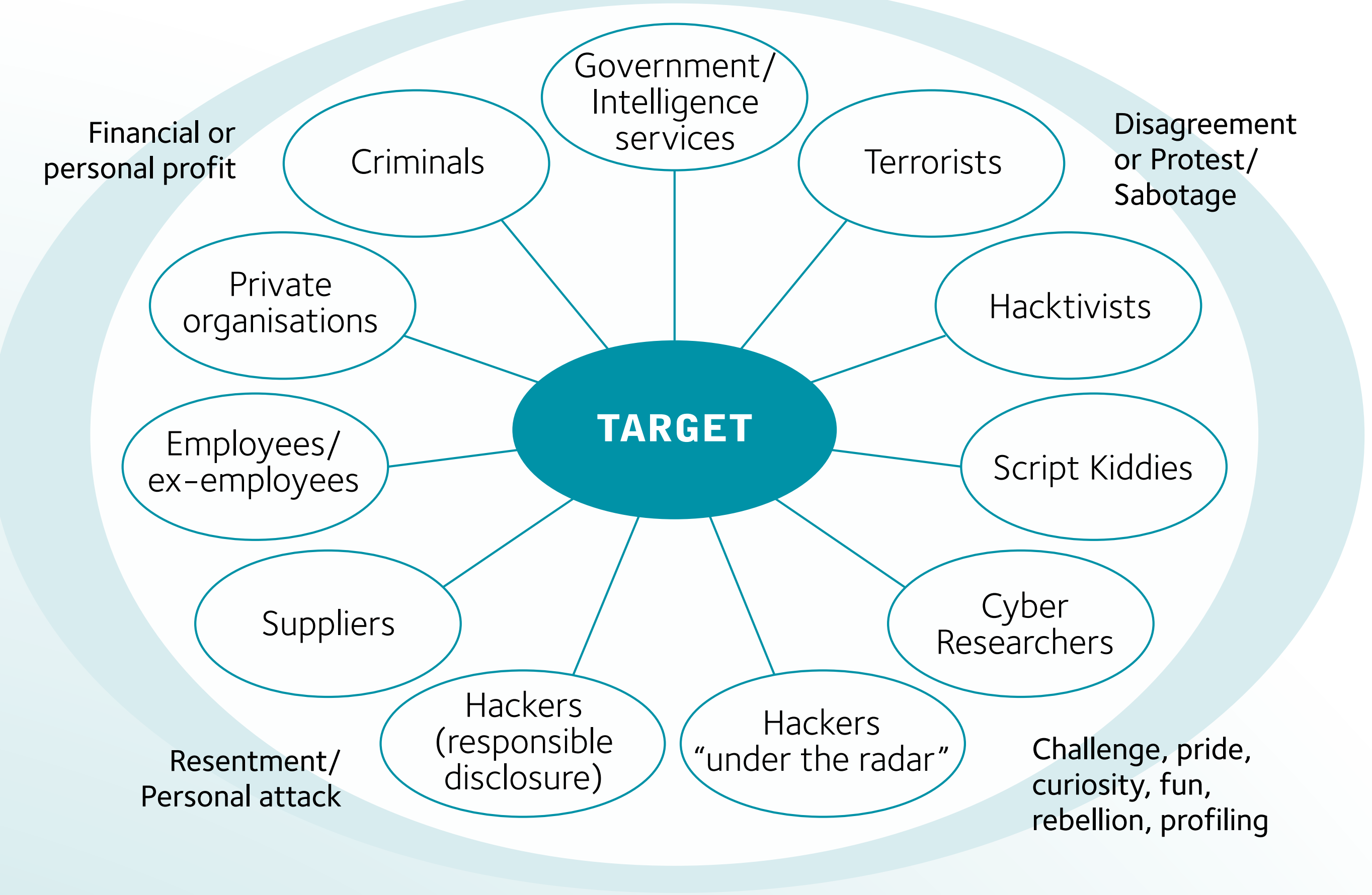
BOARD OF DIRECTORS INTEREST

- SAFETY: Prevention of casualties
- CONTINUITY: Prevention of production outages
- COMPLIANCE: Legislative and regulatory focus
- INTEGRITY: Prevention of unwanted modification
- QUALITY: Prevention of recovery or recall actions
- TRUST: Prevention of reputational damage
- AGILE: Attention to Supply Chain dependency

