[l05] solutions

[l05_p01] project

wim mees

remember the agencies

international level

- GAST: Global Agency for Ship Tracking
  ("mine")
- GASEO: Global Agency for Satellite Earth Observation
  ("yours")

national level

- CoGuaR: Coast Guard Radar station
- CoWSA: Coastal Waters Surveillance Agency

and the general concept

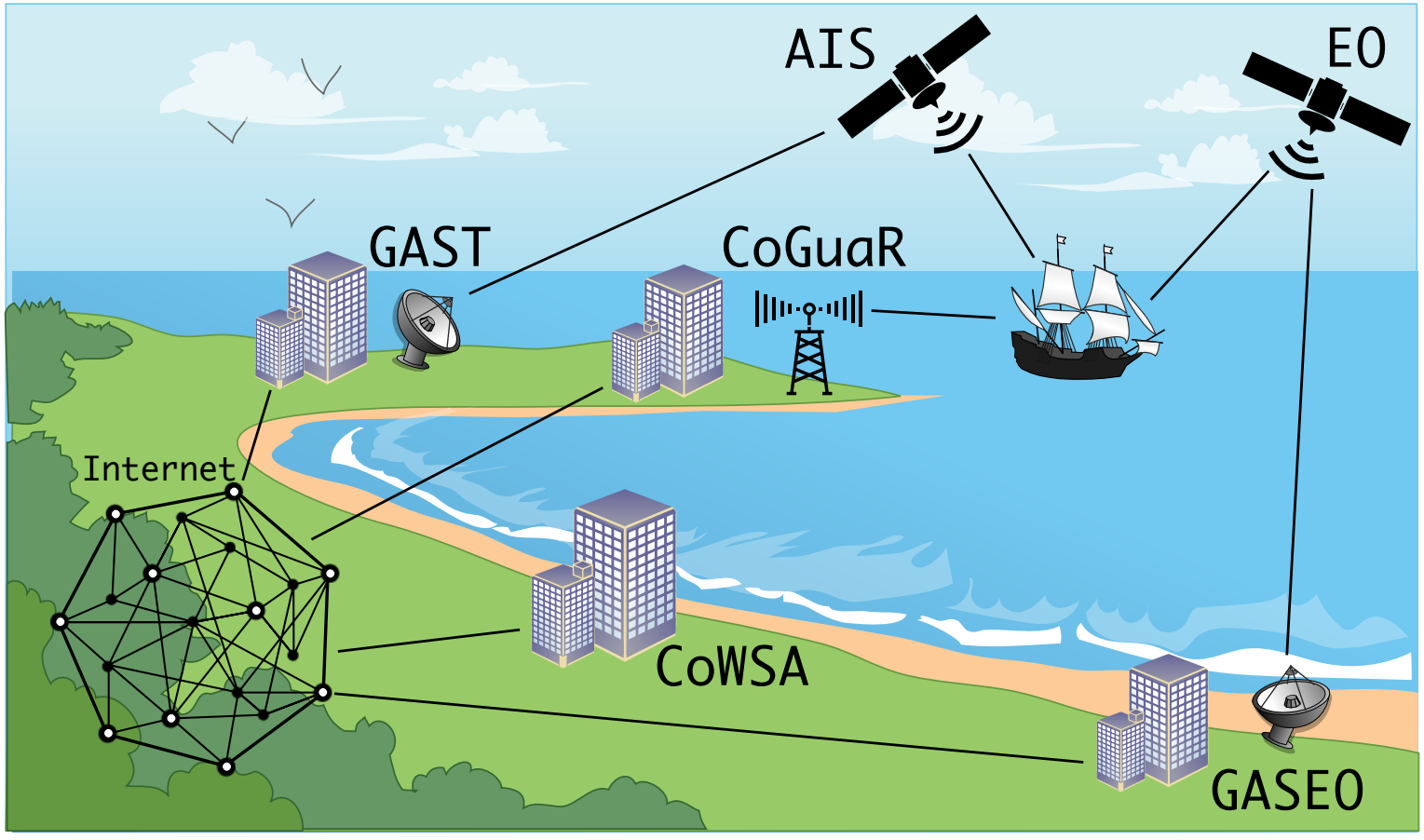

Figure 1: interactions between different organizations

GAST some diagrams

data flow diagram

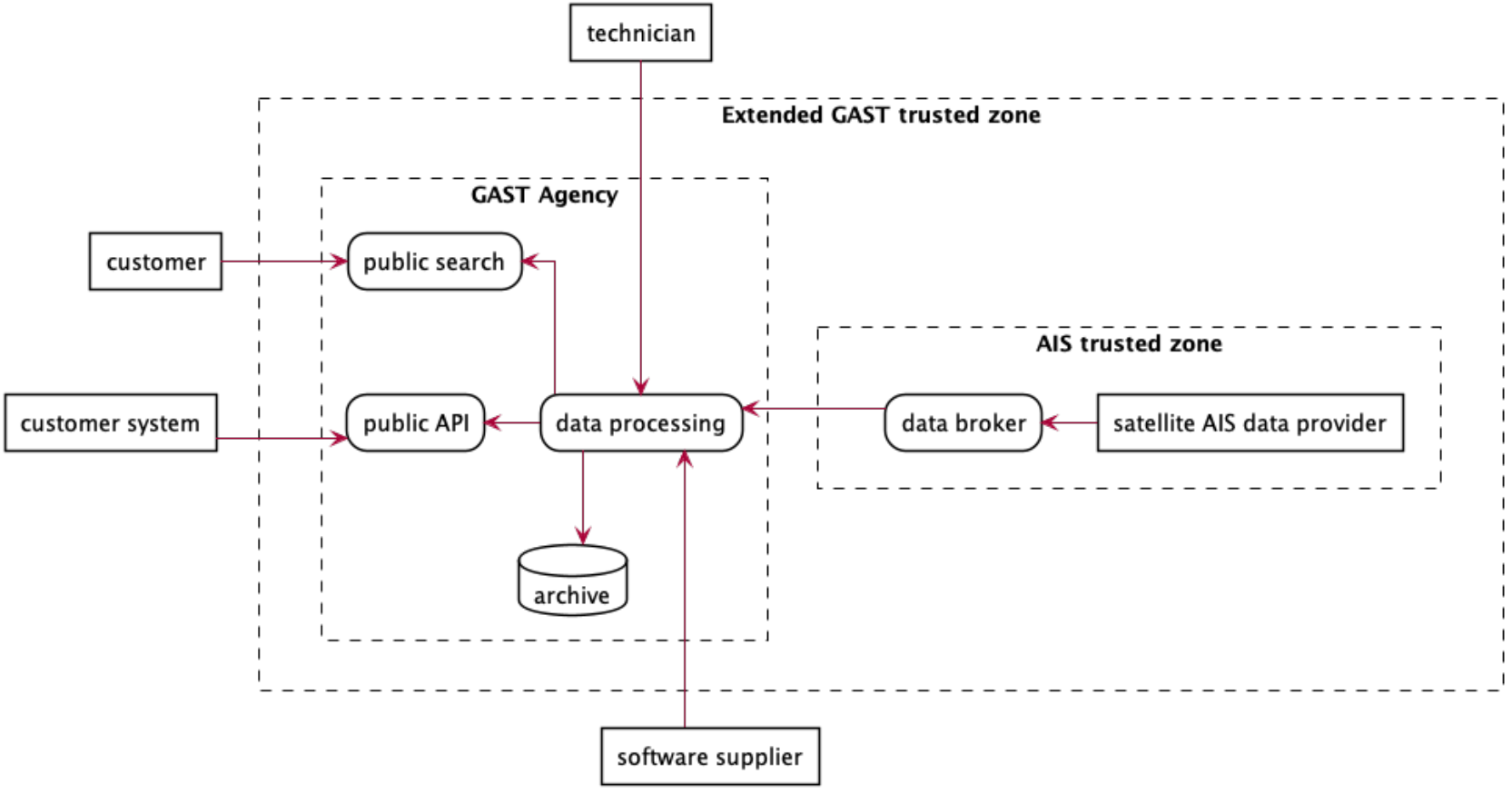

Figure 2: data flow diagram 1

network diagram

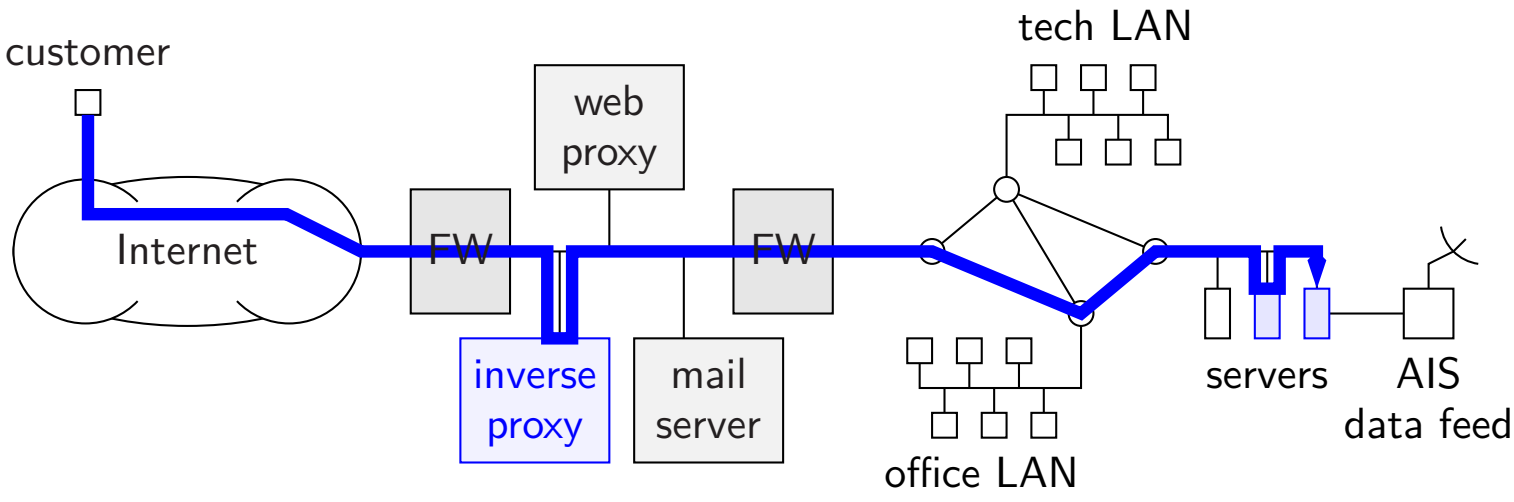

Figure 3: infrastructure for DFD 1

threat modeling

STRIDE-per-element

	S	T	R	I	D	E
External Entity	x		x			
Process	x	x	x	x	x	x
Data Flow		x		x	x	
Data Store		x	?	x	x	

Figure 4: STRIDE per element

STRIDE per element

spoofing (S) for external entities

