The Digital Way of Working and Cyber Security

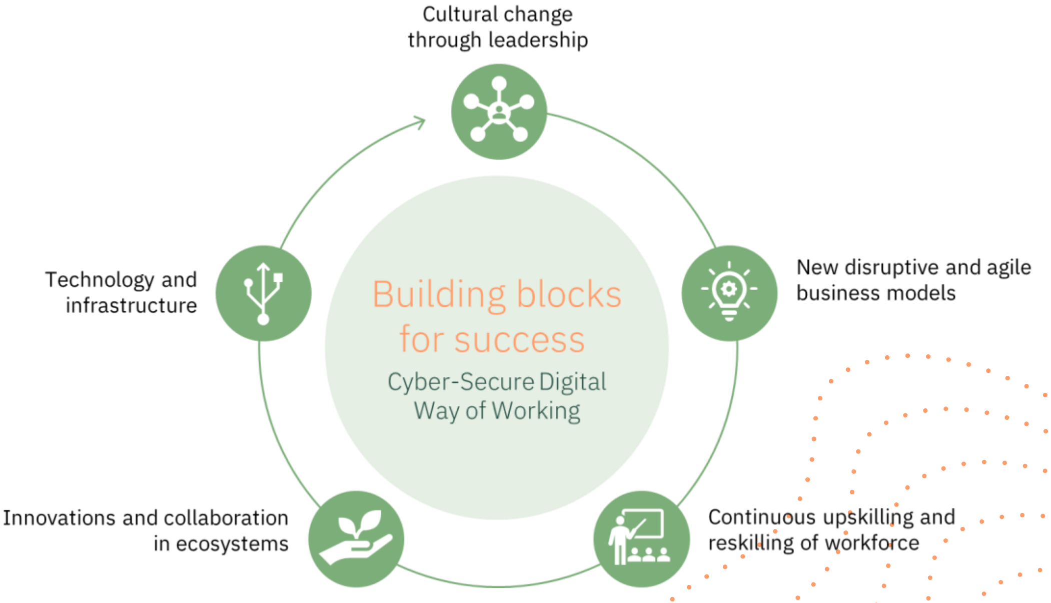
Report authors: ABB, Beweship, Cyberwatch, Danske Bank, DB Schencker, Ensto, Finnair, FISC, Fortum, F-Secure, Konecranes, Kreab, SOL, Staffpoint, Telia, Valmet, VTT & Confederation of Finnish Industries EK

Confederation of
Finnish Industries

The Digital Way of Working and Cyber Security – the Story

Digitalisation has changed our everyday working life and way of working. Digital tools and fast internet connections enable us to work remotely and operate at a distance and in multiple locations. The shift from traditional office work to hybrid work, combining remote and office work, has been speeded up by the Covid-19 pandemic. This change challenges us in many ways. New leadership skills are needed to adapt to new circumstances: How do we lead people whom we do not meet daily? How do we communicate and share information? Do we have the right skills and competencies to survive the competition and the rapid changes that are natural in a digitalising world? How much do we pay attention to secure ways of working and accessing sensitive data? Is cyber security an integral part of our digital way of working, and if not, what should we do to incorporate it? When more and more of our critical data is in the cyber domain, how do we secure it? The key question is how we lead the transformation to hybrid work and the digital way of working in the best and the most secure way.

To stay among the frontrunners, we need to quickly develop new business models and new, efficient ways of working. This requires changes in our traditional leadership models and management systems. The digital environment cannot be a substitute for human interaction and therefore it is essential to nurture well-being and human contact in digital working life.


Cultural change through leadership
Technology and infrastructure
New disruptive and agile business models
Building blocks for success
Cyber-Secure Digital Way of Working
Innovations and collaboration in ecosystems
Continuous upskilling and reskilling of workforce

The University of Vaasa has conducted research on the topic of remote work and on how to support the well-being of people who work remotely in organisations. They have identified three focus areas in which well-being should be developed: at the psychological, physical, and social levels. The work that Finnish frontrunner companies have done in Digital Game Changers supports the findings.

