Charter of Trust

Charter of Trust P6 Education Taskforce

White Paper 2021: Transforming Human Behavior in Cybersecurity

The ultimate vision of the Charter of Trust P6 Education Task Force is for cyber security to be ingrained in the culture of every organization and individual. For good reason. Just as road safety is an intrinsic part of growing up in the 20th century, cyber safety should be embedded in the way we are raised in the 21st century. Security by default should apply to our national education curricula and our continuous professional development. Our employees from every level in industry and the public sector should be cyber aware in their jobs and their daily lives.

This is an ambitious vision, and a journey on which many organizations are only just embarking. The goal of this White Paper is to share wisdom and practical advice based on the experience of leaders from the Charter of Trust's members on the topic of creating a cybersafe culture.

Charter of Trust

Key recommendations for industry and government

A joint commitment from Charter of Trust Partners and Associated Partners

1. Make the **risks** inherent in cyber-attacks **transparent and visible** – and highlight the opportunities of cyber security. Use dedicated risk management to reduce cyber risks.

   Common risk-based approach for the Digital Supply Chain

2. Ensure that all employees throughout the entire organization **receive cyber security education**. Embedding cyber security into the culture of an organization (e.g. readiness through regular phishing simulations and crisis management exercises) builds resilience.

   Webinar: "The Human Element in Cybersecurity"

3. Position cyber security with **top management** and introduce suitable governance structures. Anchor responsibility for cyber security at the highest level in the company.

   Education Campaign Booklet: Seeing cyber security as an opportunity

4. Increase **knowledge and skills** through industry-accepted standards and certifications. Offer continuous improvement of training content based on evolving threats and internal cyber security posture.

   Towards a new normal in Cybersecurity: How a systemic approach and certification create the basis condition

5. Implement a curriculum to embed "security by default" design in the **development** of services and products.

   Ensuring security by default

6. Encourage cyber security **community building** throughout the entire organization.

   Welcome to TrustNet (trust-net.co)

7. Share **best practices** and promote positive cyber security behavior with other cyber security experts through external interaction throughout the supply chain.

   Information Sharing Communities – Defending Better Together

If you would like more information on transforming human behavior in cyber security in your organization, please contact us.

Charter of Trust

Charter of Trust leaders help create a cybersafe culture in business and society

AES

At AES, our mission is to improve lives by accelerating a safer and greener energy future and safety is our first value. Aligning cybersecurity to both safety and our mission through a globally coordinated, locally delivered model has been the most effective way of creating a cybersafe culture. We are working to achieve this through embedding cyber activities in our regular safety cadences, including Monthly Safety Meetings, Safety Walks, and Plant Visitor Safety Briefings. In order to make these moments more authentic, we provide resources to enable local leadership to communicate cybersecurity through their own language and perspective.

Ryan Boulais

Vice President and Chief Information Security Officer at AES

Charter of Trust

Allianz

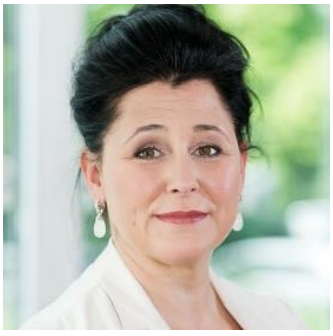
Since 2016, cyber incidents have ranked among the top 3 global risks in our Allianz Risk Barometer. There are many ways how organizations can protect themselves against this risk: With technology, with insurance, and through policies and guidelines. But the most effective defense is still our own employees.

At Allianz, our goal is to build a strong "human firewall" with alert and security-conscious employees who are our first and last line of defense. To ensure this, our security department offers a variety of awareness activities, such as phishing simulations, micro-learning modules, web-based training, webinars on specific security-related topics and, of course, our Security Awareness Month. October is packed with events covering a wide range of topics, from security evergreens like social engineering to current issues like working securely from home.

Education is also critical, as there are many areas that need to be strengthened. Therefore, Charter of Trust partners have agreed to support training on cyber security issues – especially for small and medium-sized enterprises. In Germany, for example, the Charter is cooperating with Allianz for Cyber Security to provide a so-called "emergency card" that explains quickly and simply what to do in the event of a cyber-attack.

Human errors are the most common cause of cyber insurance claims in terms of numbers. Therefore, the best way to achieve significant and lasting improvements in information security is not to implement more technical solutions alone. Instead, we need to reach out to our colleagues, raise awareness, and educate everyone who interacts with corporate data on the basics of information security.

Making our organization resilient to attacks is everyone's responsibility. That of the security team. That of the executive team. That of the IT administrator. That of the end user. The strongest and most resilient organizations are the ones that bring everything together: Technologies, processes, and most importantly, our people!