- *customer:*
  T1: an attacker could pretend to be a paying customer and get free access to the extended search functionality
- *customer system:*
  T2: an attacker could pretend to be a subscribed customer system and obtain a data stream for free
  T3: an attacker could modify the subscription configuration of a regular customer pretending to be that customer and for instance hide information for that customer

(cont'd on next slide)

STRIDE per element

spoofing (S) for external entities (cont'd)

- *technician:*
  T4: an attacker could pretend to be a technician working remotely and get full administrator access to the production servers
- *software supplier:*
  T5: an attacker could pretend to be the software supplier and send a compromised code update to the agency

STRIDE per element

repudiation (R) for external entities

- *customer:*
  T6: a customer could perform a subscription or configuration change request and later claim he did not request the change (e.g. because he accidentally broke the service delivery or does not want to pay for a more expensive subscription)
- *technician:*
  T7: a technician could perform a configuration change and later claim he did not perform this change
  (e.g. when this change has broken something)
- *software supplier:*
  T8: a software supplier could send a software update and later claim they did not send that specific update
  (e.g. when the update is found to contain important bugs)

STRIDE per element

We are not going to cover the full "STRIDE per element" table since we just want to illustrate the mechanism. We are also not going to cover all DFDs for the same reason.

We will however show one example for every type of threat in the STRIDE acronym.