It is also important to remember that when we talk about digital development, we cannot do so in a sustainable way without talking about cyber security. Cyber security is an integral and critical part of digitalisation. Security cannot be considered 'later on'. It should play an integral role in all development – Security by Design – both in digital innovations and in a hybrid way of working.

The Digital Game Changers group recognised five major themes within the phenomenon of the digital way of working. The five themes are presented in more detail later in this report.

> Our key message is that The Digital Way of Working and Cyber Security are key business enablers and topics that should be high on the leadership's agenda and part of strategy discussions.

These five themes are:

1. Cultural change through leadership
2. New disruptive and agile business models
3. Continuous upskilling and reskilling of the workforce
4. Innovation and collaboration in ecosystems
5. Technology and infrastructure

This report is based on the work of frontrunner companies in Digital Game Changers. The group worked on the theme of 'The Digital Way of Working and Cyber Security' for about six months. The result came out of group work sessions and sharing the best practices of the participants. The goal of Digital Game Changers is to ensure that Finnish companies continue to lead the digitalisation change. Participating companies therefore want to share their findings, so that others can join the group of frontrunners. It is in everyone's best interests that Finnish companies succeed.

Building blocks for success

Cyber-Secure Digital Way of Working

Cultural change through leadership

- Change in leadership, management and mindset
- Continuous target setting and reviewing
- Agile performance management
- Cyber security as a strategic issue at top of management and board agenda
- Strategic situational awareness on cyber security
- Hybrid work

New disruptive and agile business models

- Flexible and adaptive models
- Sustainability as a driver
- Organisational processes adapted to the digital world
- Security by design in all processes and systems
- Digital solutions as enablers

Continuous upskilling and reskilling of workforce

- Lifelong upskilling and reskilling
- Self-leadership skills and mindset
- Ability to quickly learn new things and use new tools
- Digital and cyber security competencies on all levels
- Global talent pools and location-independent work

Innovations and collaboration in ecosystems

- New agile organisational culture, fail fast
- The increased importance of ecosystems
- New concepts and tools enabling innovation
- Established rules and routines: correctly timed meetings and efficient meeting protocols
- New growth and investment programme in cyber security

Technology and infrastructure

- Digital transformation starts with workflows that unite people and technology
- Cyber security as a critical technological enabler
- Digital platforms enabling new business models and innovations
- Cyber-secure connections in remote working
- AI and automation

The themes in the digital way of working and cyber security identified by frontrunners

1. Cultural change through leadership

Top management needs to show the way

Leadership is challenged by the rapid digitalisation following the Covid-19 pandemic. Remote and hybrid work challenge traditional leadership models and require a change of mindset. Human encounter and contact need to be supported in remote work. Employees should not feel isolated and must feel that the organisation supports them and that help is available when needed. Performance management will have to be more agile with continuous target setting and reviewing.

Hybrid working requires clear principles in the organisation. These principles need to be communicated well. This requires work from everyone in the organisation. Adopting agile working models and development sprints helps the organisation to keep up with current trends. Timely and effective meetings are needed, especially between supervisor and employee. Pulse meetings and frequent one-to-one meetings help with awareness of the targets at work but also give the supervisor information on how the employee is doing.

Employee well-being must also be ensured in hybrid mode. At times this can be challenging if we do not meet face to face, since in a remote world many difficulties can remain hidden. Employers need to make healthcare services, including mental health services, easily accessible for employees. There should also be monitoring to ensure that the number of working hours stays at a reasonable level. Employers should make sure that their procedures for dealing with symptoms of burnout, stress and other health issues are updated for the hybrid working world.

Employers should focus on building a culture of trust and psychological safety in their organisations. People who feel trusted and safe perform better. This also holds true for hybrid work. Trust helps to ensure that problems are brought to leaders at an early stage, before they have grown into bigger issues. Trust is also needed when working with partners, and a culture of trust in organisations helps with this.

