# the *total* feed business

## How will we protect our “crown jewels” @ ForFarmers?


YOU HAVE BEEN
HACKED !

# What is your worst Security nightmare?

# What is your worst Security nightmare?

# What is your worst Security nightmare?

## Hackers Attack Safety System, Shut Down Plant

Dec 15, 2017

# What is your worst Security nightmare?


**The Next Wave of Cyberattacks Won't Steal Data — They'll Change It**

# What is your worst Security nightmare?

BY FRED SEARLE

Wednesday 18th September 2019, 16:50 London

## *Cyber attack risk 'growing' in food supply chains*

New report warns that as other sectors become more resilient to attack, criminals are more likely to target food industry's vulnerable systems

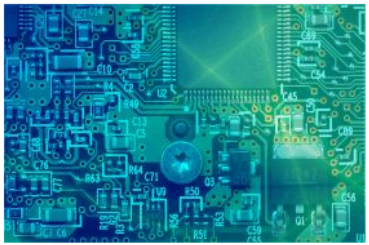
Global food supply chains are increasingly vulnerable to cyber attacks that could pose a risk to public health, a new report has warned.

Contaminated food, physical harm to workers, destroyed equipment, environmental damage and huge financial losses for food companies are among the potential consequences outlined in the study by the Food Protection and Defense Institute at the University of Minnesota.

Experts warn that the Industrial Control Systems (ICSs) that firms use to process and manufacture food have many vulnerabilities that are easy to exploit and will become an increasingly attractive target for criminals.

"As the energy, financial, and healthcare sectors harden their defenses in response to attacks, it's safe to assume criminals and other threat actors will move on to lower hanging fruit," the report reads.

"This could well be the food industry, which continues to use vulnerable ICSs [that are discoverable on the internet."

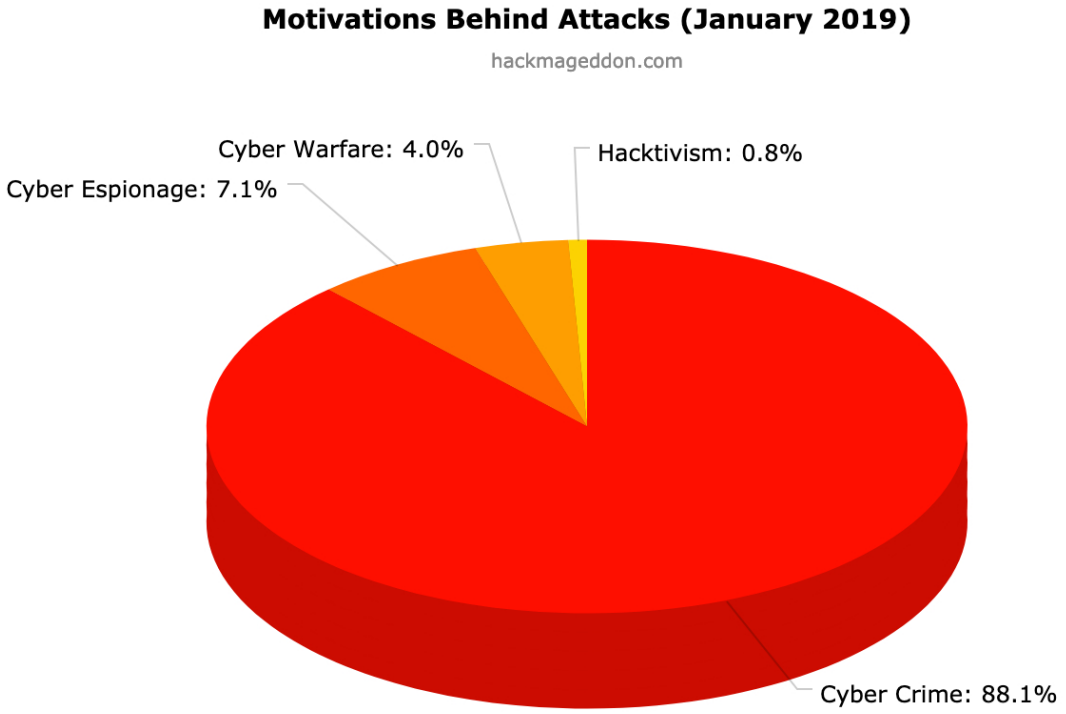


RELATED ARTICLES

1. Christiane Bell to leave BayWa
2. GWF lays foundations for growth
3. IGS reveal "hugely exciting" £5.4m funding
4. Huge online growth to transform global groce…
5. Distracted shoppers 'spend 41 per cent more…
6. JBT Corporation to acquire Proseal

