Towards a User Centric Cybersecurity

It's time to empower ourselves: we are the first line of defence in our digital world

“What if users were not only a threat, but rather one of the answers to the challenges posed by cybersecurity?”

Instead of 'zero trust' architectures based on 'distrust by default', it would certainly be more effective –and cheaper– to put users in a central position, to turn them into real cybersecurity players within their organisation. However, this approach would require to rethink the 'Human-Machine' interactions, to make security more intuitive, and to integrate the 'security by default' requirement into processes and uses. In other words, to give priority to the 'user experience'...

The goal is certainly not to oppose Human Beings and technology! On the contrary, the aim is to make the most of both: on the one hand, users whose awareness has been raised and who have been empowered will not try to systematically bypass security rules; on the other hand, more 'empathic' technologies would better adapt to users' needs and put more emphasis on data security, as close as possible to users.

Guillaume Tissier
President, CEIS

General (Ret) Marc Watin Augouard
Founder, FIC

“It’s time to empower ourselves: we are the first line of defence in our digital world.”

With this statement, we want to recognise all those who form the first line of defence in making our digital world safer. This is the purpose of the theme for FIC 2020: “Putting human beings at the heart of cybersecurity.” This statement is for you if:

- *At home,* you enjoy the benefits of digital life, the immediate access to unlimited content, sharing information with friends and families anytime, anywhere;
- *At work,* you are responsible for information security, you develop new solutions to make the digital community safer, you contribute to the fight against online crime.

“Cybersecurity may sound technical and virtual but it is far more than that. As for any other challenge that our modern society faces, it is critical to recognise the human factor and to empower people to protect what is dear to us. Whether cybersecurity is your daily job or not, you and I are the first line of defence.”

Elly van den Heuvel-Davies, Chairwoman of the FIC Advisory Board and Secretary to the Cybersecurity Council, The Netherlands

Together we the members of the Advisory Board of the FIC Forum, together with CISOs, CIOs, analysts, researchers, developers, trainers and teachers from all over Europe, need to work on the cybersecurity of our respective organisations, countries and of the European Union. Together we must work to meet our challenges, finding solutions to protect what we hold dear. There is much at stake for us: an open, free and prosperous society with our own standards and values.

“Ultimately, cyber space is a man-made domain – and we define what its natural laws are. When our perceptions change, those laws will change.”

Alexander Klimburg, Director, The Hague Centre for Strategic Studies, Austria

Humans are (still) at the core of the digital world

Nowadays, people and technology are closely connected. Digital technologies have been the source of many improvements and developments in the world around us, including expanding access to knowledge, increasing our ability to communicate and revolutionising the ways in which information can be spread and shared with others. In many ways, technology is so interwoven into society that it can be difficult to separate the good from the bad. But whilst we may sometimes feel that technology has taken control of our lives, ultimately humans are still in charge. After all, artificial intelligence, algorithms, robotics and privacy and security-by-design are – for the time being – human inventions. Humans are still at the core of our digital world: as citizens, consumers, developers, victims or criminals. We are the architects of it all.

Digital transformation storm is engulfing the companies in an unprecedent way generating new business models, new organization structures and new way of thinking. Everything is changing, everything is transforming, everything become digital. The new technologies bring however not only tremendous benefits but also severe risks associated with cybercrime. Data is the new oil that fuel our entire ecosystem and it is our role as IT professionals to protect our new digital life.

Yugo Neumorni, Cybersecurity Council Chairman, European CIO Association, Romania

Cyberspace will not last without a trust model

The global technology companies, primarily from the USA and China, seem to rule our (digital) world. For many governments, they seem out of reach despite the fact that they manage server farms and clouds that contain our data, they implement smart cities based on sensors, robots, self-driving cars and other digital services, and they process our sensitive information using non-transparent algorithms

"Over the past ten years, digital security and trust have become strategic policy issues: from critical infrastructure protection to digital strategic autonomy, from education to data and innovation... and who knows tomorrow, maybe also cybersecurity in face of the accelerating climate crisis? Looking at Europe, with the Cybersecurity Act bringing trust through certification and at France, with an ecosystem eager to build more synergies and co-construct common solutions, 2020 could be the beginning of a new era

Jean-Baptiste Demaison, Chair of the Management Board of ENISA – Senior Innovation strategy advisor at ANSSI, France

Yet for all the socio-economic benefits that digital technologies bring, we also become more susceptible to malicious actors and those seeking to subvert or manipulate technology for their own motives. A powerful example of the harm caused by such actions includes nationwide Internet shutdowns against the population. Instances of sensitive data harvested by multinational corporations being lost or stolen also highlight the risk of digital technologies to the privacy of individuals. Similarly, digital technologies can be weaponised and used in cyberattacks that are difficult to detect and trace. There is also therefore a strong need to make sure that those with the power to act are doing so responsibly and can in some way be held accountable.

The question is: are we still in control of our sovereignty, independence and data? No individual, no government or company has full control. There must come a point where we place our trust in others to act with due respect to our rules and values. Trust cannot be given based solely on good words and promises - it is earned based on the capacity to make verifications of others' behaviour.

"Cyber-risk is difficult to calculate because neither its probability nor the cost of its consequences can be mathematically modelled. Losses are essentially caused by conscious and deliberate acts of human beings (cybercriminals). To quite Philippe Bonte, CFO of the leading Luxembourg insurance group: «A storm is stupid, it doesn't learn anything, unlike a cybercriminal who learns from every attack». It is therefore vital to invest in human skills to strengthen our defences."