Cyber security is an important enabler of the digital way of working and should not be seen as an afterthought. Situational awareness in leading cyber security is essential, and it needs to be up to date in both the public and the private sectors, in the government and companies.

We have a fairly solid foundation of operational situational awareness in relation to acute cyber security situation and detected vulnerabilities, but we currently lack a national cyber security risk analysis. Together, these would lead the way for strategic-level situational awareness, which would support decision-makers and enable more reliable, risk-conscious decisions. To achieve this, we would need a common platform, where information on phenomena in the cyber security world could be collected and shared from both the public and the private sectors, including from third-sector associations. The new digital way of working and cyber security needs to be on the daily agenda of the top management and should not be the responsibility of technical experts only.

Recommendation for business leaders: Define clear principles and rules for hybrid work and engage your managers and employees in drawing up these principles. The following areas need to be defined:

1. How remote and hybrid work will change leadership work and management systems (e.g. performance management, management forums, need for pulse meetings).
2. What principles, rules and contracts are needed for remote and hybrid work (e.g. insurances for homework, time management, common rules for remote work including cyber security).
3. What skills and competencies are needed.
4. What the impact is on the need for office space and workplaces, and how efficient ways of working for multilocation work can be developed.

Set clear goals for hybrid working that can be measured. Follow the KPIs and focus on effective pulse meetings to evaluate continuously whether targets are being met.

Make sure that cyber security is regularly on the agenda of the board and management teams on all levels.

Hybrid working models enable a better balance between working life and private life, which can flexibly support families so that everyday life runs more smoothly. Giving the option of hybrid work to employees can be seen as a competitive advantage when attracting the best talent.

Recommendation for policymakers: Hybrid and remote work will have an impact on work legislation and agreements because more local flexibility is needed. It is important to develop our policies for hybrid work.

Ensure that both the public and the private sectors have a shared operational situational awareness of the acute cyber security situation and detected vulnerabilities, and that we have a national cyber security risk analysis. Develop a common platform on which information on the phenomena in the cyber security world can be collected and shared from both the public and the private sectors, including third-sector associations.

Recommendation for employees: Lead yourself and do your part for your own well-being. Focus on self-leadership. Seek help and support. Play your part in cyber security. Take your time (avoid the trap of urgency). If you are uncertain, seek advice.

Recommendation for education: The digital way of working and cyber security should be a part of or a module in all business and leadership education and training programmes.

2. New disruptive and agile business models

Finland benefits from creating new models

Digitalisation enables new business models to be developed. In future, models must be flexible and dynamic to quickly adapt to changing customer requirements. New business models also ensure that all organisational processes are adapted for the digital world. New digital business models are the foundation for future success.

Sustainability and the green transition as business drivers will increase the importance of digital business models. Sustainable business models will gain advantages in the markets. Organisations need to develop sustainability strategies and their operations to meet the regulations and also to develop their brand and employee brand value.

The purpose of cyber security, as of all other elements of security and risk management, is to enable business and create the necessary trust. Digitalisation will not succeed or develop in a sustainable way without security requirements being considered. Security should be considered as a natural must-have element of the developed process, system, product or service by applying the Security-by-Design principle. Cyber security needs to be an integral part of business models and not just something that stands alone. Innovations need to be supported to meet the ever-changing needs of the customer.

Recommendation for business leaders: It is crucial to follow business model development both in the company's own branch and globally to ensure that the business model is up to date. Reskilling and upskilling can also be used as a tool for creating the competence to develop new models. Ensure that cyber security is part of the design of all digital processes and systems.

Recommendation for policy makers: Ensure funding for RD&I and business-driven ecosystems. Together we are stronger, and this also applies to the business world. Create permanent structures for public–private cooperation and collaboration when planning and designing cyber security policies and regulation.

Boost the data economy and enable the use of data with the help of MyData. This includes persons in public–private partnerships.

Recommendation for employees: Consider cyber security when creating new innovations, ways of working and doing business.

Recommendation for education: Support entrepreneurship and cooperate with innovative start-ups.