Classification : Public

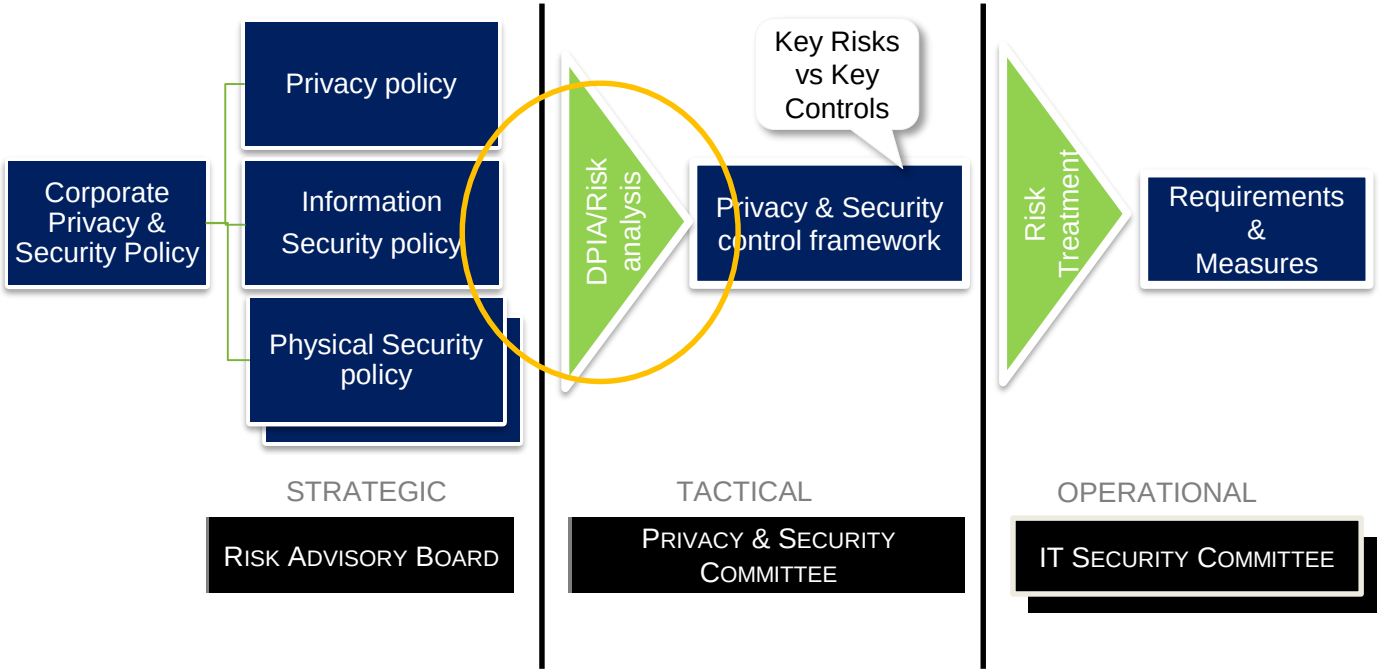
# What are the motivations behind attacks?



# What are the threat and risk landscapes?

# Privacy & Security scope @ ForFarmers

# Privacy & Security governance framework



# Our scenario-based risk assessment approach helps us to prioritise our investments in security in the most effective way

Annually we perform security workshops attended by Business and IT aimed at :

1. **Identify our 'Crown Jewels'**
   - What are the key business processes used in serving our customers?
   - Which systems are required to support these processes e.g. order processing, factory automation etc.