STRIDE per element

tampering (T) for a data flow

- **T9:** an attacker could tamper with the data flow between the data broker and the data processing in order to inject errors into the data and in this way break the integrity of the published AIS data

information disclosure (I) for a data flow

- **T10:** an attacker could break into the data flow between the customer and the public search process in order to steal the customer's credentials or banking information when he performs a payment

STRIDE per element

denial of service (D) for a data store

- **T11:** an attacker could send a large volume of fake data to the data store to saturate the bandwidth or fill the storage capacity, resulting in a loss of information that could not be archived

elevation of privilege (E) for a process

- **T12:** an attacker could send a manipulated request to the processing node in order to run code on that node with elevated privileges and install a backdoor

cyber kill chain

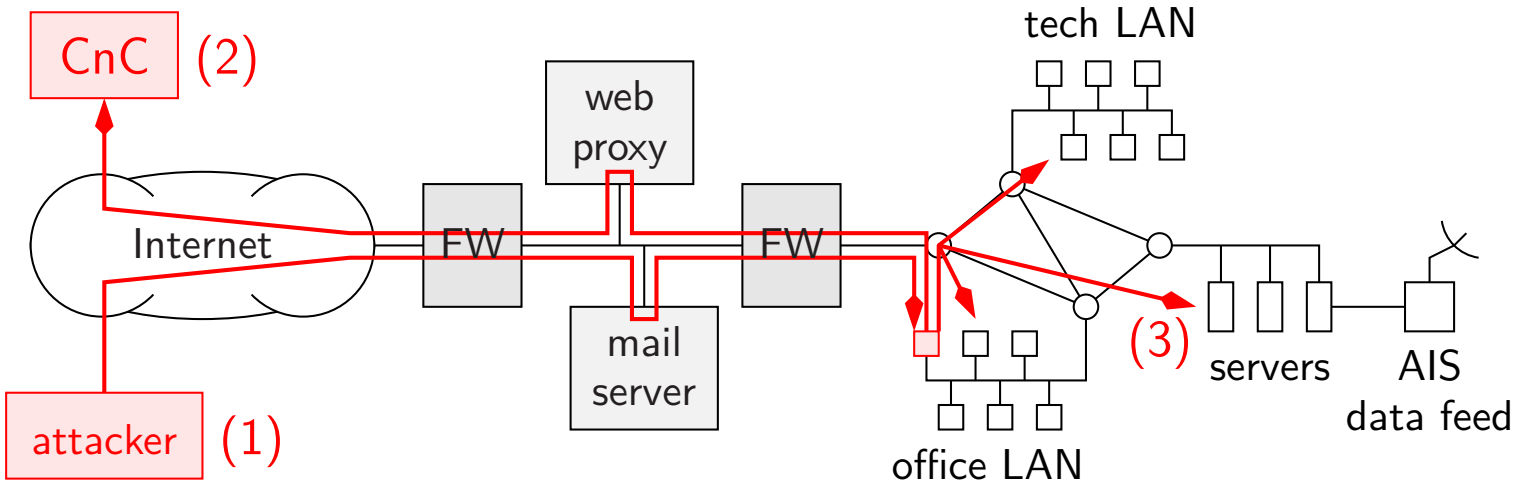

Figure 5: attacker actions

- step (1): attacker sends weaponized spear-phishing mail
- step (2): malware infects host and connects to CnC server
- step (3): malware scans and attacks tech LAN and servers

cyber kill chain

observation

the cyber kill chain scenario opens up to a threat source a large number of threats that require access to the internal network

risk assessment

threats

T1: an attacker could pretend to be a paying customer and get free access to the extended search functionality

- *probability:* we may have customers who use simple passwords or re-use the same password on different sites, and these sites may be hacked and the passwords dumped
- *impact:* the attacker would probably not have bought a paying subscription anyway
- *controls already in place:* we enforce a number of conditions on a password (length, special characters) and prevent brute force password guessing using a captcha after 3 misses

conclusion:

- moderate probability
- trivial impact

threats

- **T4:** an attacker could pretend to be a technician working remotely and get full administrator access to the production servers
- *probability:* the currently used VPN solution for the technicians only uses a password and the VPN client provides the option to save this password, therefore if someone steals or finds the laptop and manages to find the user's password he is in
- *impact:* technicians have full access to our internal network and possibly save passwords in their browser for certain critical internal web-based applications
- *controls already in place:* awareness training to warn technicians to be careful

conclusion:

- unlikely probability
- extreme impact

threats

- **T5:** an attacker could pretend to be the software supplier and send a compromised code update to the agency
- *probability:* an attacker could inject malicious code, either by gaining access to the software supplier's systems, or by sending it to us directly
- *impact:* this could completely break our operations
- *controls already in place:* the software updates are signed by the supplier

conclusion:

- moderate probability
- extreme impact

qualified risks

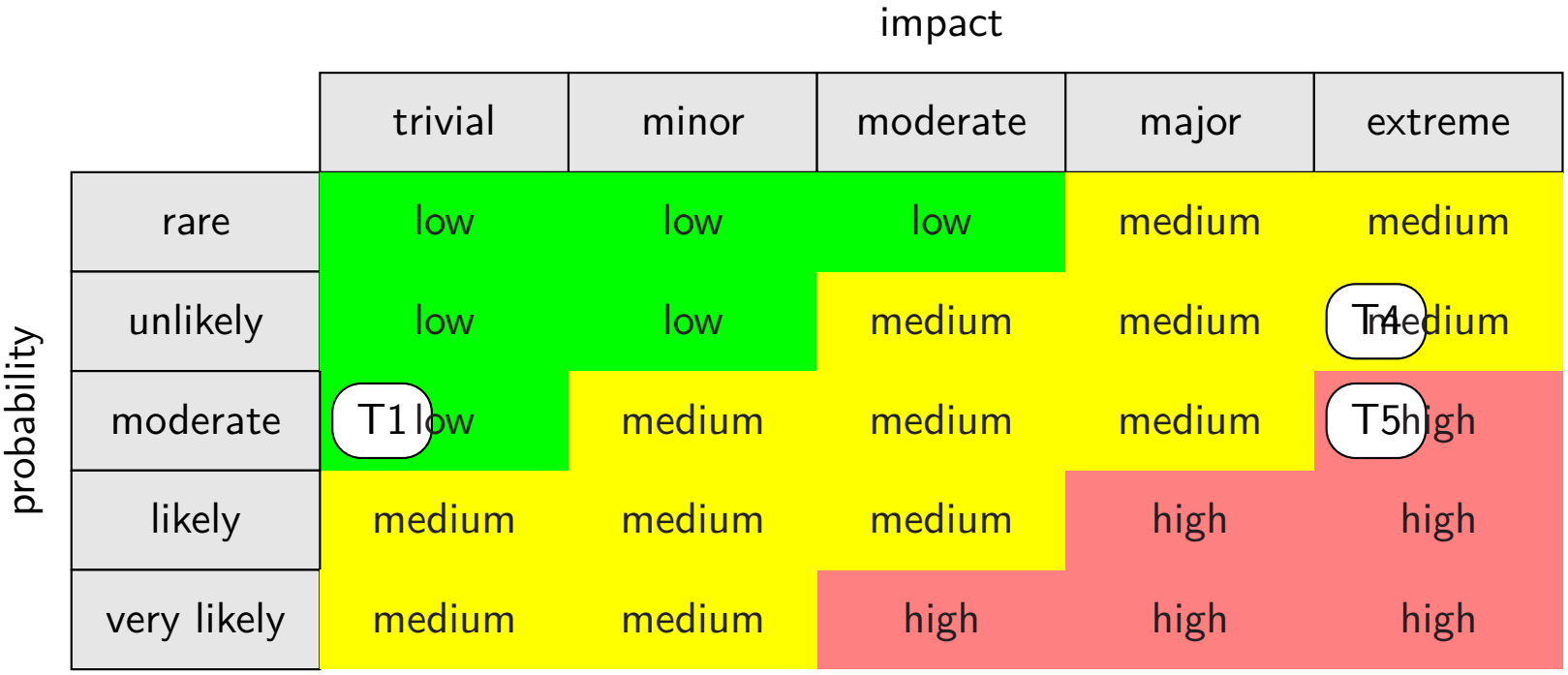

Figure 6: risks shown on the scoring matrix

threats

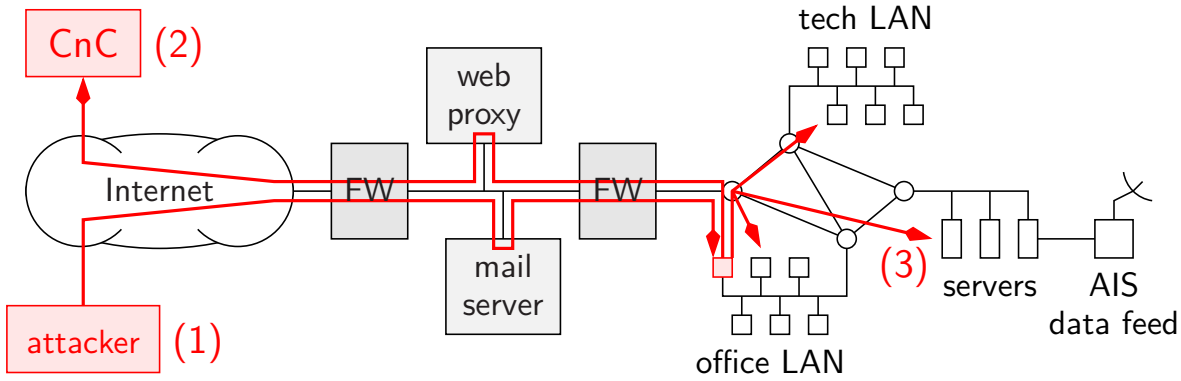

Figure 7: cyber kill chain

