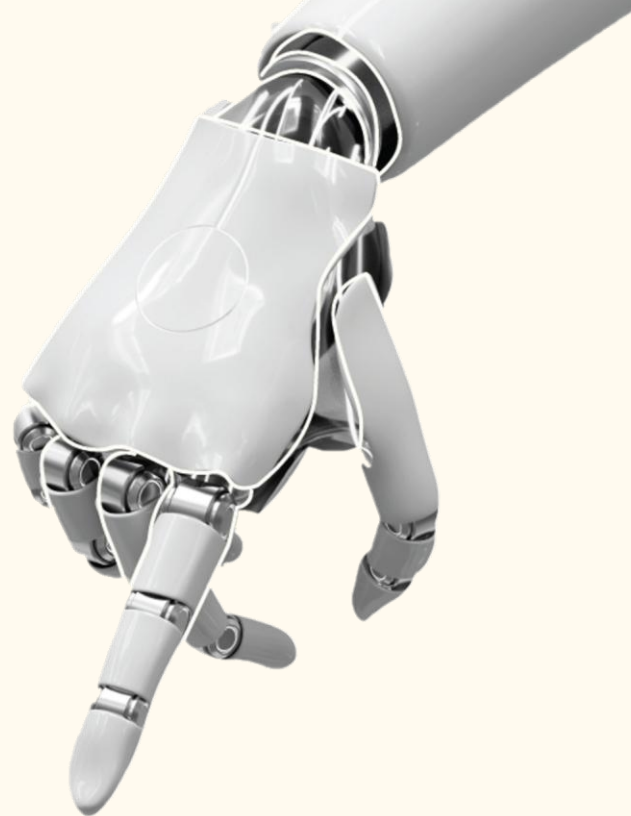
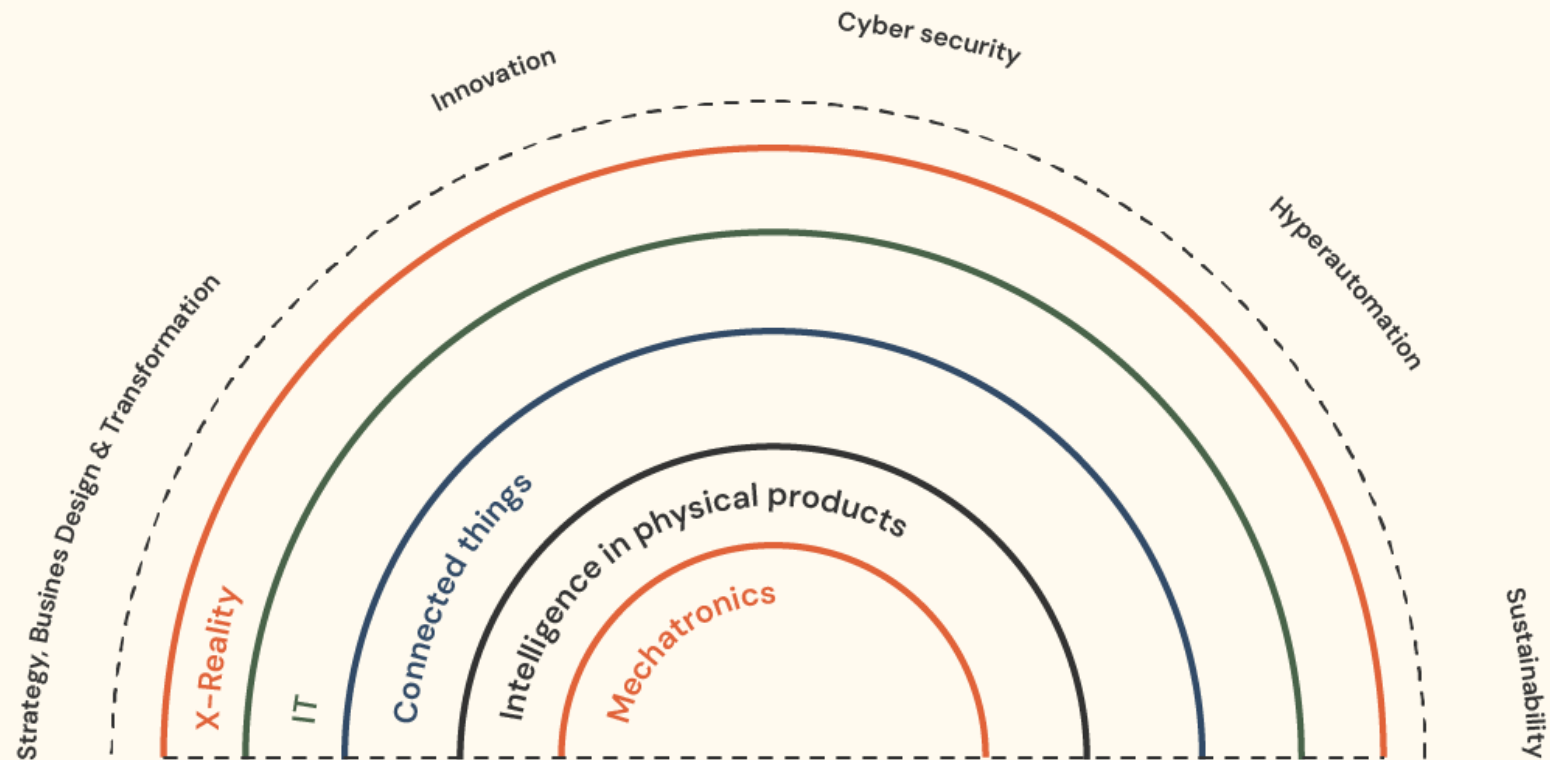




