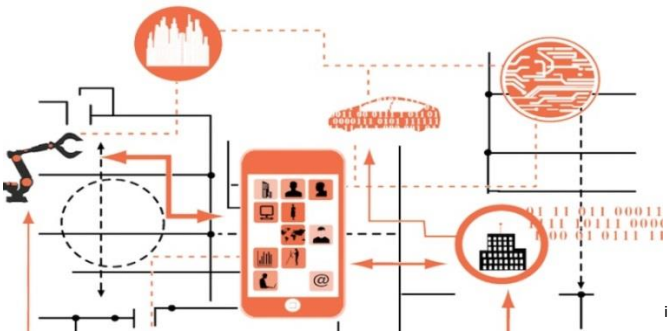
"De werkgever zorgt voor de veiligheid en de gezondheid van de werknemers inzake alle met de arbeid verbonden aspecten. Heeft u uw cybersecurity ook geregeld voor computergestuurde arbeidsmiddelen?"



Dankzij de introductie van ICT-systemen ingebed in de besturing van arbeidsmiddelen via lokale netwerken en publieke netwerken zoals het internet hebben bedrijven en organisaties grote stappen kunnen zetten in termen van efficiëntie. Deze ontwikkelingen brengen echter ook nieuwe dreigingen en kwetsbaarheden. Vooral de mogelijkheid dat individuen of malware ook ongeautoriseerd toegang krijgen tot bedrijfssystemensystemen en netwerken in de arbeidsomgeving en deze dusdanig ongeautoriseerd verstoren dat er een arbeidsonveilige situatie optreedt. Ook wordt de complexiteit vaak onderschat en wordt er daardoor onvoldoende geanticipeerd op mogelijke onverwachte storingen als gevolg van die complexiteit. Toch wordt er in veel bedrijven en organisaties dit risico nog niet onderkend. Gezien de snelle technologische ontwikkelingen en de toenemende verbondenheid van systemen en processen is het echter een kwestie van wachten tot het een keer goed fout gaat. Voorkomen is beter dan genezen. U, als een van de actoren in de levenscyclus van arbeidsmiddelen, bent aan zet!

Wat zijn de risico's voor bedrijven en organisaties?

- Procesverstoringen bedreigen business continuity en beheerste productie.
- Medewerkers met letsel of dood ten gevolge van een arbeidsonveilige situatie door onbedoelde cyberverstoring of door hacking, malware of signaalverstoring, en daarbij komende financiële schade (e.g., ziektekosten en verzuim).
- Via chantage kan toegang tot proces en machines worden afgedwongen (e.g., fysieke bedreiging medewerkers of creëren van access point via 'phishing').
- Imago schade ten gevolge van voor publiek zichtbare incidenten (e.g., waarbij slachtoffers te betreuren zijn).

Tabel 1. Wat zijn kwetsbaarheden die de kans op het risico vergroten?

Kwetsbaarheden	Toelichting
Communicatie	Bestuurders en technici spreken een andere taal. Hierdoor is het gedeelde inzicht en onderlinge communicatie tussen (ICT) security en operationeel personeel of veiligheidskundige over (cyber)technische risicoaspecten voor arbeidsveiligheid, als die er al is, vaak beperkt.
Kosten cybersecurity	De huidige concurrentiemarkt zorgt er voor dat met name het MKB nauwelijks investeert in cybersecurity in relatie tot arbeidsveiligheid en in plaats daarvan focust op functionaliteit (i.e., men wil een kraan die een container van A naar B kan verplaatsen, de cybersecurity is van ondergeschikt belang). Hetzelfde geldt voor fabrikanten en systeemintegratoren. Onderliggende factor is dat er nog maar weinig (publiekelijk breed bekende) incidenten zijn geweest met impact op de veiligheid van medewerkers en personen die de urgentie van investeringen in cybersecurity vergroten.
Snelle ontwikkelingen	Snelle technologische ontwikkelingen zorgen er voor dat programmatuur en cybersecurity de veiligheid van arbeidsmiddelen snel veroudert. Daarnaast neemt de complexiteit toe van ICT-gecontroleerde en bestuurde (24/7) processen.
Achterhaald risicomanagement	Ondanks de toenemende verbondenheid van systemen en processen, wordt nog te vaak geprobeerd om vanuit gescheiden invalshoeken naar risicofactoren te kijken (e.g., onderhoud versus uitvoering, safety versus security, of staf versus management). Dit is echter een verouderd paradigma. Een integraal risicomanagement is noodzakelijk. Ook ontbreekt vaak een bewustzijn en overzicht van de samenhang van de technische systemen alsook de actoren die bij het bedreigen/zorgen voor veilige oplossingen een rol spelen.
Ontbreken cyber-situational awareness	De cyber-situational awareness is nog betrekkelijk laag bij de meeste organisaties. Daarnaast is er schroom incidenten te delen met anderen om ervan te kunnen leren. Per 1 januari 2016 gaat een wetsvoorstel in die bedrijven verplicht stelt om datalekken te melden.
Onbewust onbekwaam	Onbewust onbekwame medewerkers die onbewust invloed uitoefenen op machine programmatuur en daarmee geïmplementeerde beheersmaatregelen teniet doen. Huidige risicoanalyses nemen deze factor vaak niet mee en gaan uit van de juiste intentie in handelen van hun medewerkers.

