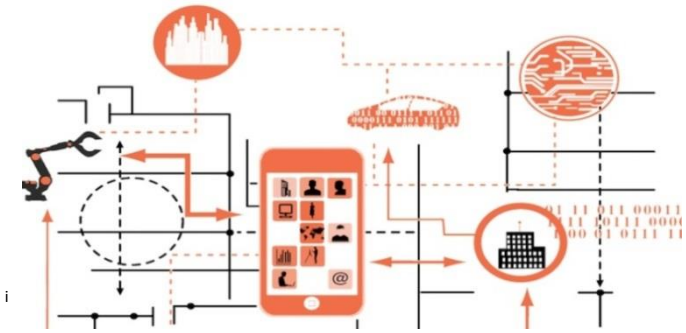
"Employers ensure the health and safety of their employees with regard to every work-related aspect. Have you also organized your cyber security for computer-operated work equipment?"



Thanks to the introduction of ICT systems that are embedded in the operation mechanisms of work equipment via local networks and public networks like the internet, businesses and organizations have been able to make great strides in terms of efficiency. However, these developments also entail new threats and vulnerabilities. Not the least of these is the possibility that individuals or malware could gain unauthorized access to business systems and networks in the work environment and disrupt them in a way that creates hazardous situations. The complexity of the issue is often underestimated, which means that the measures taken in anticipation of possible unexpected disruptions resulting from such complexity are inadequate. In spite of this, there are many companies and organizations where this risk is not recognized. Given the rapid developments in technology and the increasingly strong links between systems and processes, it is only a matter of time before a serious disruption occurs. Prevention is better than cure. As one of the actors in the lifecycle of work equipment, the ball is now in your court!

What are the risks that businesses and organizations face?

- Process disruptions threaten business continuity and controlled production.
- Employees could be injured or killed as a result of an unsafe situation caused by an accidental cyber disruption or by hacking, malware or signal disruption – there is also the related financial damage (such as sick pay costs and sickness-related absenteeism).
- Access can be gained to processes and machines through coercion (such as physically threatening employees or creating access points through 'phishing').
- Reputational damage as a result of publicly visible incidents (such as those that result in victims).

Table 1. What are the vulnerabilities that increase the risk?

Vulnerabilities	Explanatory notes
Communication	Managers and engineers do not speak the same language. As a result, this often places limitations on any shared insights and communications between security (ICT) employees and operational employees or safety experts in relation to technical risk aspects (including cyber aspects) of employee safety.
Costs of cyber security	The current competitive market ensures that SMEs in particular invest hardly anything in cybersecurity in relation to employee safety, and instead focus on functionality (that is, they want a crane that can move a container from A to B, while the cyber security aspects are of secondary importance). The same applies to manufacturers and system integrators. An underlying factor is that there have been very few (as far as the public are aware, at least) incidents that have affected employee safety, and that there are very few people who emphasize the urgency of investing in cybersecurity.
Fast-moving developments	Fast-moving technological developments mean that software and cybersecurity quickly render the safety of work equipment outdated. Moreover, processes controlled and operated (24/7) by ICT are becoming more and more complex.
Outdated risk management	Despite the ever-closer linking of systems and processes, there is still a widespread tendency to view risk factors from separate angles (for example, maintenance versus implementation, safety versus security, or employees versus management). However, this is an outdated paradigm; what is needed is integrated risk management. Awareness and overview of the interrelationship between the technical systems and of the actors involved in threats and the provision of safe solutions are lacking.
Lack of cyber-situational awareness	Cyber-situational awareness levels are still relatively low in most organizations. There is also a reluctance to share incidents with other parties, from which lessons could be learnt. A law obliging companies to report data leaks took effect on 1 January 2016.
Unconsciously incompetent	Unconsciously incompetent employees who affect machine software without realizing it, and therefore undermine control measures that have been implemented. Current risk analyses often fail to factor in this aspect, assuming that all employees are aware of what they are doing.