- **T9:** an attacker could perform an APT attack to get access to the internal network, and subsequently tamper with the data flow between the data broker and the data processing server in order to inject errors into the data and in this way break the integrity of the published AIS data

quantitative risk analysis

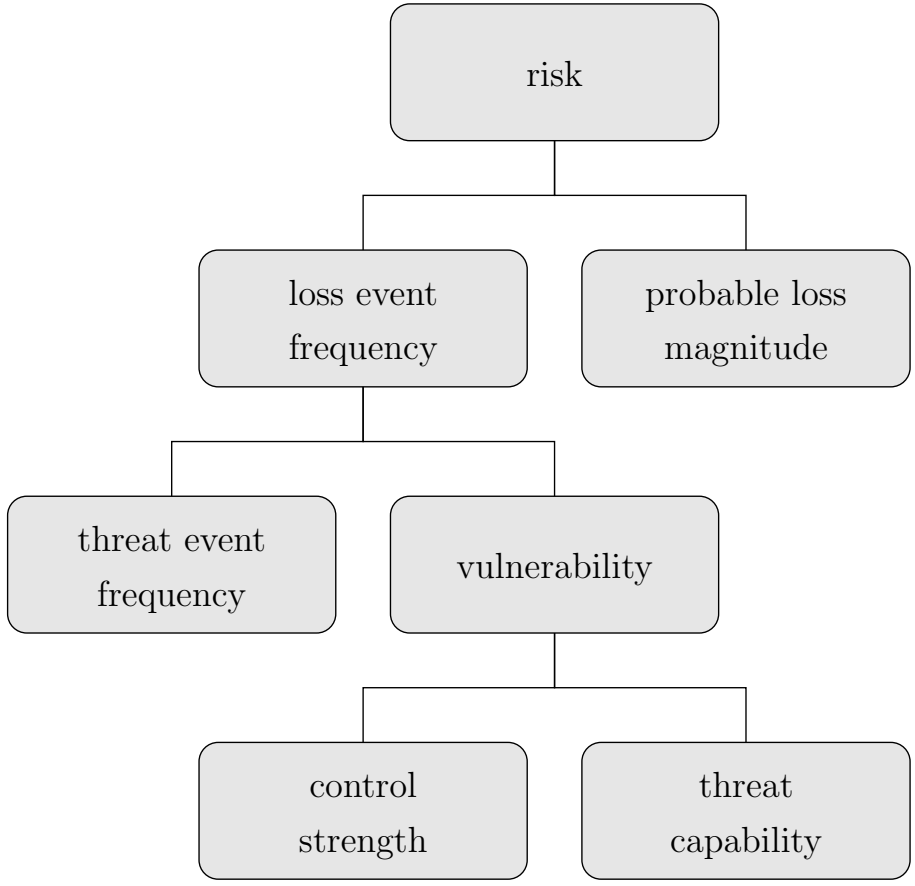

Figure 8: factor analysis for information risk (FAIR)

quantitative risk analysis

rating	description
very high (VH)	>100 times per year
high (H)	between 10 and 100 times per year
moderate (M)	between 1 and 10 times per year
low (L)	between 0.1 and 1 times per year
very low (VL)	<0.1 times per year