Tabel 2. Maatregelen om het risico te minimaliseren

Levenscylus	Beheersmaatregel
Ontwerp	✓ Intrinsiek veilig ontwerp (gestuurd door technische standaarden). ✓ Integrale veiligheidsrisico -inventarisatie en -evaluatie over de gehele levenscyclus van het arbeidsmiddel. ✓ Ontwerpen gericht op fail safe/safe fail en damage control bij blootstelling aan cybercrime.
Productie, leverantie en installatie	✓ Leveranciers en dienstverleners (bijvoorbeeld voor onderhoud)leveren secure-out-of-the-box producten. ✓ Systeemintegratoren en installateurs leveren Industrial Control Systems (ICS) integraal veilig op. ✓ Cybersecurity is integraal deel van het verwervingsproces en de testfase van producten en diensten. ✓ De beveiliging van (informatie-) systemen of componenten contractueel vastleggen met (toe)leveranciers.
Gebruik	✓ Integraal en multidisciplinair risicomanagement. ✓ Veiligheidsmanagement en veiligheidscultuur mede richten op cybersecurity ✓ Arbeidsveiligheidsgedragsregels/protocollen omtrent omgang met ICS en andere interne systemen met cybersecurity aspecten aanvullen ✓ Cybersecurity procedures om ICS en netwerken veilig te houden. ✓ Hardening van ICS en minimalisatie koppelvlakken. ✓ Voorlichting risico's en gewenst gedrag onder (tijdelijke) medewerkers en leveranciers/contractors ✓ (Bij)scholing personeel voor omgang met ICS. ✓ Toezicht op ICT-netwerkanomalieën (bijv. auditing).

Levenscylus	Beheersmaatregel
Gebruik	✓ Ontwikkel beleid voor het intern en extern delen van cybersecurity-gerelateerde informatie. ✓ Arbeidsveiligheidsgedragsregels/protocollen omtrent omgang met ICS en andere interne systemen met cybersecurity aspecten aanvullen ✓ Screening eigen personeel ✓ Integrale aanpak incidentmanagement (safety en security) ✓ Bedrijfs(nood)organisatie ook inrichten op anticiperende en snelle response bij cybercrime dreigingen.
Onderhoud	✓ Onderhoud(services) mede inrichten op beheersing vanuit integrale veiligheid ✓ Malware detectiebeleid en -uitvoering: zorgen voor tijdige actuele malware-detectie. ✓ Signaleren van pogingen tot inbraak in systemen tijdens onderhoud. ✓ Patchbeleid en -uitvoering: tijdig patchen. (bijv. updates op beheersbare schaal uitvoeren) ✓ Controle op toegang en werkzaamheden eigen medewerkers en derde partijen bij onderhoud. ✓ Testen / voorkomen nieuwe beveiligingslekken door installatie nieuwe componenten.
Vernieuwing	✓ Zorgen voor een management of change proces gebaseerd op integrale veiligheid. ✓ Zorgen voor toekomstige oplossingen: research en ontwikkeling stimuleren t.b.v. vernieuwing van de huidige stand van wetenschap en techniek op het gebied van cybersecurity. ✓ Testen / voorkomen nieuwe beveiligingslekken door binnenbrengen nieuwe (functionaliteiten van) arbeidsmiddelen.
Afvoeren	✓ Verwijderen gevoelige (configuratie)informatie en inschakelen betrouwbare partijen. ✓ Verouderde of niet meer geschikte installaties of systemen onbruikbaar maken

Belangrijke (actoren en) informatiebronnen voor preventie

- De uitvoerendenbetrokkenen bij cybersecurity en veiligheid in de levenscyclus van arbeidsmiddelen
- Kennisinstituten en kennispunten (bijv. ncsc.nl)
- Verzekeraars
- Brancheverenigingen (informatie delen, kennis ontwikkelen, richtlijnen ontwikkelen)
- Overheden en normalisatie-instituten (normkaders, (inter)nationale regelgeving)

Stappen om het risico aan te pakken vanuit bedrijfsperspectief

- Zorg voor coördinatie van integrale veiligheid en cybersecurity op boardroomniveau in één portefeuille bijvoorbeeld op topniveau bij een Chief Information Officer of CEO.
- Zorg voor een multidisciplinair team dat het cybersecurity-gerelateerde risico voor arbeidsveiligheid integraal evalueert en daarin de human factors nadrukkelijk meeneemt, incidenten waarneemt en zo nodig noodmaatregelen kan treffen.
- Analyseer waar in het hier en nu netwerk koppelingen tussen arbeidsmiddelen en "risicovolle" interne omgevingen en buitenwerelden zijn.
- Zorg voor het delen van kennis, wissel good practices uit en waarschuw elkaar over incidenten en dreigingen.
- Anticipeer op veranderingen van arbeidsmiddelen en de koppeling van arbeidsmiddelen met ICS en (publieke) netwerken, door middel van integrale veiligheidsanalyses en producteisen.
- Neem veiligheid en cybersecurity mee in ontwerp, systeemintegratie en levering of het geven van opdrachten hiertoe zoals het uitvoeren van onderhoud. Neem daarbij de onderlinge samenhang (bijvoorbeeld systeemarchitectuur of relevante actoren) in acht.
- Zorg voor bewustwording bij alle betrokkenen van het belang van een integrale behandeling van arbeidsveiligheid en cybersecurity. School mensen (in management, staf en uitvoering) zo nodig bij.

[i] Bron Plaatje: 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*