Bettina Dietsche

Member of the Board of Management at Allianz Global Corporate & Specialty

Charter of Trust

Atos

Today, cybersecurity has been identified as the number one “problematic shortage” area across all of Digital. It is very worrying that the shortfall has increased dramatically in recent years. To cope with this situation, many companies are looking for additional cyber security personnel and are also under a lot of pressure to implement the latest innovative digital security solutions whilst ensuring the daily uninterrupted operation of their systems.

Due to constant new technologies, weaknesses in the IT environment often arise unnoticed. Without appropriate digital security measures, these quickly become unmanageable risks. Especially with new technologies like the Internet of Things and with BYOD (Bring Your Own Device), these are a big challenge for many IT departments. Upgrading security systems begins with governance and company culture such as password management, patch management, and all recognized practices, along with continuous information and training of employees.

Therefore, applying and maintaining good cybersecurity practices across all your Digital organizations: for IT, for Development, and for Production in a ‘Defense-in-Depth’ approach is always the best policy. Train yourself to think about your cyber security as you are doing it in case of your daily personal hygiene.”

Pierre Barnabé

Senior Executive Vice-President, Head of the Global Division Big Data & Cybersecurity

Charter of Trust

Dell

Every year, the world becomes a better place thanks to advances in, and greater global access to, technology and information. I see this daily in the digital transformation journeys of our customers – from enabling more timely and accurate genetic sequencing of terminal diseases, to greater access to education for our world's youth, to better safety outcomes as predictive analytics find and fix system faults before they happen. What I also see though, is that for the world to gain these benefits, the technology that underpins and drives them has to be trusted, and the evolving cybersecurity threat landscape is threatening that trust.

To tackle this head on, as an industry we should invest heavily in employee training and awareness, creating a cybersafe culture and shifting the employee mindset to one in which security is everyone's responsibility. As one of the world's leading technology companies, Dell Technologies takes this responsibility seriously, and security and trust are at the core of all we do, not just in our security organization, but amongst every team member and process across our company.

John Scimone

SVP and Chief Security Officer, Dell Technologies

Charter of Trust

NXP

At NXP, we've set out to help our employees understand their security environment and understand the adversaries they face. We want these development experts to think like hackers. This is especially crucial for companies like NXP that build security products for e-government, automotive, banking, industrial, and IoT applications.

With this mindset, NXP established a "Security School" to teach employees how to recognize attack surfaces, become more fluent in the vocabulary of cybersecurity, and gain a foundational understanding of cryptography, security implementations, and system security – to think like a hacker. The goal was to become more attuned to the nuances of security and to train our team members to recognize common behaviors and patterns. The format and approach of our program are similar to a university curriculum. Students start with the basics of cybersecurity and security design methodology and then ramp up to advanced training. For example, tracks for in-depth architecture address security in the product development (concept-to-release) life cycle. We also train our employees to meet new standards, laws, and regulations in different markets, geographies, and industries. This includes the emerging standards ISO/SAE 21434, for automotive, and IEC 62443, for industrial markets.

Immersive in-person experiences where mistakes are allowed often result in learning that "sticks" and is better remembered. At NXP, we use an "escape room" scenario that requires trainees to think like a hacker. In this format, a team of employees must find the way out of a room by following clues and solving puzzles related to security. Using hacking techniques and good security practices, they encounter and solve physical and logical attack situations as well as social engineering traps. Time-driven tasks increase the likelihood of making mistakes, which forces the team to think quickly and take decisive action. Because Covid-19 has moved our training online, we plan to offer a virtual escape room to encourage participation from our employees around the world, as well as those working from home.

Wolfgang Steinbauer
Head of Crypto & Security,
NXP Semiconductors

Charter of Trust

Siemens

Digitalization can make our lives easier, better, and more sustainable. That is why more and more areas of our lives are being digitalized, whether it is the door of a train, the production line in a factory, the sensors of a smart building or patient records in a hospital – everywhere, data and its intelligent use make all the difference. The pandemic has accelerated the digital transformation.

Yet this also brings challenges. Hackers are getting better and faster as their potential points of attack increase. We are seeing a huge rise in threat levels. And we must react to this evolving threat, by responding faster than ever. We can only achieve this if we work together to create a resilient cybersecurity ecosystem, involving all players: large companies, but also SMEs and startups, universities, and research institutions as well as governments. To energize, promote, and coordinate this robust community working together, we see education and workforce development as key.

As such, cybersecurity is a key ingredient to our company's transformation and evolution. It gives us and our customers confidence in a trustworthy, digital future.