TechSeed

Cyberrisker och cybersäkerhet inom livsmedelsindustrin

TechSeed develops the digiphysical network



Vem är Carl-Göran Domeij

Ingenjör



Cyber-Risk Specialist



Datanörd - nej

IT-Revisor



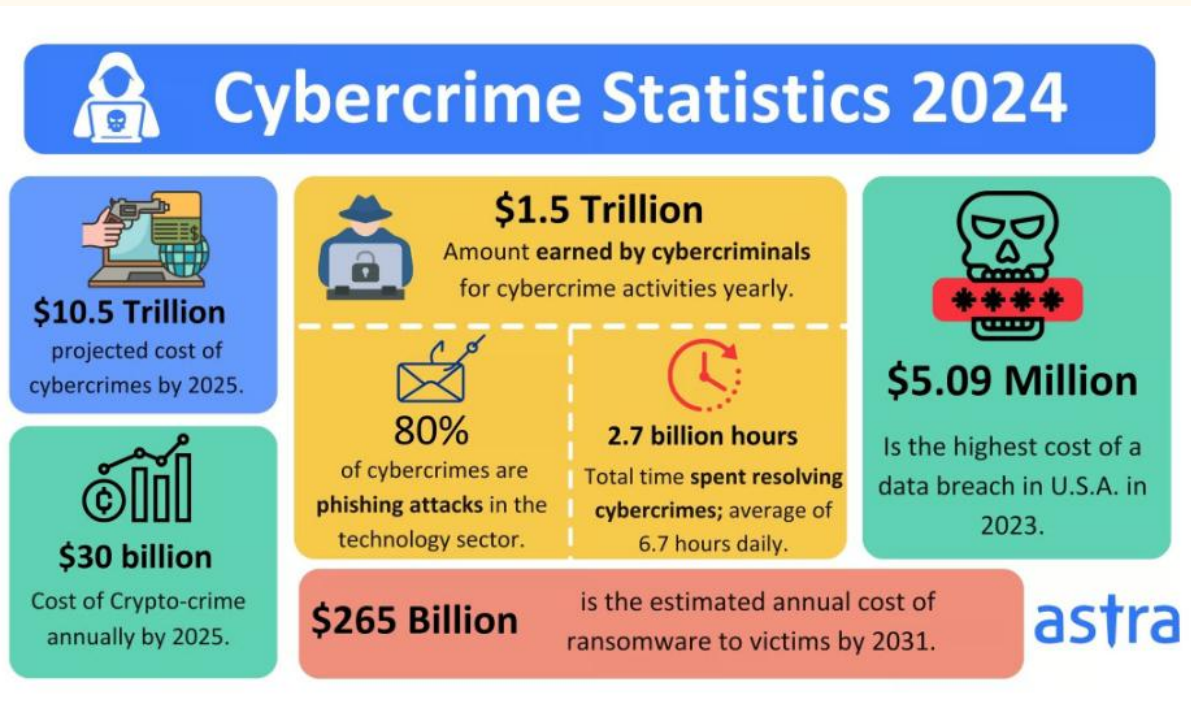
Sweden Food Arena - Ambition



- ✓ Ökad effektivitet
- ✓ Högre innovationstakt
- ✓ Stärkt konkurrenskraft



"Cybercrime arean"



