adnovum

Stay safe with a healthy cybersecurity culture

How to reduce the risk of a cyber attack in your organization to a minimum

The risk has never been greater: more than 60% of all businesses do not survive a cyber attack.

Contents

An introduction to cybersecurity

Today, most organizations need information systems to survive and prosper. Within this realm, information has become a valuable asset. It is therefore imperative for modern organizations to take the protection of their information resources and data seriously. The protection of these resources – also known as information security – consists of many processes which will be detailed in this ebook.

The threat is real

When it comes to cybersecurity, the size, industry, number of assets, or employees of your business or company does not matter. In today's world, approx. 60% of small companies and startups go out of business within six months following some form of cyber attack. A single security breach can cost a company up to 180'000 CHF. The chances of your business suffering a cyber attack are higher than ever. Experts reveal that hackers attack on average 2'224 times on a single day. In other words: Every 39 seconds, a cybersecurity attack is launched. At the same time, hackers and cyber attacks have become more sophisticated and prevalent. With employees worldwide working remotely rather than in the office, the risks of data breaches have increased significantly. According to the FBI, cyber attacks have gone up by 400% during the COVID-19 pandemic alone. But that is not all!

With the increased use of new technologies, such as advanced software applications, cloud computing, and Internet of Things (IoT) devices, cybersecurity has become a major concern for organizations of all sizes and types. Due to these technological advancements, organizations have set up a large attack surface that opens the door for potential cyber attacks.

Key take-away

The chances of your business suffering a cyber attack are higher than ever. Every 39 seconds, a cybersecurity attack is launched.

A cybersecurity culture is essential

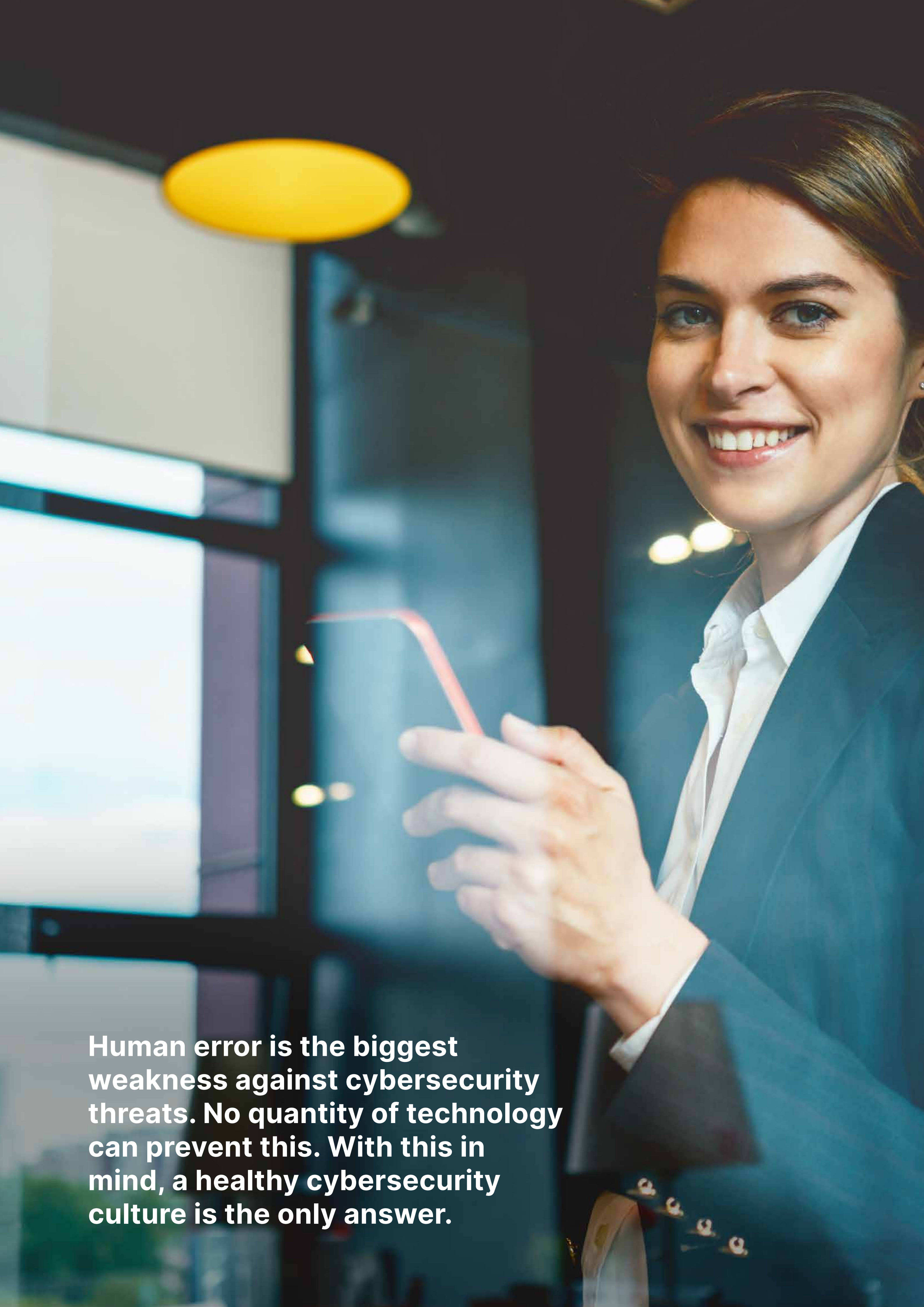
The numbers show it clearly: surviving in today's cyberspace is a huge challenge for both users and businesses across the globe. While the past year brought upon the pandemic of COVID-19, it also opened the door for a barrage of security threats that most of the world was not prepared for. Bruce Schneier makes it clear with the following statement: «If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.»