3. Continuous upskilling and reskilling of the workforce

The requirements for working competencies will change more than ever before

In a digitalised world, our needs for competence and capabilities are different from those in the pre-Covid world. The ability to quickly learn and adapt to new circumstances becomes increasingly important. As remote and hybrid work becomes more common, self-leadership skills are emphasised: to be effective, one must learn how to direct one's own tasks. Good self-leadership skills enable one to plan an effective way of working where the right tasks are prioritised. Resilience and adaptability are needed. Lifewide learning with continuous reskilling and upskilling will become more common in organisations, and the market value of employees who have their competencies and skills up to date will rise.

Learning in the workplace will be more important in the future. Learning at work is a planned and goal-oriented process, where skills and competencies are monitored and assessed. Reskilling and upskilling are important in a world that is continually digitalising. We need to adapt to continuous learning and the way to do this by reskilling and upskilling. Digitalisation also makes talent pools global, and recruitment can be globalised, since location does not matter in many work tasks and expert-level jobs. Talent management and learning will be integrated in companies.

Employees' knowledge about everyday security principles, protocols and practices should be enhanced. When we work in hybrid mode, the security knowledge and practices of employees become more important since we cannot always control our surroundings and who overhears our conversations. Continuous training in these subjects will therefore be essential in the future. This will establish a solid foundation for a sustainable security culture.

At minimum, everyone needs a basic cyber security understanding – what does cyber security require from me in my profession or as a citizen? Cyber security skills also need to be included in all levels of education: all the way from kindergarten to higher education and training in the workplace. In particular, coders, software architects and all those involved in service, product or process development need to have relevant cyber security skills. We also need to encourage more women and girls to choose cyber security as a career, as security considerations are relevant to all sectors of society.

The proposed National Cyber Security Development Programme for Finland recognises this and proposes that it be embedded in education at all levels, from kindergarten to vocational higher education and training, and also in higher education.

Both short-term continuous learning programmes and long-term education are needed. In a fast-paced world we cannot wait five years or longer for people with the right knowledge to graduate from universities or universities of applied sciences. We need new ways of finding people and their capabilities and matching them with the duty to be performed. One way to gain new knowledge is to utilise open learning platforms, for example FITech, which the Finnish universities have provided lately.

It is important that skills and competencies are developed in a sustainable way. Increasing only the student quota is not a sustainable solution: in the long run we cannot fill all the places with applicants from Finland. We need to increase the number of places for foreign degree students so that Finland could later benefit from their knowledge in the form of a competent workforce. A crucial part of having the best talent is to actively attract and recruit top talent from abroad to Finland. Being competitive on the global job market requires that the process of relocating to Finland be easy and relatively fast. We already have some fields of expertise where competence from abroad is desperately needed, for example cyber security.

Learning will more often take place at work and continuous learning will become the new normal. In education and training there is a need to invest in modular learning and rapid upskilling and reskilling of the workforce according to the new challenges of working life.

Recommendation for business leaders: Promote learning at work because that is the primary place for employees to gain new skills. Reskilling and upskilling at work should be a flexible, planned and goal-oriented process, where skills are monitored and assessed. By ensuring that your employees have the required skills and competencies, you can rely more strongly on the capability of agile working models to produce quality results. Develop modular and microlearning content to complement existing learning programmes and education. Ensure that all your employees have sufficient cyber security training and the skills they need in their role.

Recommendation for policymakers: Increase funding for lifelong, modular learning and other shorter education periods, e.g. microlearning. These should be available online in digital format to cover topics related to digitalisation and cyber security. Education needs to match the rapidly changing requirements of post-Covid working life. In particular, the amount of modular cyber security education should be increased. Raise the level of cyber security understanding and skills of policy makers and civil servants.

Recommendation for employees: Continuous learning is the key for individuals to operate in a digitalised world. Learning alongside your daily work is an essential way of reskilling and upskilling. This will increase your market value as an employee.