2. **What are the typical threats and threat actors do we (fore)see?**
   - In general
   - In the Agricultural sector in Europe

3. **What is the potential impact on our Business and our customers?**

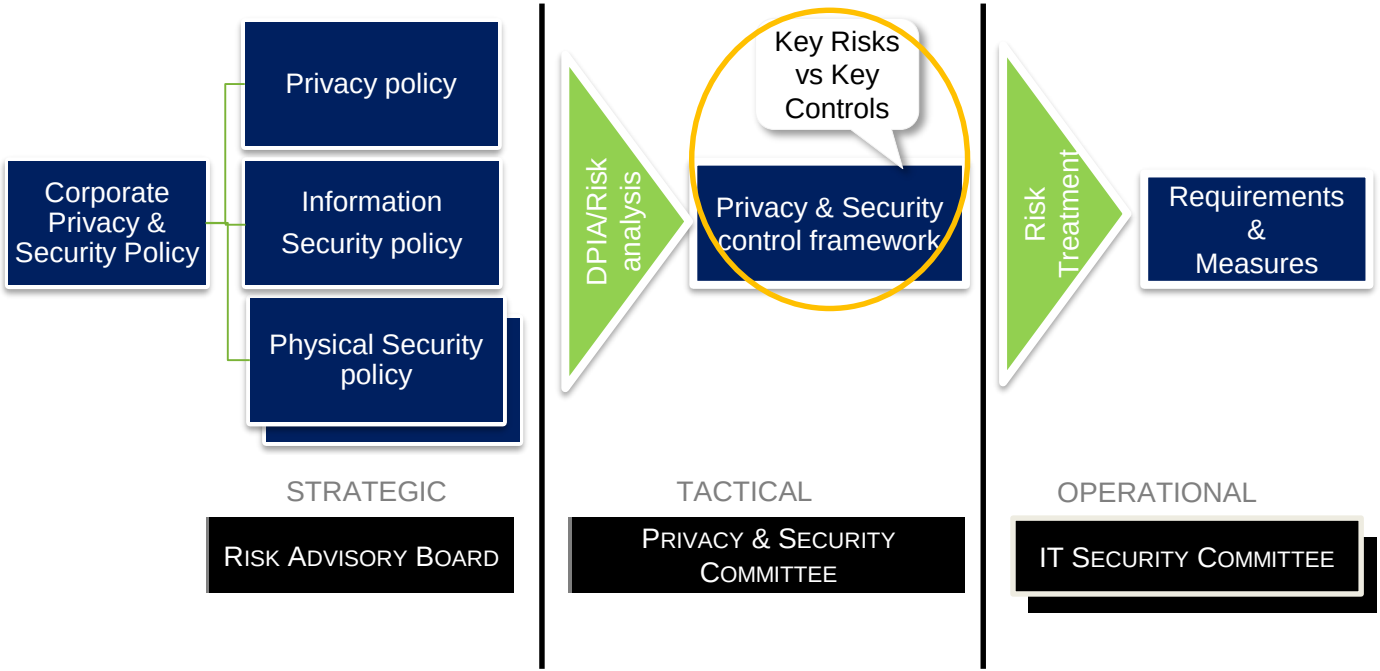
4. **What arrangements does ForFarmers already have in place?**

Objective is to focus on realistic threat scenarios that would have unacceptable business impact and are technically feasible

# We use templates/questionnaire to perform site assessments

| Topic | Question |
|---|---|
| **Acces Control** | Are there access zones identified and secured with tags/badges at the site? |
| **SCADA server** | Is the SCADA server room locked and secured with authorization to relevant ForFarmers personnel? |
| **Control room** | Is the Control room locked and secured with authorization to relevant ForFarmers personnel? |
| **Visitors** | Do visitors have to register themselves and wear identified visitor's badges? Are the visitors guided all the time at the site? |
| **Truck drivers** | Do the truck drivers have their own room and do they go to other areas like control room and/or factory? |
| **Camera's** | Are there camera's at the site and installed on all relevant places? Are the camera images recorded? |
| **User Accounts** | Are all user accounts identifiable to personnel of ForFarmers? Are there also any generic user accounts? |
| **Vendor access** | Do the system vendors have autonomous remote access to their systems and are these credentials known within ForFarmers? |
| **Patch mgmt** | Are the patches of the factory production systems performed under the supervision and patch scheme of ForFarmers? |
| **Awareness** | Are there procedures in place at the site to raise the attention of security threats and/or breach notification to the personnel of ForFarmers? |