Table 2. Measures for minimizing the risk

Life cycle	Control measure
Design	✓ Intrinsically safe design (governed by technical standards). ✓ Integrated security risk inventory and risk evaluation throughout the lifestyle of the work equipment. ✓ Designs aimed at fail safe/safe fail and damage control when exposed to cybercrime.
Production, supply, and installation	✓ Suppliers and service providers (for maintenance, for example) supply secure-out-of-the-box products. ✓ System integrators and installers supply Industrial Control Systems (ICS) that are integrated and secure. ✓ Cyber security is an integrated part of the acquisition process and the test phase of products and services. ✓ Set down the security of information and other systems or components in contracts with suppliers.
Use	✓ Integrated and multidisciplinary risk management. ✓ Safety management and safety culture to be based in part on cyber security. ✓ Add cyber security aspects to work safety rules of conduct /protocols regarding dealing with ICS and other internal systems. ✓ Cyber security procedures for keeping ICS and networks secure. ✓ Hardening of ICS and minimizing interfaces. ✓ Provision of information on the risks and desired behaviour for employees (including temporary employees) and suppliers/contractors. ✓ Training and refresher training for employees on dealing with ICS. ✓ Monitoring ICT network anomalies (by auditing, for example).
Use	✓ Develop policy for internally and externally sharing cyber security-related information. ✓ Add cyber security aspects to work safety rules of conduct /protocols regarding dealing with ICS and other internal systems. ✓ Screening of internal employees. ✓ Integrated approach to incident management (safety and security). ✓ Set up emergency organization that anticipates and responds quickly to any cybercrime threat.
Maintenance	✓ Set up maintenance services according to control - based on integrated security. ✓ Malware detection policy and implementation: ensure prompt and up-to-date malware detection. ✓ Identifying unauthorized access attempts in systems during maintenance. ✓ Patch policy and implementation: patching in time (for example, carrying out updates at a manageable scale). ✓ Checks on access and work activities by internal employees and third parties during maintenance. ✓ Testing / preventing new security leaks by installing new components.
Innovation	✓ Ensure a management or change process based on integrated security. ✓ Ensure future solutions: encourage research and development in order to renew the current status of science and technology in the field of cyber security. ✓ Testing / preventing new security leaks by introducing new work equipment.
Remove	✓ Remove sensitive configuration and other information and involve reliable parties. ✓ Put outdated or equipment and systems that are no longer suitable out of use

Important actors and information sources for prevention

- The parties involved in cyber security and safety in the lifecycle of work equipment
- Knowledge institutes and knowledge points (such as ncsc.nl)
- Insurance companies
- Trade associations (sharing information, developing knowledge, developing guidelines)
- Government bodies and normalization institutes (norm frameworks, national and international legislation)

Steps for dealing with the risk, from the perspective of businesses

- Ensure coordination of integrated safety and cyber security at boardroom level in one portfolio – by a Chief Information Officer, CEO, or other top-level office holder.
- Create a multidisciplinary team to hold integrated evaluations of cyber security-related work risks, emphatically including the human factors, observing incidents, and taking emergency measures if necessary.
- Analyse where network links between work equipment and 'risky' internal and external environments are at present.
- Ensure that knowledge is shared, good practices are exchanged, and warn each other of incidents and threats.
- Anticipate changes to work equipment and the link between work equipment and ICS and public and other networks with the help of integrated security analyses and product requirements.
- Incorporate safety and cyber security in designs, system integration, and supplies, or when giving orders in relation to these areas, such as carrying out maintenance. Take account of the various interrelationships (such as system architecture or relevant actors).
- Make sure that all parties involved are aware of the importance of taking an integrated approach to work safety and cyber security. If necessary, give refresher training to relevant people (management, employees, those who implement).

[i] Source picture: Bloem, van Doorn, Duivestein, van Manen, van Ommeren (2013). Things: Internet of Business Opportunities. *VINT research report 1 of 4. http://www.fr.sogeti.com/globalassets/global/downloads/reports/vint-research-1-things-internet-of-business-opportunities.pdf*