Cyberbrottens "ekonomi" består av:

- Ransomware (utpressning med krypterad data)
- Phishing och bedrägerier
- Stulna kreditkort och identiteter
- Datastöld och försäljning på dark web
- Hackade molntjänster
- Cyberterrorism
- Illegala kryptovalutatransaktioner
- DDoS-attacker mot företag och statliga system

Intressanta fakta

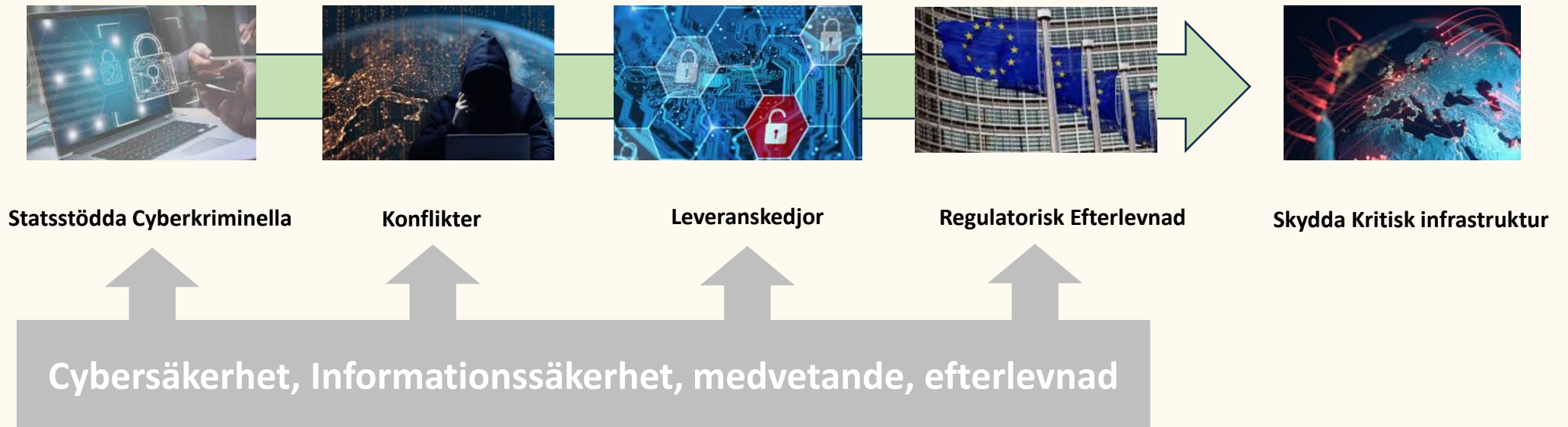
- Att tidsmässigt lösa inträffade cyberincidenter tar tid. Sammanlagt per år= 2,7 miljarder timmar
- Cyberattacker kostar världen mer än droghandeln.
- Den största delen av all malware (skadlig kod) anpassar sig för att vara svårare att upptäcka.
- Sverige är ett av de länder som drabbas hårdast av ransomware

källa:
<https://www.getastra.com>
<https://comprd.com/>

Livsmedelsbranschen och Cyberrisker ?

TechSeed

livsmedelssäkerhet och samhällsberedskapsperspektiv !



Låt oss titta lite närmare - Cyberkriminella

Cyberkriminella



Cyberkriminella har funnits i olika skepnader så länge det funnits digitala hjälpmedel

I dagens komplexa IT-strukturer finns incitament till finansiella möjligheter

- Utpressning (Ransomware)
- Stjäla information (Recept, produktionssiffror, förberedelse för nästa steg)
- Jobba i symbios med nationella stater...



Låt oss titta lite närmare - Konflikter

Konflikter och Statsstödda cyberkriminella



Utnyttjande av cyberrelaterade medel som förberedande för eller under en pågående konflikt

- Förstöra - fabriker, infrastruktur, kommunikationsvägar,
- Skada - människor, fysiskt
- Missleda – lura, förvilla eller skapa opinion
- Inhämta information- Underrättelser, Spionage, dataläkage (IPR)



Låt oss titta lite närmare - Leveranskedjor

Leveranskedjor



I leveranskedjor ingår ofta 3-partsleverantörer, "supply-chain"

- Digitala system som används av logistikföretag, jordbrukare eller distributörer kan vara **ingångspunkter** för attacker.
- SW supply Chain Attack, HW Supply attack

Livsmedelsindustrin är beroende av digital spårbarhet (ex. batch-nummer, ursprung).