Cedrik Neike
Member of the Managing Board of Siemens AG and CEO Digital Industries

Charter of Trust

TotalEnergies

Cybersecurity is not only an IT topic – it is also a question of human behavior and understanding of cyber risks.

Parallels can be found with safety at work, one of TotalEnergies' value which is widely understood and applied by our colleagues. In our business, cyber incidents could have impacts in real life and generate bad consequences on the environment and affect human lives. Like safety at work, everything must be done to avoid Cyber-incidents and all employees have a role to play

Managers are committed to communicate key cybersecurity messages to train their team and promote best practices among them. But cybersecurity culture also needs ambassadors to spread in our organizations. As younger employees often have better digital literacy, they can help spread cyber messages and help their colleagues to understand best practices and apply them.

This cyber reverse-mentoring by the younger generation can accelerate the change of culture required to raise cyber risk awareness, not only at work, but also at home. Like safety, best practices at the workplace can avoid major problems when also applied at home!

Each of us has a role to play to promote cybersecurity. Let us improve our daily behavior to protect everyone!

Thierry Renard
TotalEnergies Global HR Service Director

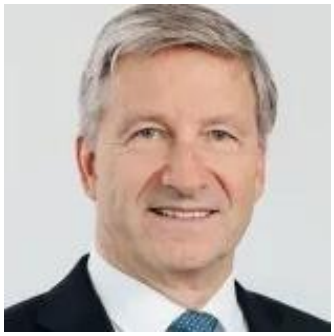
Charter of Trust

TÜV SÜD

Safety and security are becoming increasingly inseparable in our digitalized world. With the exponential rise in digitization, next to functional safety, cybersecurity has transformed into a crucial prerequisite to ensure trustworthiness. However, how do you raise awareness of cyber risks among your own workforce and achieve changes in behavior? For TÜV SÜD, the well-known guiding principle "Security is everyone's responsibility" is decisive here. In concrete terms, this means that cybersecurity is not something that employees simply receive from their management. Instead, employees need to understand the pivotal role they play as the “human firewall” and their vital role in contributing to the cybersecurity of the company with their behavior.

This understanding of the central role of employees makes it more effective in creating the mindset of a cybersafe culture and the use of modern technologies supports our employees in this. TÜV SÜD empowers its workforce with regular cybersecurity training as part of the CISO Academy. With the help of modern gamification approaches, it becomes easier to internalize the effects and consequences of the right actions and to ensure that there is an effective response mechanism during emergencies.

As a trusted partner of choice for safety, security and sustainability solutions, TÜV SÜD's goal for over 150 years has been to enable progress by protecting people, the environment and assets from technology-related risks, in the physical and in the digital world. For this to succeed, we must start with our own employees and live a cybersafe culture throughout the company.



Prof. Axel Stepken
CEO TÜV SÜD

Charter of Trust

Academic perspectives on behavioral change from the Charter of Trust's Associated Partners

Hasso Plattner Institute

Cyberspace is a threatened place. Over 300,000 new malware files are created every day, millions of digital identities are leaked, and new methods for compromising digital systems are constantly being devised. Most recently, the case of the Colonial Pipeline hack in the U.S. and also the spectacular SolarWinds hack have shown again how vulnerable critical infrastructures in the digital space are today, despite all precautions and security efforts.

This permanently insecure situation not only causes incredibly high costs, but also continually shakes confidence in the digital technologies and infrastructures without which our lives no longer function and our prosperity cannot be sustained. They also put the brakes on economic momentum. This applies in particular to the much-needed digital transformation of SMEs and the implementation and testing of new digital ideas by startups. Networked systems with inadequate protection provide a perfect ecosystem for spreading malware and scaling its damaging effects, enabling the DDoS and APT attacks on sensitive IT systems that occur every day, including in public administration, healthcare systems, and schools.

For the general population, the Internet and the Web are a daily commodity – not much goes on without access to the Internet and the digital services it provides - but to speak of secure, non-threatening, and enlightened use is far from reality. On a large scale, usage data and confidential personal data are disclosed thoughtlessly on the Internet, and for many users it does not even matter who gains access to this data. The widespread and extensive use of social media on foreign digital platforms is sad proof of this carelessness and lack of awareness of the problem. The lax handling of one's own digital identities is also frightening. The most popular password worldwide is still "123456," and it is used to "protect" about 1% (!) of all digital identities.