SOCIAL VALUES

- Risk-avoidance for customers
- Safe production and production processes
- Prevention of unwanted modification in products: no health risks
- Prevention of large scale economic damage
- Avoidance of social disruption as a result of failure of vital infrastructures

THREATS



TARGET
Government/ Intelligence services
Terrorists
Hacktivists
Script Kiddies
Cyber Researchers
Hackers "under the radar"
Hackers (responsible disclosure)
Suppliers
Employees/ ex-employees
Private organisations
Criminals
Financial or personal profit
Disagreement or Protest/ Sabotage
Resentment/ Personal attack
Challenge, pride, curiosity, fun, rebellion, profiling

Source: National CyberSecurity Center

Cybersecurity for Operational Technology

Where the physical and digital world meet

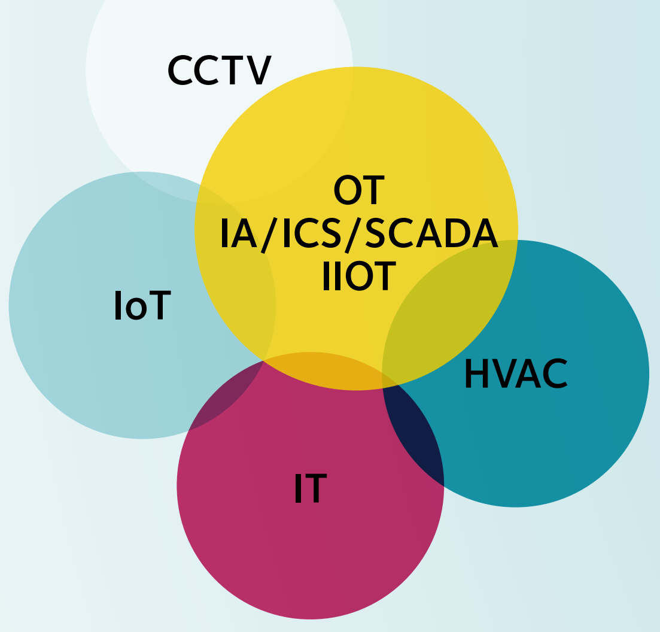
VISION ON SECURITY OF INDUSTRIAL CONTROL SYSTEMS

- Risk-based approach
- Focus on Assets: security of objects
- Focus on information: when integrating OT with other environments
- Provide an integral approach of physical and logical access security
- Protect industrial systems:
  - Zoning and Layering
  - Unidirectional Security Gateways
  - Defence in Depth
- Establish lifecycle management: if possible replace outdated and vulnerable systems/applications
- Where possible apply best practices from ICT security, but:
  - Know the limitations of Operational Technology
  - Implement management processes, responsibilities and governance
- Implement 'threat intelligence'
- Ensure regulation of the traffic flows between the IT, OT and IIOT domains: define a data management strategy

CYBERSECURITY FOCUS

- In process automation, there has traditionally been a lot of focus on physical (access) security. (Access control is also digital)
- Linking OT – IT (office environment) increases chance of cybersecurity risks
- Growing number of connections increases complexity
- Risk of process automation is risk IT plus risk OT (summation of risks)
- Human factor is also the greatest risk in OT environments
- Shift Safety to Security (can safety also be involved)

COHERENT MODEL



- OT = Operational Technology
- IA = Industrial Automation
- ICS = Industrial Control Systems
- SCADA = Supervisory Control and Data Acquisition
- IIoT = Industrial Internet of Things
- HVAC = Heating, Ventilation and Air Conditioning
- IoT = Internet of Things
- CCTV = Closed Circuit Television (surveillance cameras)
- IT = Information Technology