# Privacy & Security governance framework



# The Privacy & Security control Framework consists of ISO 27001, IEC 62443, GDPR controls and best practices

1. Policy
2. Organization
3. Human Resource
4. Asset Management
5. Acces Control
6. Cryptography
7. Physical and Environmental Security
8. Operations Security
9. Communication Security
10. System acquisition, development and maintenance
11. Continuous monitoring
12. Vendor management
13. Incident management
14. IT/OT Business Continuity Management
15. Compliance
16. GDPR legislation

NEN

ISO 27001

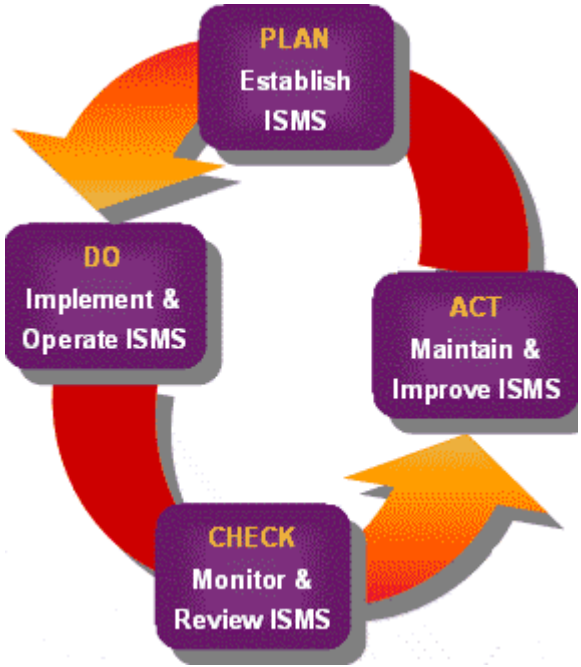
IEC

General Data Protection Regulation

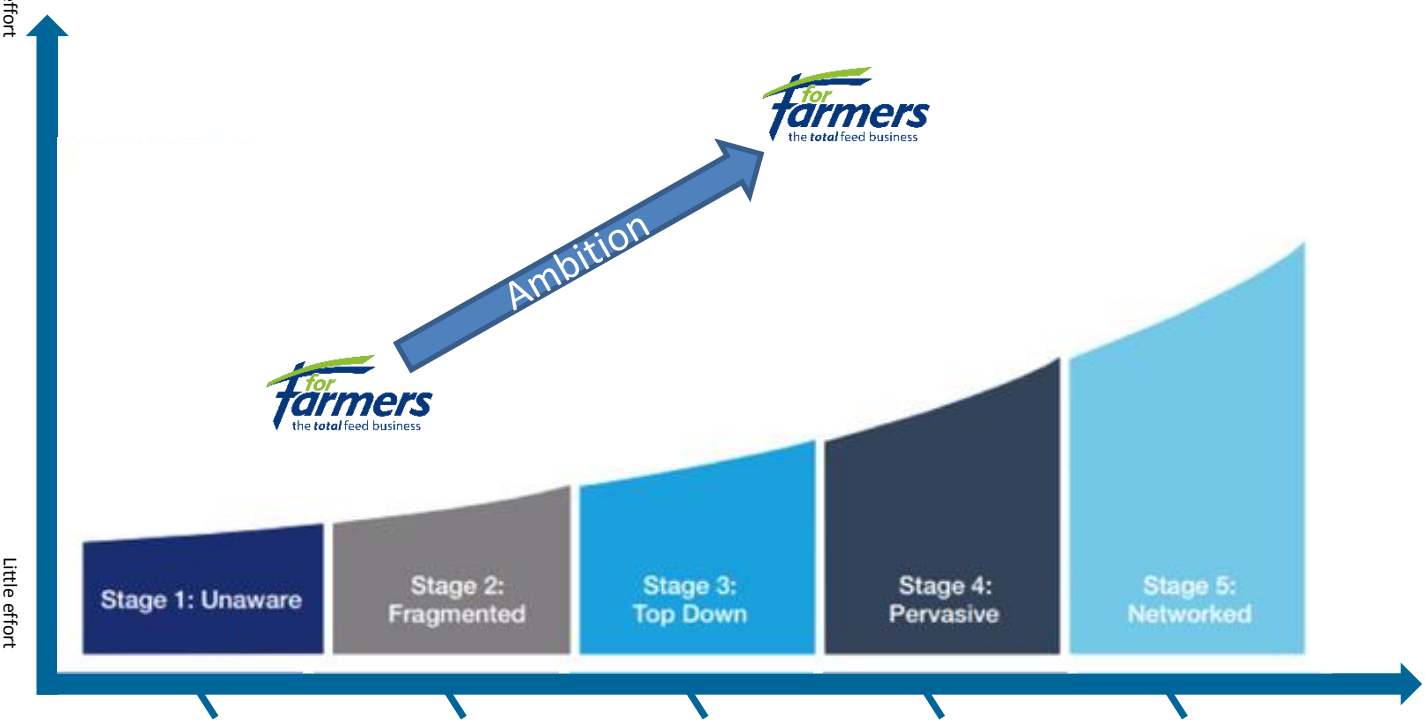

Classification : Public

for farmers the total feed business

# The Privacy & Security controls are implemented in P&SMS tool “GRC control” to monitor the PDCA cycle

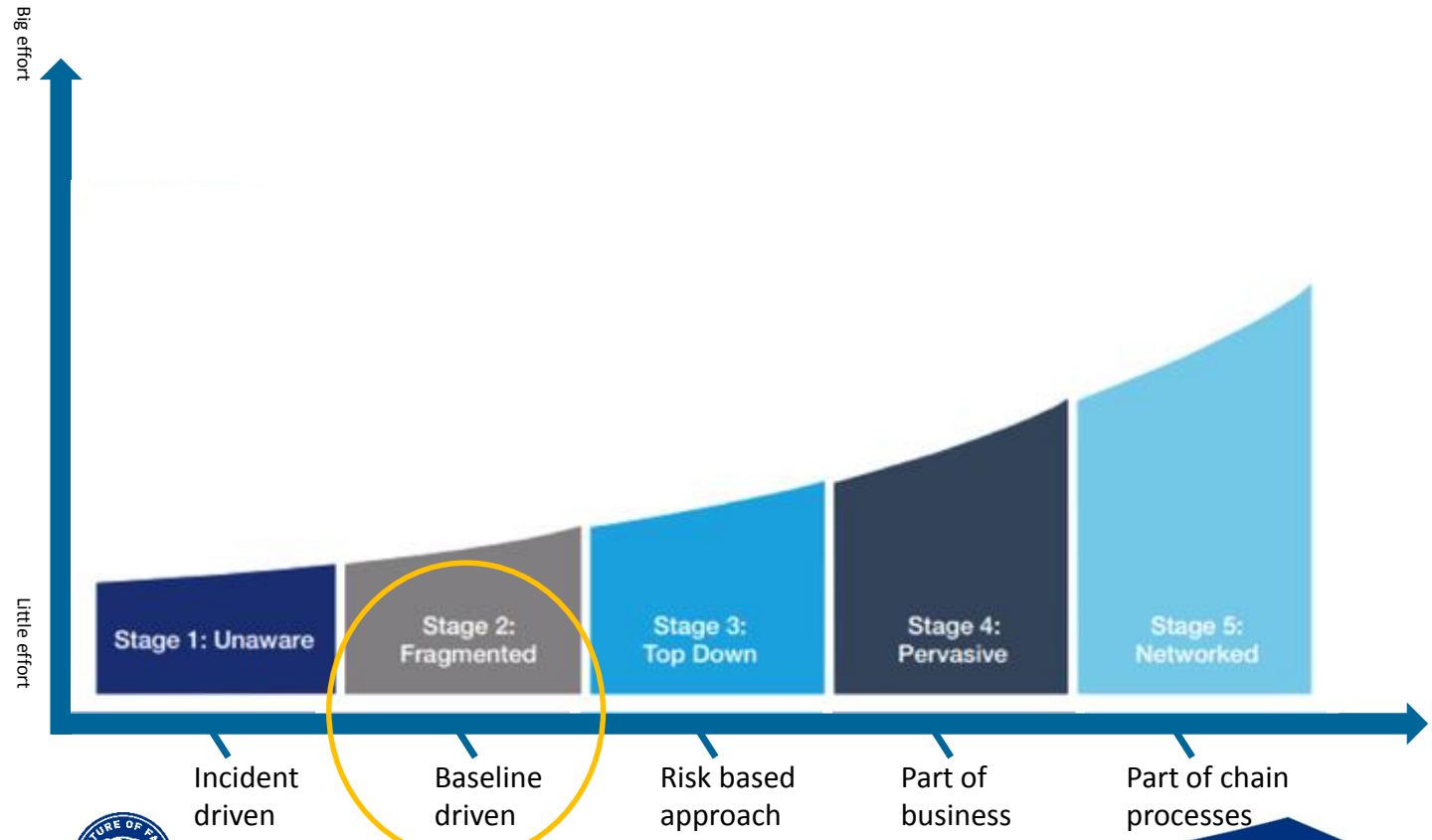
# Ambition of ForFarmers for the coming 5 years is to improve Privacy & Security into ‘the way we work’