Recommendation for education: Education should invest more in lifewide modular learning and in providing upskilling and reskilling that supports the needs of working life. Education should respond to the needs of working life in an agile way to support lifewide learning. Stronger cooperation with leading companies is required to develop learning catalogues based on customer needs.

4. Innovation and collaboration in ecosystems

Hybrid ways of working challenge innovation

Innovation at work is challenged by remote work. When people do not meet each other physically daily, new tools are needed. New tools and concepts enable innovation together in a digital format. The organisational culture can also be adapted to support innovation processes. Well-established rules and routines in an organisation support innovation. Efficient meeting protocols, along with timely meetings, are needed to create an environment where innovation is possible. It is also important to remember that face-to-face meetings are essential and cannot be completely replaced by a digital format.

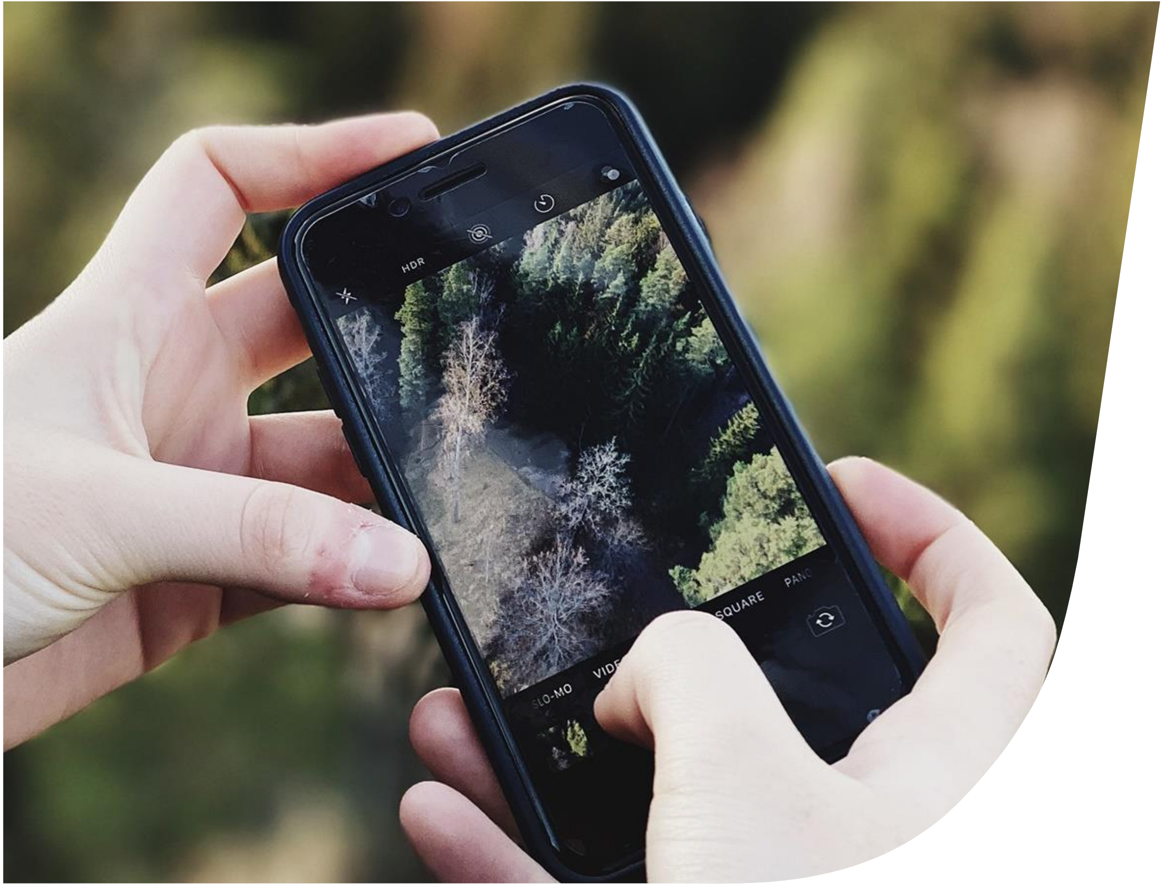
Cyber security is one of the areas in which Finland and Finnish technology companies could lead the world. To make this happen we should develop a national cyber security growth and investment programme and set up a national cyber security growth and skills centre. This would be of benefit not only to Finnish cyber security companies, but to all companies in Finland, including SMEs, by bringing the technological and funding needs together with companies capable of creating the products and services for global markets.