Figure 9: probable threat event frequency (TEF)

estimated level TEF: moderate (M)

quantitative risk analysis

rating	description
very high (VH)	top 2% when compared against the overall threat population
high (H)	top 16% when compared against the overall threat population
moderate (M)	average skills and resources (between top 16% and bottom 16%)
low (L)	bottom 16% when compared against the overall threat population
very low (VL)	bottom 2% when compared against the overall threat population

Figure 10: threat capability (TCap)

estimated level TCap: high (H)

quantitative risk analysis

rating	description
very high (VH)	protects against all but the top 2% of an average threat population
high (H)	protects against all but the top 16% of an average threat population
moderate (M)	protects against the average threat source
low (L)	only protects against the bottom 16% of an average threat population
very low (VL)	only protects against the bottom 2% of an average threat population

Figure 11: control strength (CS)

estimated level CS: moderate (M)

quantitative risk analysis

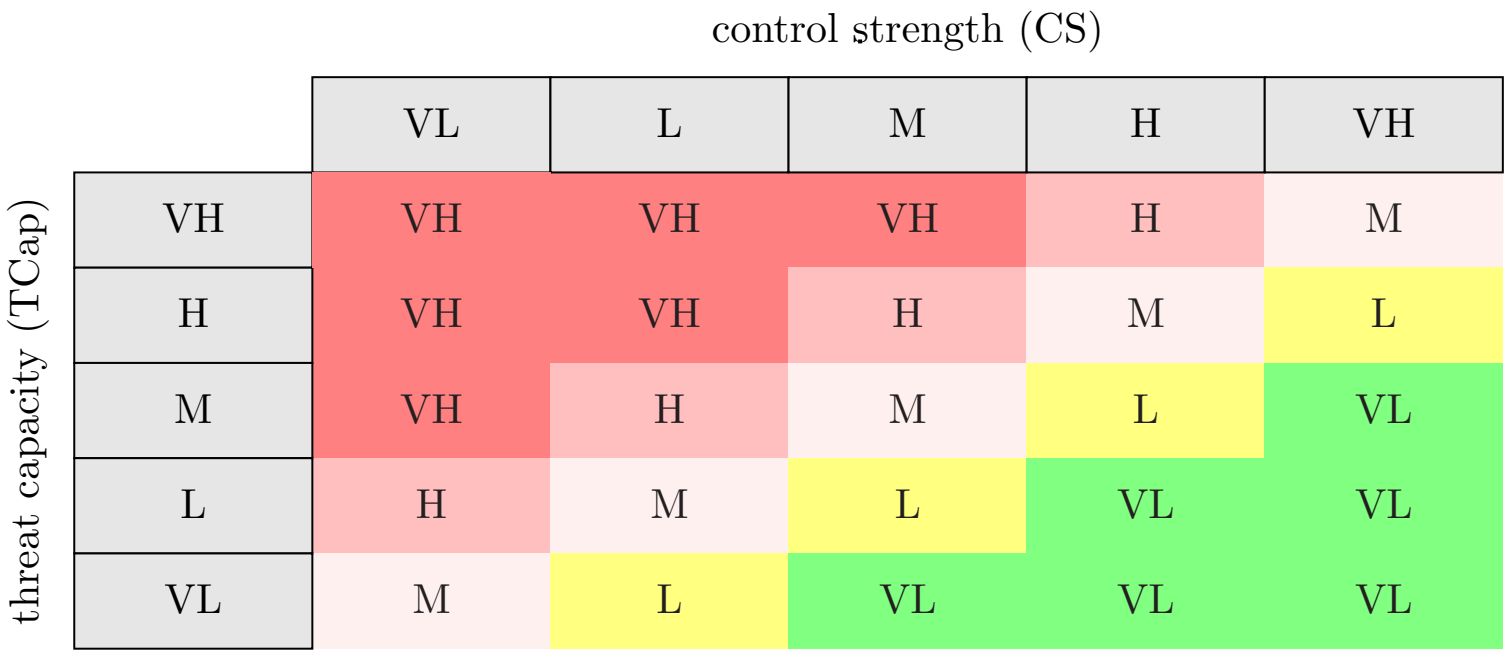

Figure 12: vulnerability matrix

estimated level Vuln: high (H)