Establishing and ensuring cybersecurity is a very complex undertaking. Each new smart device and user adds to the complexity of the digital space and potentially provides new gateways for cybercriminals and cyberattacks. Interestingly, dealing with, combating, and mitigating threats in cyberspace can be compared very well with the state of societal hygiene measures to maintain and raise the level of health and to prevent and combat diseases and epidemics. There, too, the spread of diseases depends not only directly

on the behavior of people themselves, but also on the existence and condition of appropriate public infrastructures. In light of such a comparison, the digital space and our cyber vulnerability currently find themselves in a situation similar to that found worldwide in the pre-industrial age with regard to the health issue: ignorance of the causes of diseases, lack of hygiene awareness among the population, and lack of sanitary infrastructures for the general population.

It was only 110 years ago when the spell of biological epidemics was broken, at least in the Western world. At that time, the “1st International Hygiene “Exhibition” took place in Dresden, Germany. It attracted more than five million visitors at the time, underscoring a claim to world stature. This "World Health Exhibition" of 1911 documented the breakthrough of a social movement that had already formed on a broad front in the 19th century and had set itself the goal of familiarizing broad sections of the population with the rules of health and hygiene in order to increase public health. As a result, infectious diseases in particular, which were widespread in Western societies, declined rapidly, leading to greater health, well-being and economic prosperity.

The current pandemic reminds us that human existence and the prosperity of societies are under constant threat. Before the Industrial Revolution, epidemics were permanent companions of mankind. In Europe, the severe plague epidemics are well anchored in the collective memory. Also, everyone has heard of epidemics introduced by colonists in the Americas. Disease and pestilence have been a pervasive leitmotif of human civilizations, in Europe at least until the Industrial Revolution, and in some regions of the world to this day. They brought disease and death, were accompanied by economic decline and stagnation, sparked or intensified political and religious extremism, and in the worst cases led to the demise of entire cultures.

Since the era of Enlightenment, we have been increasingly successful in counteracting the spread of epidemics and diseases and increasing public health. Research into the causes of diseases was carried out on a scientific basis. Bacteria and viruses were discovered as pathogens and triggers of epidemics, which were able to multiply well in contaminated water, through poor cleanliness and lack of waste disposal. The response of the Enlightenment was to educate people at large about the causes of disease, to propose simple measures to diminish ecosystems for bacteria and viruses, and to build societal infrastructures – both private and governmental – to make it more difficult or impossible for pathogens to spread.

Thus, a broad "hygiene movement" formed in the 19th century, manifesting itself in the form of associations, government regulations, infrastructure projects, and private initiatives by industrialists. Hygiene associations ran large-scale educational campaigns to establish simple hygiene rules, such as hand washing, as a cultural practice. Physicians and scientists, such as the St. Gallen physician Jakob Laurenz Sonderegger, and representatives of the Red Cross societies succeeded in bringing hygiene issues relating to the handling of air, water, housing, and food into widespread discussion via numerous regional groups that branched out deep into working-class milieus. Hygiene guidelines for work in hospitals or at factory workplaces were also developed and their observance enforced.

The state invested heavily in science and research to discover the causes of diseases and develop effective preventive measures and medicines. The discovery of the pathogens of syphilis (at the Berlin Charité), tuberculosis and cholera (by Robert Koch, founding father of modern microbiology) were milestones of research. Ignaz Semmelweis proved that pathogens could be contained by disinfection, and doctors henceforth washed their hands when in contact with patients. Joseph Lister used disinfectants for wounds before surgical interventions, and Louis Pasteur developed the process that is still used today to disinfect food by heating it.

Infrastructurally, too, decisive steps were taken to make it easy for people to keep themselves clean. Although there was already a sewer system for wastewater disposal in Roman antiquity with the "Cloaca Maxima," these systems did not become widespread until the 19th century, starting in the European metropolises of Vienna, Hamburg, London, and later Berlin. Similarly, drinking water and fresh water supply via cast iron pipe systems could not be widely spread and installed to provide clean water to households until the Industrial Revolution.

These measures were flanked by private initiatives, such as that of Odol founder Karl August Lingner, who in the wake of the "1st International Hygiene Exhibition" in Dresden, founded the "German Hygiene Museum" in 1912, which to this day is known far beyond Saxony. The museum was conceived as a place of education on public health and is still today a platform for various information events around basic hygiene and health.

Today, it seems natural to us to have sanitary infrastructures in every home. Education on cleanliness measures such as hand washing, dental care or other cleanliness measures begins as early as infancy. This has not only promoted general health, but also increased life expectancy and ultimately contributed to greater economic stability and prosperity.

Seen in this light, we can learn a great deal from the historic hygiene movement of the 19th century for developing strategies to contain and combat cyberthreats. In many respects, we are still in a similar situation in the field of IT security that prevailed in the Middle Ages with regard to infectious diseases: the Internet and our dependence on its increasingly widespread use is a wonderful biotope for digital diseases and epidemics, like the expanding cities in the pre-industrial age.