Innovation programmes that focus on the intersection of two strong megatrends, namely digitalisation and combating climate change, need to be a special focus in the Programme of Sustainable Growth. Financing instruments that already exist need to be used and developed in this context.

Working with partnerships in ecosystems can also boost innovation processes. New business ecosystems will be the working mode of the future. This model requires trust and understanding of your business partners. Everyone must feel that they give and gain equally in the project. Creating the framework for the project together gives it the legitimacy it needs. Ecosystems need a good facilitator for the ecosystem to succeed. Ecosystem development would also require new and more flexible funding instruments and support from the public sector.

A good way of supporting innovation is to adopt agile business and cooperation models. One such model worth mentioning is brainstorming and collaborating with start-ups. This way, larger, more established companies can adapt to the agile way of working in start-ups and start-ups can learn from the experience of larger companies, and everyone benefits.

As described above, creating an agile culture in the organisations is the key to supporting innovation. A new organisational culture fosters innovation.



Recommendation for business leaders: Create a culture that supports innovation and enables networking and information sharing. Create new ways of working that support innovation in an organisation that operates in the hybrid world. Make sure cyber security is considered in the early stages of the innovation process.

Recommendation for policy makers: Ensure that the RD&I ecosystems run by the government are productive in the digitalised world. Enable flexible funding models for ecosystem development.

Together with industry and academia, prepare a Cyber Security Growth and Investment Programme and set up a national Cyber Security Growth and Skills Centre to develop and support a strong national cyber security ecosystem prepared for global markets.

Recommendation for employees: Support the agile organisational culture with your own input. Be creative and willing to try new ways of innovating and developing new ideas in your team.

Recommendation for education: Universities should re-evaluate the content of education and refocus it to support the needs of working life. Universities should be active in research subjects that are relevant to industries in the long term. Universities should also participate in partnership models and engage in dialogue with companies.

5. Technology and infrastructure

Technology makes or breaks it

We could not work digitally without the necessary technology and infrastructure. Along with competence, this is the foundation for all digitalisation. A part of this foundation is cyber security, which must be integrated into the company's strategy and must run through all processes and systems to ensure security. Digital platforms are being used more and more, and they have also become a critical part of a company's business model. When processes are digitalised, it starts with workflows that unite people and technology.

Cyber security is not only about technology; to be efficient, security must be harnessed to ensure the confidentiality, availability and integrity of data, as well as the functioning and reliability of critical systems and infrastructure. Physical security must also be considered in order to ensure that data is secured.

Technology is the enabler for business models, but the business and strategy are the drivers. Only then can all processes and systems be established on a solid technological foundation.

Recommendation for business leaders: The technology architecture should support business processes and architecture, and business goals must be defined and kept in mind throughout the whole technology development process to ensure high-quality results. It is important to ensure and allocate adequate funds and resources for the necessary technological services and solutions.

Recommendation for policymakers: Infrastructure that functions well and is secure is the basis for the smooth running of all modern societies. It is important that choices of technology are defined by policy goals and decisions, and that adequate resources are allocated for the necessary technological services and solutions.

Recommendation for employees: Be open to new technology and sign up for training when it is provided in your organisation. You will benefit from being an early adopter of new technology.

Recommendation for education: Invest in digital learning environments and technologies. Augmented reality can help with learning and promotes new skills in the business world.

In addition: Working life is challenged by the changes brought by digitalisation

Digital working life is challenging us in many ways: in what tools we use, where we work and when we work. The five themes mentioned above disrupt the models and ways of working we are used to.