Because no quantity of technology can appropriately make reparation for the incorrect mindset and knowledge about securing an organization's assets. People are key. No question.

Studies show that an unprepared workforce can actually expose a company to a wide range of digital threats and ultimately cost hundreds of thousands of Swiss Francs to the organization in recovery costs. Regardless of how effective or cutting-edge your security defensive measures may be, if your employees are uneducated regarding the latest cybersecurity threats, chances are that sooner or later one of your employees may mistakenly download malware into the organization's systems or be tricked by other malicious scams of the hackers. Businesses that invest heavily in cybersecurity often have their investments in technology. But they do not adequately consider the human side of it, due to which organizations face potential cybersecurity risks.

Implementing a healthy cybersecurity culture in a workplace plays a vital role in the entire organization's security posture. In realization of this, organizations are putting more effort into implementing a cyber secure environment. They aim to encourage a cyber-secure culture among employees because protection from cyber attacks can only be attained with a coordinated effort. Cybersecurity culture in an organization promotes better security practices which integrate seamlessly with the employees' work. It helps them be aware of cyber threats and encourages them to change their behavior accordingly to mitigate potential risks.

Read further to find out how establishing a cybersecurity culture in your organization helps reducing the risk of suffering from a cyber attack.

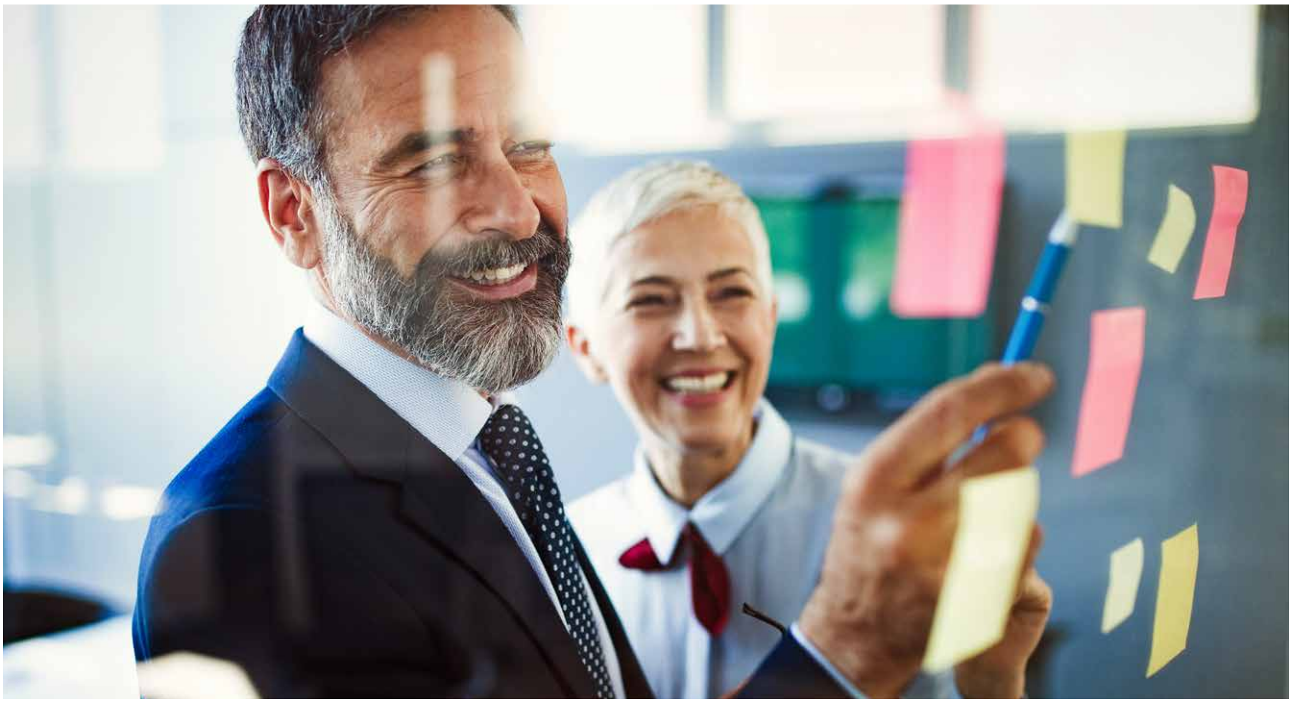


Human error is the biggest weakness against cybersecurity threats. No quantity of technology can prevent this. With this in mind, a healthy cybersecurity culture is the only answer.

