of sharing knowledge and strengthening awareness[18]. Furthermore, Adobe has created a secure culture which touches almost every area of the company. Starting with regular security awareness training and activities for all employees, certain job functions receive additional function-specific security training and certification.

Adobe's integration of gamification, bug identifying competitions, and presentations on security issues allows for diversification of its secure culture program. This holistic approach to security at Adobe ensures a proactive prevention of security issues from affecting Adobe's customers and the company itself[19] .

A secure culture encompasses information security frameworks and cybersecurity awareness. It is broader in both application and scope, whilst being concerned with making security an integral part of employees' jobs and conduct. In essence, the established cybersecurity culture should be integrated seamlessly with people's work, and shape the security thinking of all staff, improving resilience against cyber threats. In the end, an established secure culture will make employees the strongest link instead of the weakest link and will serve as a human firewall.

17 David, M., How Uber used mobile performance engineering to pull ahead (TechBeacon, 2018)
18 Gustaffson, E., We need to create a secure culture (The Cloud Report)
19 Arkin, B., Nurturing Security Culture at Adobe (Adobe, 2018)

The PwC Netherlands Secure Culture team

Bram van Tiel
Partner, PwC Netherlands
T: +31 (0)6 224 329 62
E: bram.van.tiel@pwc.com

Sanne Amber Maas
Manager, PwC Netherlands
T: +31 (0)6 221 443 58
E: sanne.amber.maas@pwc.com

Julia Burghartz
Senior Associate, PwC Netherlands
T: +31 (0)6 824 972 10
E: julia.burghartz@pwc.com

How PwC can help

As every organization has different needs and requirements to ensure a cybersecurity culture, a thoroughly tailored program should be opted for. Differently to traditional security awareness techniques, PwC is highly experienced in setting up engaging programs in the field of secure culture. Owing to the cross-disciplinary expertise in our team ranging from information security to applied psychology, we are able to address secure culture from a wide angle.

As clients may choose a variety of activities tailored to their needs, a full security culture change can be achieved, targeting stakeholders both inside and outside of the organization. The program can include an appropriate variety of activities ranging from vulnerability assessments to crisis simulations. The program will be tailored to the organization's needs, allocated budget, number of employees and specific departmental needs. PwC's approach to building a secure culture program is made up of four key steps which are demonstrated in figures 2 and 3.

Due to varying organizational needs, the specific roadmap differs per organization. Some organizations prefer to initiate their secure culture program with a few smaller interventions, whereas other organizations wish to pursue an intense and detailed program. Ideally, organizations improve their secure culture by allowing for an iterative approach. After having conducted several interventions, it is recommended to evaluate and determine the next steps which are needed for a continuous increase in secure culture. The end result is a framework of true value which empowers individuals to place organizational security at the forefront of their day-to-day activities.

Figure 2 – PwC's secure culture process

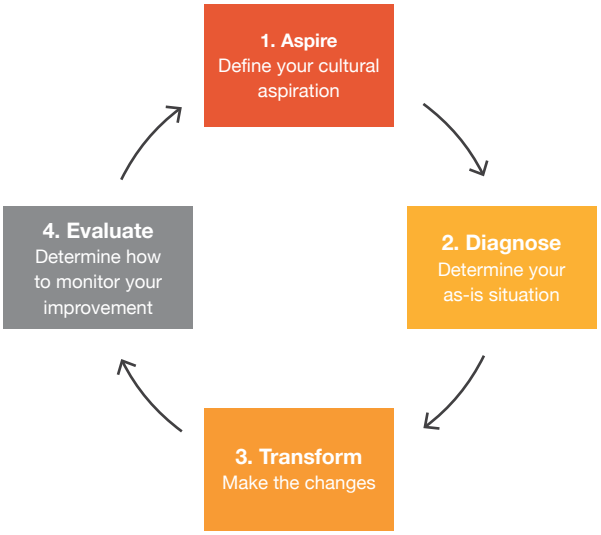


Figure 3 – PwC's Secure culture roadmap