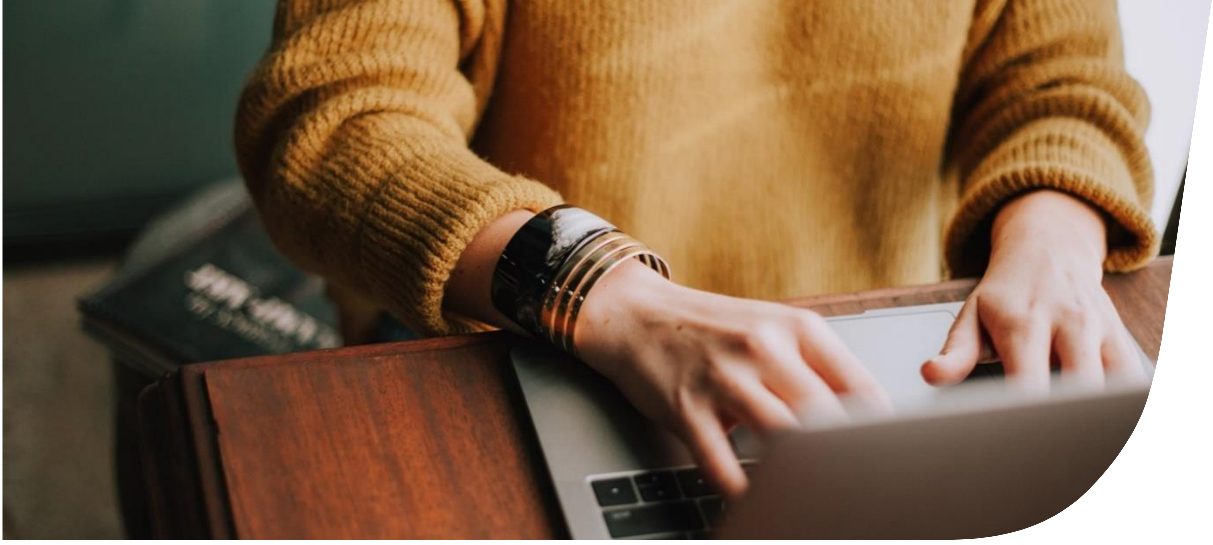
When we work from home or remotely, the normal office hours of 9 a.m. to 5 p.m. do not necessarily apply. We might do some work during the day and some in the evening, for example. In a working environment where location is not important, exactly when work is done loses its importance if the objectives and deadlines are met. In the future, many details related to work will be negotiated using local bargaining.

What will working life look like after Covid-19? Only time will tell, but there will be pressure to modify the Working Hours Act to match the current reality of working life. Collective agreements may also be amended accordingly and we may see a lot more local bargaining in the future. Thus, working models can be developed in an agile way to respond to our digital way of working.

Recommendation for business leaders: Companies should increase local bargaining because it enables flexibility in organisations.

Recommendation for policymakers: Covid-19 made hybrid working models mainstream in expert-level work. We should evaluate the Working Hours Act in order to better meet the needs of modern working life.

Recommendations for employees: Be active in your organisation and give feedback on what is, and is not, working. This way, working life can be improved for the better.



Checklist for Hybrid Work

When preparing for hybrid work, check the following in your organisation:

☑ Create principles for hybrid work

- defining roles and responsibilities
- when and where to work remotely
- meeting practices, availability
- safety, security including cyber security
- well-being

☑ Involve your teams and employees in the development

☑ Provide tangible checklists

☑ Educate and train your leaders in Hybrid Leadership

☑ Prepare to adapt based on experiences and changing situations

☑ Communicate, communicate, communicate!

Checklist for Cyber Security Leadership

☑ Create comprehensive and reliable cyber security awareness

☑ Ensure adequate capacity for cyber risk assessment and management

☑ Build an agile cyber preparedness and continuity plan

☑ Create well-trained cyber crisis management competence

☑ Build superior cyber competence in the human sector

☑ Procure superior cyber technologies – make smart choices

☑ Allocate an adequate cyber budget

☑ Build an agile and comprehensive cyber culture.