Essentials of cyber-security culture

Cybersecurity in an organization is more than enforcing policies without proper explanation and notifying employees they need to change passwords regularly. Organizations need to focus on building their cybersecurity culture.

It includes policies incorporating seamlessly with the employees working routines and practices, spending more time raising awareness, and showing them how their actions can affect the entire organization's structure.



Cybersecurity culture refers to the beliefs, knowledge, perceptions, assumptions, attitudes, values, and norms of people regarding cybersecurity and how they exhibit themselves in people's actions with information technologies. Cybersecurity culture encompasses familiar topics, including information security frameworks and cybersecurity awareness, broader in application and scope.

Cybersecurity culture is unique for each organization and not applicable for others due to its specific characteristics in terms of processes, technologies, and people's value. It has to be considered an integral part of an organizational culture. It strengthens the culture adherence with organizations and makes people realize that security is not an IT department issue, but a mission for the entire organization.

A complex structure on many levels

To improve your cybersecurity culture, it is essential to understand the elements that bring it alive and either support or hinder your organization's efforts to strengthen the resilience against cyber threats. To understand the different aspects of a cybersecurity culture, it is a good start to look at the elements of organizational culture, as «cybersecurity culture» can be seen as a subculture of the «corporate culture». The most tangible way of explaining «culture» is the popular expression: «the way we do things around here» (Schein, 1999). This expression covers an integral part of a culture: the directly visible artifacts like existing organizational structures, processes, or your organization's written security policy. But while this saying expresses an essential part of a culture, it is also a simplification and misses other crucial elements.

Cybersecurity is more than simply enforcing policies

- It is an interplay at different levels and these levels all need to be aligned.
- For instance, an information security policy must respect the needs of the ones who have to comply with it.
- Optimally, it is also supported by official statements that communicate the importance of information security on a corporate level.
- It has to be clear that an information security policy change might experience resistance from invisible but very strong beliefs that have been built over a long period.
- Finally, knowledge about cyber risks and information security supports the employees to perform their job in a secure manner.

Another way to understand corporate culture at a deeper level is to examine the different levels of culture (see Fig. 1) (Schein, 1999). This understanding of culture is widely accepted in information security:

Level 1 – Artifacts

The artifacts are the directly visible things you can observe, see and feel if you look at your organization. This first level represents the expression «the way we do things around here» by considering the formal and informal processes, structures, and documents that explain how the organization coordinates its business. For instance, an information security policy document is a formal artifact that defines how information security is to be handled within your organization. Another example would be the formal structure of an organization – it is a directly visible artifact that reflects all the past knowledge of how the organization can perform most efficiently. How the organization is divided into units and subunits is basically «how we do things around here» on a macro level. From the visible artifacts, you can conclude a lot about culture, especially the cybersecurity culture. Just take a few minutes and try to figure out the visible artifacts of your company's cybersecurity program. Is it hard to find any? Do you already know all the documents and where to find them? Do all of the employees know about them?

Level 2 – Espoused values

Espoused values are the official statements of your organization concerning values, beliefs, and principles. Such an official statement can be, for instance, an official commitment to respect the privacy of users concerning user data. Other sources of values, beliefs, and principles are vision or mission statements. At Adnovum, we have the mission to «unite innovation, security and excellence to transform our clients' technological potential into powerful digital solutions». Among others, this is a clear signal that security forms an integral part of our mission.

Level 3 – Shared tacit assumptions

Shared tacit assumptions are the hidden layer of any organizational culture. They are the reason why cultures, in general, cannot just be changed by creating and publishing a new policy document or by formulating a new mission statement. Shared tacit assumptions are built over time and reflect an organization's cumulative experience and knowledge of how to succeed in the market. For instance, in a market where efficiency and fast time to market are critical, employees build strategies to succeed in this market. Over time, these strategies may not be discussed anymore because they are so inherent to the organization that they become unconscious and hidden. Because these unconscious beliefs and strategies are an integral part of the company's past success, it is so hard to work against them and adapt them if, for instance, the external environment changes and asks for a cultural change. A good example of a change of the external environment is the introduction of the GDPR in 2018. It forced all companies storing or processing customer data to comply with the new regulation. This might be a problem for some, because if a new information security policy conflicts with an organization's unconscious beliefs, it will be hard for the organization to incorporate the new policy.