Pascal Steichen, CEO, SECURITYMADEIN.LU, Luxembourg

How do earn this trust? At national level, citizens have to trust the government to be able to adapt the surveillance architecture to the new realities; governments have to trust their citizens with increasingly powerful tools, such as encryption, whilst both citizens and governments have to trust that private industry will act in the interest of their shareholders whilst causing as little harm as possible. At organisational level, the Zero Trust approach provides CISOs with a model that help them identify threats and limit the impact of breaches.

"Digital humanity: we still have a choice!
We live under algorithms. We can't go back to the Flintstones's disconnected era. There's no need to believe that every one of us is a potential elite hacker. Preservation of our own data is becoming a luxury. How to go beyond the state of a simple vulnerable user to that of an enlightened user? By creating common points of reference, landmarks, #CyberCivism. By taking the time to understand the business models of service providers and by selecting the most virtuous ones first. By becoming aware of the reverse side of the «marshmallow and silicon» digital age."

Lennig Pedron, co-founder and President, ICON NGO, Switzerland

We need you – we need each other!

To those who work in information security or against cybercrime: you are the first line of defence in protecting our community, at work and at home. Your voices need to be heard, your role properly valued and supported by your management, whilst you must also be able to pursue a career. It is our duty to invest in the human factor of cybersecurity. Empowered people are the most critical weapon in our battle against cybercrime and instability in cyberspace.

"The CISO is a rare bird who combines the qualities of a seasoned technician, masters the concepts of risk management and international security standards, and reconcile them with the skills of a negotiator and communicator to convince top management to invest money in securing the systems against attacks that may never affect the organization (make no mistake! Either you have been hit or you will be). The one we don't listen to too much until the catastrophe occurs! The one that no organisation can do without, in the face of the ever-growing cyber threat."

Phédra Clouner, Deputy Director, Belgium Cybersecurity Center, Belgium

Recognising and empowering people is essential. It is about common sense – and it starts with putting human beings at the top of the agenda, as FIC does this year. It is continued by developing relevant outcomes such as publications and white papers, recognising existing best practices, rewarding motivated people, all the while keeping social values in mind.

"Security is very much about bridging the knowledge gap. While we can't get everyone to do the most secure thing all the time, we can reduce the risk and impact of incidents by having a resilient user population. One way to get better is to leverage «teachable moments». Training a user once a year on security best practices doesn't work - they'll sit through the training but forget. Training them when they make a mistake is much more effective. Having the best incident response team, that only kicks off after a data breach happened, isn't anywhere as effective as having well-educated users who notice when they, or others, make a mistake, and let you know when the incident is still relatively minor."

The future of cybersecurity belongs to initiatives that enable and empower people to protect themselves from attackers, empower each of us to report what we perceive is of concern, and for judicial authorities to track down criminals. Our first line of defence must be strong and resilient.

New technologies like the cloud increase the number of hazard sources since these systems themselves can be used as bases for attacks. We have not yet witnessed any catastrophic failures in the energy, transport or financial sectors, but this is more down to good fortune than to functioning security measures. Every company has the need – and the right – to evaluate their cloud services in depth. Appropriate processes, competencies and financial means are still often lacking, but CISOs will need to get the cloud back under their control. Better sooner than later."

Tobias Höllwarth, President of EuroCloud Europe, Austria

During the three days, be prepared to put the human being at the heart of cybersecurity.

Welcome to FIC 2020.

Come and meet the Advisory Board members at the following sessions

Elly van den Heuvel-Davies,
Chairwoman of the FIC Advisory Board and Secretary to the Cybersecurity Council, The Netherlands

- **A27** - How can we combine security and corporate strategy?
- **Thursday 30 January 2020 14:00 - 15:30**

Phédra Clouner;
Deputy Director, Belgium Cybersecurity Center, Belgium

- **A05** - How far does a CISO's responsibility extend?
- **Wednesday 29 January 2020 11:30 - 13:00**

Tobias Höllwarth,
President of EuroCloud Europe, Austria

- **A18** - Cloud computing: how to manage hybrid clouds and multiclouds?
- **Wednesday 29 January 2020 13:45 - 15:15**

Alexander Klimburg,
Director, The Hague Centre for Strategic Studies, Austria

- **A06** - International negotiations and cyber diplomacy: from profusion to confusion?
- **Wednesday 29 January 2020 11:30 - 13:00**

Yugo Neumorni,
Chairman, European CIO Association, Romania

- **A15** - Data governance: what about security ?
- **Wednesday 29 January 2020 13:45 - 15:15**

Pascal Steichen,
CEO, SECURITYMADEIN.LU, Luxembourg

- **A12** - How can Executive Boards be fully involved in cybersecurity?
- **Wednesday 29 January 2020 13:45 - 15:15**
- **A24** - «Cyber insurance": inducing trust
- **Thursday 30 January 2020 14:00 - 15:30**

David Van Duren,
Head of Office, Global Forum on Cyber Expertise, The Netherlands

- **A20** - Capacity building: do we have the means to match our ambitions?
- **Wednesday 29 January 2020 13:45 - 15:15**

Lennig Pedron,
co-founder and President, ICON NGO

- **A03** - PhilosoFIC : la transformation numérique annonce-t-elle la déshumanisation de la société ?
- **Wednesday 29 January 2020 11:30 - 13:00**

FIC 2020

www.forum-fic.com