Action plan

1. Assess risks on Assets and Information (prioritization, Quick Wins)
2. Get support from management (sponsorship)
3. Create Cybersecurity Awareness to all employees
4. Create a test framework with Cybersecurity requirements to which the OT environment must comply
5. Check OT environment against the framework and deal with shortcomings in an implementation plan
6. Think of people, processes and technology from an architecture viewpoint
7. Protect OT environment as much as possible (Zoning and layering, Defence in Depth)
8. Carry out Patch management where possible
9. Where feasible, replace high risk outdated systems/ applications
10. Manage offline back-ups, including restoration
11. Implement active monitoring
12. Implement a well tuned incident reporting and response process
13. Design crisis management
14. Connect with business continuity management
15. Practice incident reporting and response process (and crisis management)

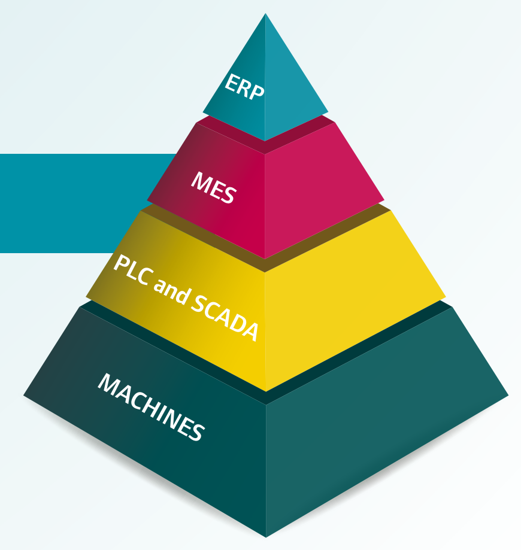
STANDARDS AND REFERENCES

- NIST SP 800-82 – Guide to Industrial Control Systems (ICS) Security
- ISO27019 – Information Security for the Energy Utility Industry
- ISA99 – Industrial Automation and Control Systems Security
- IEC 62351 – Security Standards for the Power System Information Infrastructure
- IEC 62443 – Cybersecurity for Industrial Automation and Control Systems (IACS)
- NCSC – Checklist security of ICS / SCADA systems
- NCSC – Your ICS/SCADA and building management systems online
- ENISA – Communication network dependencies for ICS/SCADA Systems
- ICS CERT – Recommended Practices
- CPNI – Good Practice Guides – Process Control and SCADA Security

DIFFERENCES BETWEEN IT AND OT ENVIRONMENTS

IT		OT
1,5 to 4 years	lifespan	10 to 30 years
information processing	focus on	physical industrial systems
office hours	in operation	real time, 7x24
generic and often	hack attack	specific/targeted
data loss	impact hack attack	physical damage/chance of casualties/economic loss
personal	user account	none or common
faster detected	malware	remains undiscovered (longer)
often	updates and patches	barely updates or patches
separated OTAP	develop and test environment (OTAP)	rarely separated OTAP
to a large extend	standardisation	a lot of customisation
many	suppliers	few
much	available knowledge	limited
a lot of	internet connectivity	increasing
datacenter / cloud	data processing	on premise

FUTURE



Developments with impact on cybersecurity:

- Increase in network environments:
  - 'Always connected': anywhere, anytime, anything
  - Industry 4.0: OT, IIOT and Cloud Computing
  - New applications
- IoT: contactless locks, (surveillance) cameras, temperature sensors etc. linked to office environment and/or internet
- IIoT: sensors and connections from the physical production environments (OT) to the information processing (IT) environments
- Integration of the operation and control chains (from ERP to machine level)
- Increased number of chain suppliers and security risks in the chain
- **Commodity**: new technologies become commonplace, for example in the medical world
- **In control/governance**: comply with (new) legislation and show this in the policy definitions and practical implementations
- IT – OT Big Data analytics, GIS, Forecasting, for example: weather forecast

Verdonck, Klooster & Associates (VKA) is committed to making ICT work for people. We are a strategic ICT consultancy and we love complex issues. Because it is ultimately all about people, we at VKA not only have technical specialists in house, but also people who can understand an organization. We realize successful projects that ensure that ICT does what it is meant for: making life easier and create smarter, more efficiënt and faster solutions. VKA has more than 30 man-years of experience in securing Industrial Control Systems.

Verdonck, Klooster & Associates | Baron de Coubertinlaan 1 | 2719 EN Zoetermeer | T 079 368 1000 | E info@vka.nl | **www.vka.nl**

VERDONCK
KLOOSTER &
ASSOCIATES