In addition to the three levels above, there are arguments that, with respect to cybersecurity culture, there might be a fourth level (van Niekerk J.F., 2010). For the definition of organizational culture it is assumed that the job-related knowledge can be ignored because an employee has the required knowledge and the skills to do his/her job. This may be different for a cybersecurity subculture because, in general, it cannot be assumed that an employee has the required knowledge and the skills to perform his/her job in a secure manner (van Niekerk J.F., 2010). This is why knowledge builds the fourth level of a cybersecurity culture:

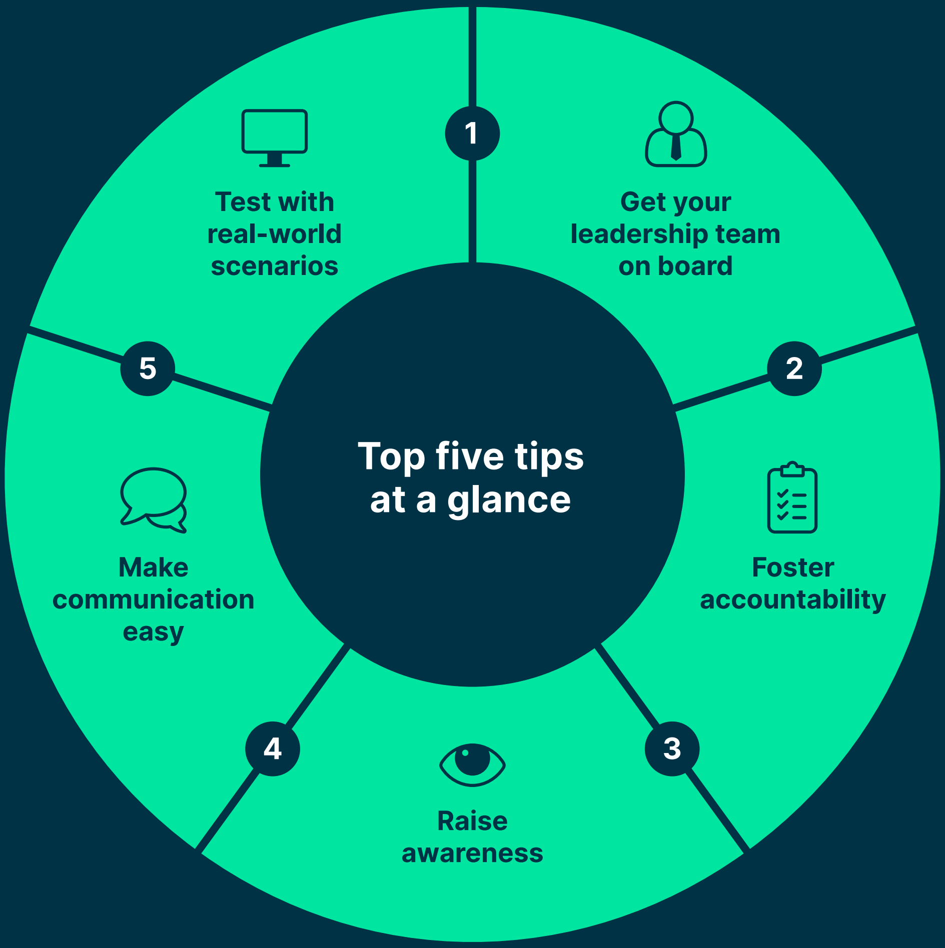
Level 4 – Knowledge

Knowledge with respect to cyber risks and information security builds the basis and can even be considered a requirement for performing daily business activities in a secure manner. It therefore builds the fourth level of the cybersecurity culture framework outlined above. Even more, the existence or absence of knowledge is able to influence all previous layers in a positive or negative way. Knowledge and awareness with respect to cybersecurity risks and threats provide the means to formulate adequate artifacts and communicate values that signal the importance of cybersecurity. But most importantly, this knowledge about the risks and their direct consequences can provide a reason to comply with a new policy, even if it is in conflict with the espoused values.

Top five tips for building a solid cybersecurity culture in your organization

The development of a healthy cybersecurity culture demands care and the ability to provide the necessary guidance. For organizations, cybersecurity culture could be effectively utilized to build up the appropriate security beliefs and values and to guide the security behaviors of employees when interacting with information assets to understand and to avoid activities that may be a risk to the organization and their assets.

It is not just something that grows organically or automatically in a healthy manner. The organization must invest real efforts in their cybersecurity culture. Having a sustainable cybersecurity culture is more than just a one-time event. It is a lifecycle that will generate returns on investment forever.