# Privacy & Security Maturity Model (WEF)

| Stage | Maturity | Description |
|---|---|---|
| 1 | **Unaware / Incident driven** | ○ The organization sees privacy & (cyber) security as largely irrelevant, and cyber risk does not form part of the organization's risk management process. The organization is not aware of its level of interconnectedness. |
| 2 | **Fragmented / Baseline** | ○ The organization recognizes hyper connectivity as a potential source of risk, but has limited insight in its risk management practices. The organization has a silo approach to privacy and/or (cyber) security, with fragmented and incidental reporting. |
| 3 | **Top down / Risk analysis** | ○ The Chief Executive Officer has set the tone for privacy and/or (cyber) security, has initiated a top-down risk treatment program as part of risk management but does not view privacy & security as part of the organization and its business processes. |
| 4 | **Pervasive / Part of business processes** | ○ The organization's leadership takes full ownership of privacy & security and risk management, has developed policies and frameworks, and has defined responsibilities and reporting mechanisms. It understands the organization's vulnerabilities, controls, and interdependencies with third parties. |
| 5 | **Networked / Part of chain processes** | ○ The organization is highly connected to its peers and partners, sharing information and jointly mitigating (cyber) risk as part of their day to day operations. Its people show exceptional (cyber) security awareness and the organization is an industry leader in managing privacy & security as part of enterprise risk management. |

# What will be the initial stage for our sector?



# Launch of a sector collaborative workgroup

AgroConnect
passion to connect people

Vion
FOOD GROUP

de heus
powering progress

for farmers
the total feed business

nutreco

# What will we do together?

- **Set up sector Privacy & Security (baseline) standard**
- Share information on sector common threats, vulnerabilities, alerts and incidents
- Share lessons learned and best practices on solutions and technology from vendors
- Creation of an Agro-ISAC with support from Ministry of Economic Affairs and Climate Policy (DTC)

# What will we do together?

Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

## Start een ISAC:
## Sectoraal samenwerken

Handreiking

# Collaboration is crucial to improve our sector!!

**Feel free to contact me for more information**


- **Johan Rambi** : Group Security Officer
- **Telephone** : +316 22870746
- **E-mail** : johan.rambi@forfarmers.eu

# Thank you very much for your attention!!