Cyberthreats seem like an uncontrollable external force whose origins we do not know. Far too often, businesses and other institutions hope (and "pray") not to be affected by the compromise of their IT systems. In particular, SMEs and startups are at risk to their existence if cyberattacks are successful. Attributions remain vague and culprits are quickly found to blame without compelling evidence, and exclusion as in the case of foreign technology is commonplace. Often, there is no alternative but to completely abandon the IT systems in question and rebuild them.

Not only is there a lack of secure manners on the part of users of digital systems, i.e. there is no digital hygiene awareness, but there is also a lack of secure and sovereign IT infrastructures for state administration and its interaction with citizens, as well as a lack of binding standards for the development of trustworthy and reliable IT systems. There is a lack of "sewerage and sanitation" in the digital world, which is very conducive to the spread of malware and the success of cyberattacks.

"Governance" structures are also not yet sufficiently adapted to the necessities and paradigms of the digital world. Responsibilities for IT security are fractionalized, and the pursuit of cyberthreats follows the logic of national boundaries and sole responsibility of state action. This is not appropriate for cyberspace, where national borders play virtually no role and the most powerful actors are not states but large digital companies.

Just as with controlling biological pandemics, we need a concerted effort by policymakers, business, and civil society - we need a digital hygiene movement. The good news is that we have the means and knowledge to address digital hygiene on a broad scale. But it needs the understanding and the political will, and the economic incentives are there.

As with biological pandemics, digital malware spreads along digital transmission media (networks and IT infrastructures) and their weakest links. 90% of all cyber risks can be avoided by following basic digital security rules. However, these must become as natural for everyone as washing one's hands and brushing one's teeth.

In education, we now have powerful tools to provide low-threshold access to knowledge that will protect us in cyberspace. Via digital learning platforms such as openHPI and learning infrastructures such as the HPI School Cloud, the state, authorities, IT experts and companies can bring simple digital hygiene rules to all layers of the population.

It is a fact: Every student uses digital systems in their private environment on a daily basis, but education on how to use them safely is lacking. IT security and digital hygiene measures must be practiced early on with the help of digital school platforms, just like washing hands, swimming, and traffic rules. No one needs to have a degree in computer science to do this. Basic digital rules can be practiced in structured form in various educational contexts via the many high-quality and low-threshold digital learning programs. The openHPI ecosystem alone, with partners from SAP, the World Health Organization, AI Campus, the eGov platform, etc., can already provide solid basic knowledge on digital education and digital hygiene.

In numerous corporate contexts, other learning platforms provide relevant courses for your employees, of which important contributions are offered through the Charter of Trust Education Taskforce – a network of globally-acting companies, research institutions, and government agencies. Increased use of secure and privacy-compliant digital platforms in school and other educational contexts will create a natural ecosystem in which many new low-threshold and free educational offerings can be made available. All that needs to be done is to ensure that these topics are included in teaching and training curricula.

Our efforts can also intensify in research and development. Aside from basic security rules, procedures must be developed to make it easy to check new IT systems for security vulnerabilities and opportunities for compromise. Ideally, there would be methods such as pasteurization for digital systems, which could be applied without much effort by SMEs and startups (as well as any citizen) to make their digital products secure.

It must also be possible to regularly exchange knowledge about vulnerabilities in common IT systems in a trustworthy manner in order to gain collective protection against known "pathogens". Jointly operated IT infrastructures (even across national borders) can help here in order to install "IT security as a service" firmly in the portfolio of digital products and thus enable "herd protection".

Complex IT security standards and certifications must be designed in such a way that they can be applied by everyone without great cost or prior knowledge, which can also be enabled through the use of shared

infrastructures. These infrastructures would then be the sewers and freshwater pipes of the digital world, with which digital pandemics can be effectively prevented.

Finally, one can also think about establishing a "Digital Hygiene Museum" – quite possibly as a physical place that can be visited, for example, in the context of school field trips to get a comprehensive picture of cyber hygiene using "touchable" exhibits, such as live hacks. This could also be an important focal point for relevant information events, a meeting place for the exchange of science, business, and politics, where the common will to achieve digital hygiene is regularly reinforced and reaffirmed.

We have it in our hands to initiate an epochal shift from the Middle Ages to the modern era in the digital world and, with the help of the resources of science, cooperation, and technology, to make cyberspace a safe and prosperous place for all people.

Prof. Dr. Christoph Meinel
Internet Technologies and Systems,
Hasso Plattner Institute