The following top tips shall serve you as a guideline or framework for building a culture of security and productivity that will provide durable profit across your organization and give you an idea of how that investment in cybersecurity culture should look like. The guideline serves to protect the confidentiality, integrity, availability, and traceability of information, as well as to protect the rights and interests of the organization and all natural persons and legal entities that maintain a business relationship with the organization and/or work for it.

①

Get your leadership team on board and establish a security organization

As mentioned previously, developing a healthy cybersecurity culture is not just the responsibility of the IT department or the CISO. Everyone is in the same boat. Cybersecurity can only work if it is understood as a shared responsibility that applies to the entire organization: From top-level executives to managers and associates, everyone must do their part in driving cybersecurity forward. The leadership team is not excluded from this responsibility. On the contrary, the commitment of the leadership team is crucial to successfully establish a cybersecurity culture and bring about real change. What is needed is a dedicated leadership team which proactively manages and promotes cybersecurity and is willing to embrace security as part of the company-wide culture.

The executive body of the company as a whole should exemplify a healthy security culture and encourage employees to play their part throughout the organization. The active engagement of the leadership team raises employee awareness and fosters a community where everyone is willing to take responsibility and contribute to a healthy cybersecurity culture with passion. The security organization is the backbone of a sustainable cybersecurity culture. It provides the connection between employees across the organization and offers ways to communicate. The security organization helps to bring everyone together against a particular problem and resolve it.

A security organization can be established by understanding the security interest levels within an organization, the security awareness, advocates, and sponsors. Security awareness makes security leaders aware of their contributions in making security better. Security advocates are the people with a down-home passion for implementing security. The sponsors are part of the management which shapes the security direction.

In many cases, cybersecurity in an organization is seen as a set of restrictions, such as limited systems, inaccessible websites, and trouble making a wrong move. Therefore, it is of high importance to include the relevant security roles (e.g. Chief Information Security Officer) in the company structure and to foster a positive environment in which everyone is comfortable with requesting demonstrations and asking questions from the employee to the leadership team.

Key take-away

The commitment of the leadership team is crucial to successfully establish a cybersecurity culture and bring about real change.

②

Put strict security policies in place and foster accountability

A culture of sustainable cybersecurity requires everyone in the organization to be «all in» and the security policies should be known and followed by each employee. Everyone needs to feel like they are responsible for it, from the senior executives to the stakeholder advisers and the employees. Unfortunately, in many organizations, security policies are the responsibility of the security department, if this even exists. In other companies, security is the responsibility of the IT department. In some cases, there are only rudimentary policies (with missing security relevant topics) in place, which are often known by a restricted circle and have not been approved by the management. The management is often not sufficiently aware of the topic of security. In such situations or companies where the «security language» is not really spoken, it is difficult that the security policies will be considered effectively by the employees. Thus the companies are exposed to different threats like ransomware and cyber attacks.

The good news is that in many organizations we have experienced that a workplace with strict security policies and procedures in place is always more secure, efficient, and productive compared to the one without proper policies and procedures to guide the workforce. It is significant to develop compact security policies that define and address appropriate security behaviors and procedures that are to be respected and implemented by all the employees without exception. Furthermore, it is essential to make sure every employee reads and understands these organizational security policies and implements them on a daily basis.

Key take-away

Clear security policies and guidelines ensure a more secure, efficient and productive business.

Consider this when creating your own security policy

When creating a security policy, it is important to know what a security policy exactly consists of and which aspects should be addressed. In simple terms, a security policy can be understood as an internal organization's rules and regulations related to the protection of critical assets (e.g. the security of the employees). The content of the document should be tailored to the target audience. This means that the security policy for employees should define the organizational requirements and information security regulations that must be observed by all employees when using information and IT devices (e.g. personal computers, workstations, as well as notebooks, smartphones and tablets). In this case, the following security requirements of such a document should include:

- Usage of hardware, software, data media and data which is not provided by the employer is not permitted (e.g. external USB data storage devices)
- Usage of organization owned software or data on IT devices that are not provided by a third party or an approved supplier (e.g. usage on personal devices) is not permitted
- Usage of company owned software or data on storage media that are not approved (e.g. non-approved file or cloud services) is not permitted

In the second part, it is relevant to structure the security policy, so that the following questions or topics are taken into consideration:

- **Purpose:** What topics does the policy cover? Does it cover expected behavior when using computers and mobile devices?
- **Context:** Does the security policy include content on new technologies and practices?
- **Strictness:** Does the policy prohibit certain behaviors, for example, the use of external USB data storage devices?
- **Compliance:** Does the organization's security policy reflect good practices?
- **Accountability and consequences:** Does violation of the security policy include the possibility of suspension or termination of employment?