- Angrepp kan göra att **falsk information** sprids – t.ex. märkning av kött som ekologiskt när det inte är det.



Konsekvenser in om produktionsprocessen



Beroende av IoT och smarta sensorer

- Angrepp på sensorer som mäter **temperatur, fukt, rörelser** i lager etc.

Produktionsstopp genom attacker på OT/ICS

- Moderna livsmedelsfabriker är beroende av **automatiserade styrsystem** Angrepp kan **stoppa produktionen**, orsaka matsvinn, eller förstöra lager.

Manipulering av recept och produktion

- Om någon får åtkomst till receptsystem kan ingredienser ändras – med risk för **felaktiga produkter eller allergener**.

Typer av konsekvenser

Konsumenters hälsa

Varumärkes skador

Felaktiga produkter

Allergener

Förstöra funktioner (tex kylkedjan för känsliga livsmedel)

Matsvinn

Lite om – Regulatorisk Efterlevnad



Regulatorisk Efterlevnad

Nya krav på cybersäkerhet i form av direktiv och lagar kommer bli vanligare

- Många av dess är överlappande
- Svårt att se vilka som är applicerbara
- Flera av dessa kan leda till böter om man inte efterlever dem

BRCGS, ISO 22000 –

- kan kräva cybersäkerhetsåtgärder för spårbarhet.

FDA (USA) Food Safety Modernization Act (FSMA) – kräver IT-säkerhetsrutiner.

GDPR EU:s Dataskyddsförordning 2016/

AI-act förordningen 2024/1689 om artificiell intelligens

Säsksl Säkerhetsskyddslagen (2018:585) nationell säkerhet

NIS2 Direktiv 2022/2555 om hög gemensam cybersäkerhetsnivå i hela unionen (impl SOU 2024:18 -CSL)

CER direktiv 2022/2557 om kritiska entiteters motståndskraft

Ge stöd för ny säkerhetslagstiftning

DORA Digital Operational Resilience Act 2022/2554 finanssektorn

CRA Cyber Resilience act 2022/0272 om produkter med digitala element

CSA Cyber Security Act 2019/881 om Enisa och certifiering

CSoA Förslag till förordningen att stärka solidariteten och kapaciteten att bekämpa cyberhot

Data Act Förordning 20223/2854 harmoniserande regler för skäligen åtkomst till och användning av data

DGA Data Governance Act 2018/1724 offentliga sektorns dataförvaltning

DMA Digital Markets Act 2022/1925 om öppna och rättvisa marknader inom digitala sektorn

DSA Digital Services Act 2022/2065 om inre marknad för digitala tjänster

eIDAS Förordning 910/2014 om elektronisk identifiering och betrodda tjänster

E-Privacy Förslag till förordning om integritet vid elektronisk kommunikation

Open Data Directive 2019/1024 om öppna data och vidareutnyttjande av information från den offentliga sektorn (impl lag 2022:818)

Nationell Strategi för Cybersäkerhet

Hur och vad? För att agera och skydda sig

Förstå era sårbarheter

Genomför riskanalys och prioritera vad som är mest viktigt utifrån konsekvens

Jobba systematisk med frågeställningarna, (lägg inte för stor vikt på att köpa in IT-säkerhetsprodukter innan ni vet exakt vad ni vill ha)

Säkerhet i Försörjningskedjor

Utför **leverantörsgranskningar** och ställ **säkerhetskrav** i avtal.

Behandla t.ex. externa logistiksystem eller fjärråtkomst till kylaggregat som särskilda riskpunkter.

Skydd av recept och processdata

Skydd krävs genom kryptering, accesskontroll och loggning.

Säkerställ att endast behöriga personer kommer åt dessa data

Tillgänglighet som topprioritet

Produktion är ofta kontinuerlig och känslig för avbrott (kylda varor, hygienkrav, etc.).

Satsa på resiliens och backup för produktionssystem, inte bara för data.

Implementera UPS (avbrottsfri kraftförsörjning) och redundanta system.

Icke att förglömma....

Fysisk säkerhet och insider-risker.

Se till att ha säker hantering av passage och lokaler. Det finns alltid medarbetare som cyberkriminella kan styra

Se även utanför "boxen"

TACK! - Följ, skapa kontakt eller ställ frågor

TechSeed



www.linkedin.com/in/carlgorandomeij

