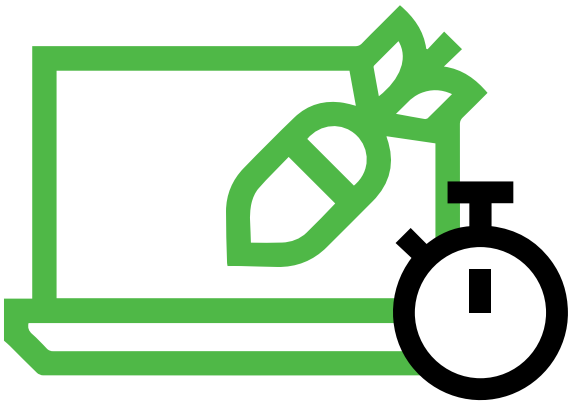
Ibec Global on Cybersecurity

Cyberattacks have emerged as major threats to businesses, civil society, democracy and security, undermining the very fabric of our societies. Enhanced international collaboration and strategic partnerships on cybersecurity are urgently needed to effectively tackle this scourge of the 21st century.

Why is this important and why now?

A cyberattack is estimated to occur every 39 seconds. Cybersecurity has never been of greater concern and urgency for every board, CEO and government than today. Organisations such as the WEF and Financial Action Task Force (FATF) have decried the extraordinary increase in cyber events, ransomware attacks and fraud. These have increased massively in the context of the pandemic-engendered acceleration of digital adoption. That rapid transition has exposed major cyber vulnerabilities, many associated with work-from-home protocols and often, unfortunately, corporate unpreparedness.

A cyberattack happens every 39 seconds



€5.5tn

The annual cost of cybercrime to the global economy

What is Ibec Global calling for?

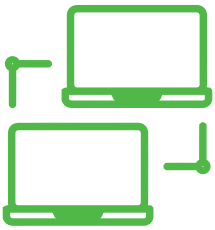
Ibec Global is focused on bringing people together to create a thriving world with a sustainable future. That future is dependent on increased cooperation on cybersecurity, not only from governments, but also business and other industry leaders. We all play a role in keeping our economies, societies, and relationships safe and secure. Ibec Global's purpose focuses on four key elements, each of which are affected by lapses in cybersecurity. Ibec Global calls on business, civil society, governmental and international organisation leaders to drastically increase cooperation on cybersecurity to ensure that multilateralism can remain intact, to strengthen the digital economy, to improve global talent, and to allow us all to invest in a greener future.

What is Ibec Global's position?

Focused on enhancing collaboration for a sustainable future, Ibec Global recognised the need for business and government to prioritise cybersecurity and build a network of leaders working to make cybersecurity and cyber threat awareness mainstream. An increasingly connected world means that cybersecurity threats are almost always cross-border. The economic price of these attacks is clear. But the nefarious effects of cybercrime on businesses, society and strategic partnerships is as much an issue and is only beginning to be understood.

25bn

The number of connected devices expected by 2025



The multiple impacts of cybercrime underscoring the urgent need for action

Economic

Only two years ago major cyber-attacks were big news, rare events even. Today they are everyday occurrences and no longer attract big headlines – but the losses involved are staggering. The pandemic has no doubt exasperated the situation, with the annual cost of cybercrime growing and in 2020 this was estimated at EUR 5.5 trillion[1], the largest transfer of economic wealth in history.

Geopolitical

Geopolitical tensions continue to exacerbate the cyber arena. Cyberattacks on critical infrastructure such as energy, transport and water systems are growing in regularity. Attacks targeting political systems around the world to spread misinformation for ideological purposes are threatening geopolitical relationships and multilateralism. The sophistication of these attacks has suggested many are state sponsored, showing that while many attacks happen locally, there are global consequences.

Digital economy

Our data needs to be held securely, and our systems should be modernised. We need fail-safe mechanisms in place to ensure the security of our data. We need a shift in how cybersecurity is perceived and how it is integrated into business plans. Too often cybersecurity strategies are seen as an operating cost. However, they must be an integral part of every business's strategy. To better support the shift to an even more digital economy, investments in cybersecurity infrastructure should be made. This will help businesses to craft cyber strategies and will ensure that citizens' data is well protected from any attempted attacks.

Sustainability

Investing in digitalisation is an investment into a greener future, but it needs to be underpinned by strong cyber defence mechanisms. We see digitalisation as the key enabler to a sustainable future, but none of this can be possible unless we can ensure that systems and the data they hold are safe and secure. The above elements are all crucial to ensuring that our sustainable future is possible, by increasing multilateral cooperation, protecting critical infrastructure, and supporting businesses and citizens by giving them the skills they need to succeed safely in a digital world.

Societal

Surveys in both the EU[2] and US[3] have found that citizens lack confidence in the ability of authorities to protect their data or think that the government needs to improve its cybersecurity. With so much of our lives online, cybersecurity has never been more important. Victims of cybercrime often report feeling ridiculed and embarrassed, which in turn often impacts on their interpersonal relationships, and mental and physical health[4]. Victims often report that after experiencing online fraud their buying patterns change as they lose trust in online shopping, or they choose more frugal living[5].

Multilateralism

Cyberattacks often happen locally, but there are global consequences. We need to build an alliance of likeminded countries to tackle this problem effectively. Cyberattacks are a new type of warfare, and state sponsored cyberattacks are on the rise. Businesses and private citizens cannot be expected to face this kind of threat alone, and neither can entire countries. Global collaboration will further facilitate best practice sharing, rapid warning systems, and information sharing which can help better protect critical infrastructures.

Global talent + skills

To better protect these critical infrastructures and personal data we need to improve the IT literacy of our citizens and businesses. Human error is often seen as the dominant problem when it comes to cybersecurity.[6] We need to empower businesses and citizens with the skills, knowledge, and tools to protect themselves. As in-person services become increasingly diminished, especially in rural areas, we need to invest in adequate training so that citizens can access the services they need safely. We also need to support SMEs and other organisations that are equally affected by cybersecurity breaches but that might not have the tools at their disposal to prevent, identify, or solve them.

Ibec Global is the International Business Division of Ibec – Ireland's largest and most influential business representative organisation. Our purpose is to bring together key international stakeholders to debate and shape the trends and priorities critical to creating a successful, shared global economy and society. That means that at Ibec Global our work is squarely focused on bringing people together to create a thriving world, with a sustainable future. We do this by identifying and harnessing the international business trends and opportunities that drive growth for businesses; advocating for enlightened policies and models in the context of major societal, policy, geopolitical and business trends; and influencing the conditions and providing the support for businesses to thrive globally. We operate through collaborating in and developing new strategic international networks to enhance these opportunities that are going to define the direction of business in the future.

[1] European Commission, A cybersecure digital transformation in a complex threat environment - brochure
[2] Eurobarometer survey: Europeans' attitudes towards cyber security (cybercrime)
[3] The Hill - Poll: 77 percent say U.S. needs improvement in cyber security
[4] Leukfeldt, R., Notté, R. & Malsch, M. (2019). Slachtofferschap van online criminaliteit. Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit.
[5] Dewi Anggun Puspitarini, Prawira Aros Purnama, & Isti Riana Dewi. (2021). Fraud risk and trust on the intention to buy of e-commerce. Journal of Contemporary Accounting, 3(1), 45-52.
[6] B. D. Sawyer and P. A. Hancock, "Hacking the human: The prevalence paradox in cybersecurity," Hum. Factors, J. Hum. Factors Ergonom. Soc., vol. 60, no. 5, pp. 597–609, Aug. 2018.