Best practices

- Rewards and recognition
- Incentives
- Career advancement
- Punishment

Accountability is key

Experience shows that the basis of practical policies is accountability. Furthermore, it is important that the person responsible for information security looks for evidence so that the organization enforces security policies and holds employees accountable for violations. The main question here is: How do organizations handle violations?

This is how you best deal with security violations

Violations of security policies can have serious consequences. This is why violations must be recorded, reviewed, and adequately punished with no consideration of the violating party's rank or position within the organization. Each and every employee should be responsible for making an effort to comply and to inform his or her superior whenever guidelines or policies have been violated. Managers should be responsible for ensuring that such information is taken seriously and that the party providing the information is listened to with an open ear. In addition, a trustful work environment must be established and cultivated for such to be possible. Wrongful or unjustified reports of misconduct can harm a colleague's reputation. Such behavior is in and of itself a violation of the policy.

Are you making sure your employees do the right thing?

The organization can also choose to reward and recognize employees who do the right thing for cybersecurity. Once someone goes through the mandatory security program and successfully completes it, give them a «high five» or something more substantial. A voucher for a dinner could be an incentive for employees and will make them memorize the cybersecurity lesson that earned the treat. They will also be quick to tell ten colleagues that they got invited to a dinner for learning, and those ten will quickly jump into training. The other type of the reward is security advancement. Offer employees the opportunity to grow into a dedicated security role by promoting them. Include security as a career choice within your organization. The company could also integrate security goals into annual employee discussions, for example. At that moment, security will be considered as a business or company goal which will increase the employee's motivation because they want to achieve their goals.

Make security fun

What's very important is to make security enjoyable and fun. This means: If you have a special security training session, make sure it's not a boring lecture on a PowerPoint presentation. Instead, start the meeting with a security game that includes a different security category each month.

③

Provide cybersecurity education and awareness trainings

The best way to firmly establish a cybersecurity culture within a company is to make your employees understand the importance of cybersecurity education, training, and awareness. Only when all employees are aware of the devastating implications of cyber attacks, they will understand why they must follow security policies and procedures in their daily work.

Cybersecurity trainings may be labor-intensive, but they are effective in encouraging a cybersecurity culture. There are several ways to perform a training, from traditional PowerPoint presentations to advanced options. An engaging way to encourage security-centric behavior is role-playing games in which employees go through security-related issues and find ways to solve them in alignment with security policies.

Although all personnel – from new employees to consultants and contractors – should attend security awareness trainings, it is important to package security awareness trainings so that each target audience receives the relevant training. It is therefore essential to create security awareness training content according to the employees' level. Consider their department knowledge, responsibility level, data they access, and tools they use. For example, employees who do not have direct access to databases systems do not require a training related to database security. The training needs to reflect to security requirements for a specific task and the training frequency depends on the organization's needs and employees' learning curve. Technical employees, typically IT professionals, need to be trained in security techniques related to architecture, system and network design.

Key definition

Cybersecurity awareness is the process of educating your organization's entire team on the fundamental lessons of cybersecurity.

From a high-level view, the content needs to be:

- **Understandable** – use useful and easy to understand content
- **Relevant** – for example, a security training on cryptography would be irrelevant to HR
- **Actionable** – as a result of the training, all employees know what to do and what not to do in common situations. For example, employees who are on travel or in home office and use their mobile devices should be aware of the following:
  - Shoulder surfing (use privacy filters)
  - Only use public networks with VPN
  - No confidential calls in public areas
  - Do not dispose of company documents in household waste
- **Memorable** – the content should enable employees to memorize and practice skills, for example, by choosing and using a secure password and reading and responding to e-mails or interacting with people outside the organization

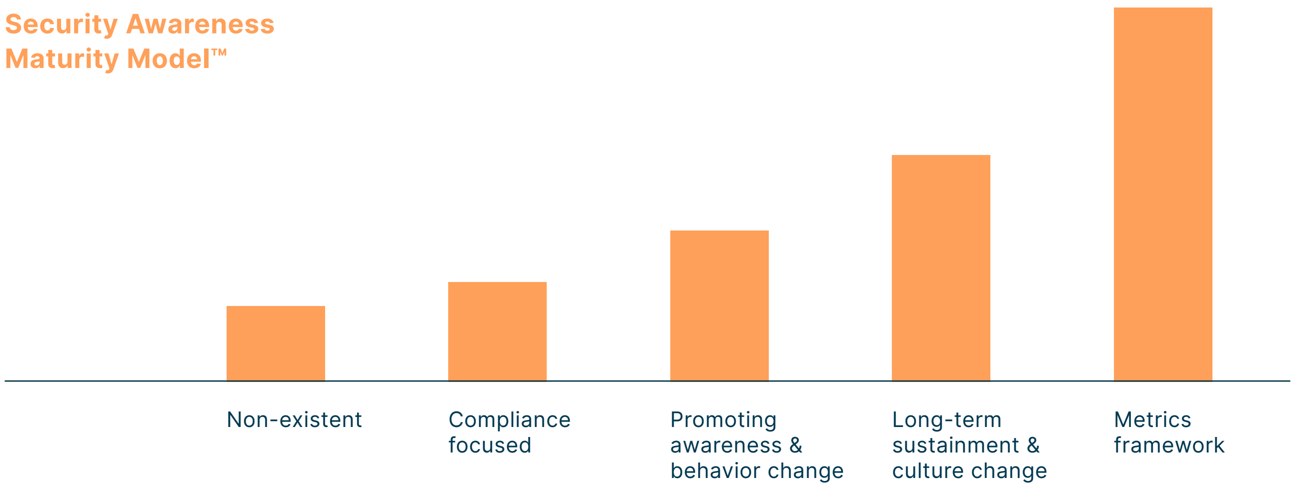
By developing appropriate knowledge and a habit of learning security best practices on a regular basis, employees will be able to detect and mitigate a security incident effectively, thus helping to make the organizational infrastructure really secure – and protect it from both inside and outside threats.

The SANS Institute developed a model to identify where your organization's awareness program currently stands and to track the progress of it. The SANS Institute hereby distinguishes five stages:

Key take-away

Only when your team is aware of the devastating implications of cyber attacks, each and every one of your employees will understand why she or he must follow security policies in their daily work.

Security Awareness Maturity Model™



Security Awareness Maturity Model™		Description
1	**Non-existent**	A security awareness program does not exist in any capacity. Employees have no idea that they are a target, that their actions have a direct impact on the security of the organization, do not know or follow organization policies, and easily fall victim to attacks.
2	**Compliance focused**	The program is designed primarily to meet specific compliance or audit requirements. Training is limited to being offered on an annual or ad-hoc basis. Employees are unsure of organizational policies and/ or their role in protecting their organization's information assets.
3	**Promoting awareness & behavior change**	The program identifies the target groups and training topics that have the greatest impact in managing human risk and ultimately supporting the organization's mission. The program goes beyond just annual training and includes continous reinforcement throughout the year. Content is communicated in an engaging and positive manner that encourages behavior change. As a result, people understand and follow organization policies and actively recognize, prevent, and report incidents.
4	**Long-term sustainment & culture change**	The program has the processes, resources, and leadership support in place for a long-term life cycle, including (at a minimum) an annual review and update of the program. As a result, the program is an established part of the organization's culture is up-to-date and engaging. The program has gone beyond changing behavior and is altering people's beliefs, attitudes, and perceptions of security.
5	**Metrics framework**	The program has a robust metrics framework aligned with the organization's mission to track progress and measure impact. As a result, the program is continuously improving and able to demonstrate return on investment. Metrics are an important part of every stage, and this level simply reinforces that to truly have a mature program, you must be able to demonstrate value to the organization.

In which stage is your security awareness program at the moment?

□ Non-existent
□ Compliance-focused
□ Promoting awareness & behavior change
□ Long-term sustainment & culture change
□ Metrics framework

④

Make communication easy

Communication is key when it comes to effective threat handling and mitigation. Make channels of communication clear, simple and accessible for everyone so that any suspicious activity can be reported to the relevant team in a timely manner and without hesitation. Never criticize your employees for communicating a suspicious incident that may turn out not to be an important threat. If you do, this could result in making them hesitant to communicate any malicious activity in the future, which may turn out to be of great threat to the organizational assets.

!

Cybersecurity Awareness Month

A very different and simple way is to celebrate the Cybersecurity Awareness Month, which takes place in October each year.

Key aspects of easy communication

The most important aspect is continuous communication. It is about reinforcing processes for security-related notifications and regularly communicating progress. Both employees and management should discuss every so often what is going well and what could be improved. A team-oriented attitude increases the feeling that everyone is acting on the same goal.

In order to draw people's attention to cybersecurity, there are many ways to facilitate communication. You can print cybersecurity awareness posters, distribute brochures with tips and tricks in a nicely designed graphical form. Furthermore, cybersecurity could be a topic in employees' annual review discussion, in which the employee's understanding is evaluated and any ambiguities can be clarified.

Dos	Don'ts
– Create a clear channel of communication – Keep communication up at all times – Foster a team-oriented attitude – Reinforce processes – Integrate security into the yearly employee evaluation feedback process	– Never criticize your employees for informing on a suspicious activity or incident that turns out not to be a significant threat – Don't ignore ambiguities in employees behavior

⑤

Test with real-world scenarios

Companies throughout the world are testing their employees by using different tricking and phishing techniques. This allows them to see how well they respond to cybersecurity attacks and what steps they take to communicate the issue and to mitigate it. Testing the security awareness of employees with some real-world cyber attack simulations can uncover the weak areas of your employees and will help you to improve it.

Another important factor is to systematically conduct penetration tests of your organization's IT infrastructure. A penetration test exposes weaknesses and examines how vulnerable a system is. A solid risk awareness encourages project managers to organize a penetration test before every major release of new software. To formalize the requirement of regular penetration tests, a security policy for projects can be put in place. Based on the results, relevant security measures should be implemented to protect the IT infrastructure of your organization in the event of an actual attack.

The development and testing of security awareness training provides a continuous learning experience for all of the employees involved.

Key take-aways

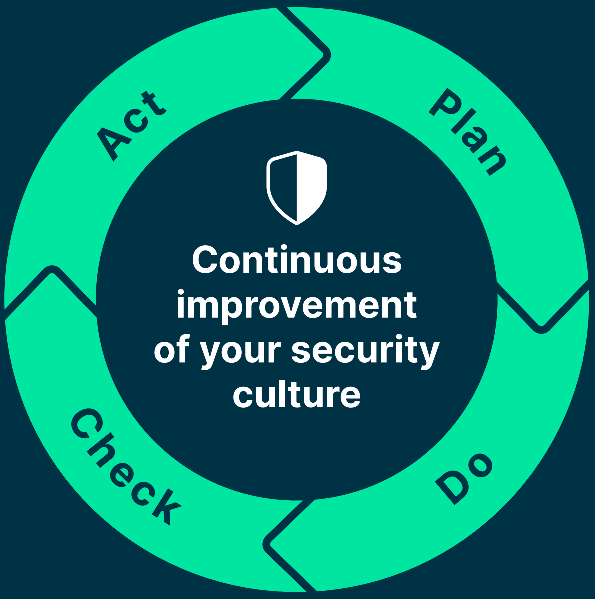
There is no better way to ensure that your workplace is prepared against cybersecurity threats than to test it with real-world attack simulations.

The «workplace» always implies the IT infrastructure, the organizational infrastructure as well as the employees.

Let's get to work

When every employee in an organization is well-educated about the security risks and necessity of cybersecurity and gets training on how to implement a secure environment, the entire organization will benefit from it. Not only will your organization be more secure, but your employees will also be motivated to participate in making cybersecurity culture better.

One important consideration is that information security culture is not a one-time activity, but needs to be continuously analyzed, promoted, and adapted. Therefore, this task can be considered a cycle, as shown on the next page.



Key take-away

Information security culture is not a one-time activity, but needs to be continuously analyzed, promoted, and adapted.

Plan	Do	Check	Act
This means that the organization in the planning phase (Plan) shall first provide a basic cybersecurity structure by putting artifacts in place.	In the second phase (Do) it is important to establish the security controls such as security awareness programs, policies and clear communication channels and release official espoused values such as statements which represent the company's principles, beliefs and values (e.g. by including cybersecurity into the mission and vision statement of the company).	After having implemented the security controls it is vital to evaluate and assess (Check) if the measures in place are effective and if the shared tacit assumptions are aligned with the artifacts and espoused values.	The last phase (Act) gives your organization the opportunity to improve the security controls in place and fill the gaps identified in the third phase, for example by adapting your security policies according to the current situation of the company.

The model is based on the Information Security Management System (ISMS) of ISO 27001:2013 standard.

We support you on your journey!

Adnovum offers a wide range of services to help organizations assess the current state of their cybersecurity culture and design individual security solutions, including awareness campaigns and tailor-made trainings.

In fact, both understanding the weaknesses of the current security culture and fostering the knowledge of the measures needed to improve security are key steps in developing a purposeful and healthy security culture in a constantly changing global threat landscape.

Do you want to learn more about our services?

Our experts will be pleased to talk to you, contact us!

- Schein EH. The corporate culture survival guide. Jossey-Bass Inc.; 1999.
- van Niekerk J.F. Information security culture: A management perspective. 2010. Accessed on 10.06.21: https://www.sciencedirect.com/science/article/pii/S0167404809001126
- Sasse A. Scaring and Bullying People into Security Won't Work. 2015. Accessed on 10.06.21: https://www.researchgate.net/publication/277784015_Scaring_and_Bullying_People_into_Security_Won%27t_Work

adnovum

The Swiss software company Adnovum offers its clients comprehensive support in the fast and secure digitalization of business processes from consulting and conception to implementation and operation. Its core competencies also include identity and access management as well as security consulting. Our client focus is on companies that want to differentiate themselves through innovative digitalization solutions, among them banks, insurance companies, transportation and logistics, and the public sector.

Adnovum was founded in 1988. At our headquarters in Zurich and our offices in Bern, Lausanne, Budapest, Lisbon, Ho Chi Minh City and Singapore, we employ over 600 staff today.

adnovum.com