quantitative risk analysis

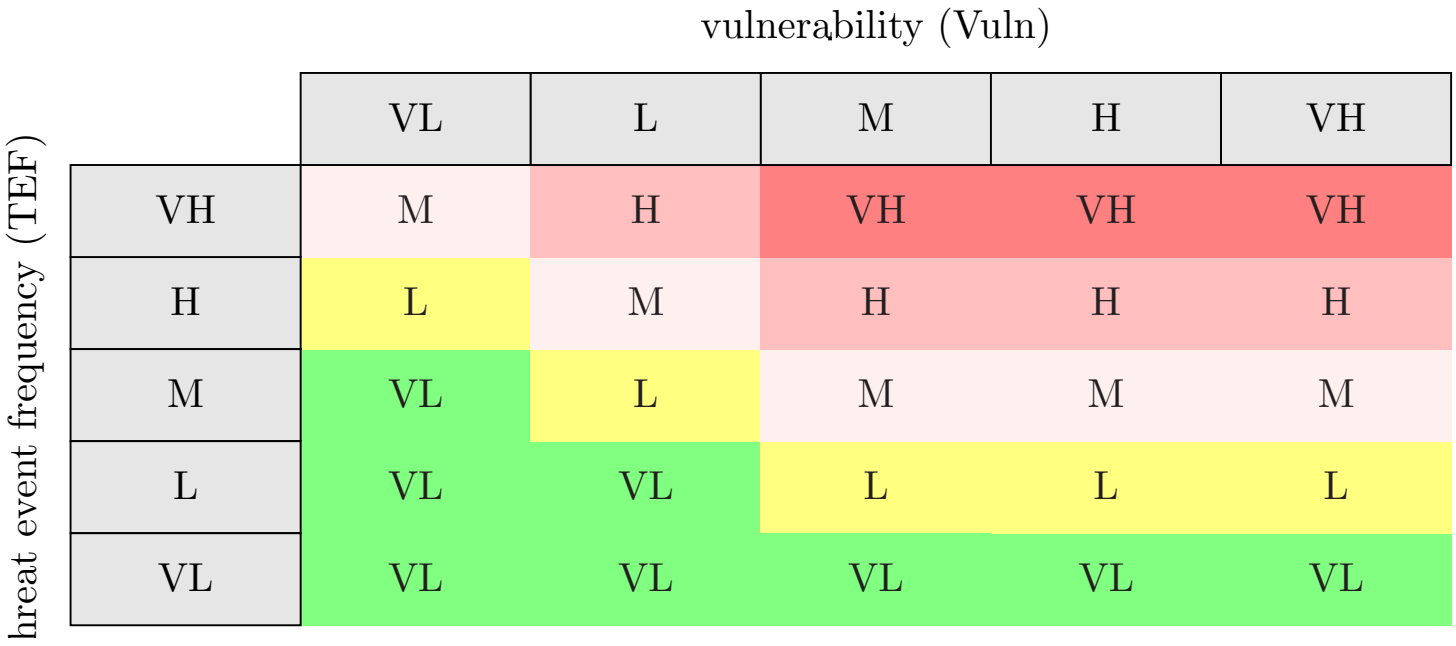

Figure 13: loss event frequency matrix

estimated level LEF: moderate (M)

quantitative risk analysis

magnitude	description
severe (SV)	10.000.000$ <= loss
high (H)	1.000.000$ <= loss < 10.000.000$
significant (Sg)	100.000$ <= loss < 1.000.000$
moderate (M)	10.000$ <= loss < 100.000$
low (L)	1.000$ <= loss < 10.000$
very low (VL)	loss < 1.000$

Figure 14: probable loss magnitude

estimated level PLM: high (H)

quantitative risk analysis

loss can be due to...

- *"replacement":* intrinsic value of asset itself
- *"response":* cost associated with managing the incident (man-hours, logistics, ...)
- *"productivity":* organization looses (part of) its capacity to produce value
- *"fines and judgments":* legal or regulatory actions against the organization as a result of the cyber incident
- *"competitive advantage":* losses due to for instance trade secrets, or merger and acquisition plans getting released
- *"reputation":* external perception that the organization is unethical, staff or leadership is incompetent, ...

quantitative risk analysis

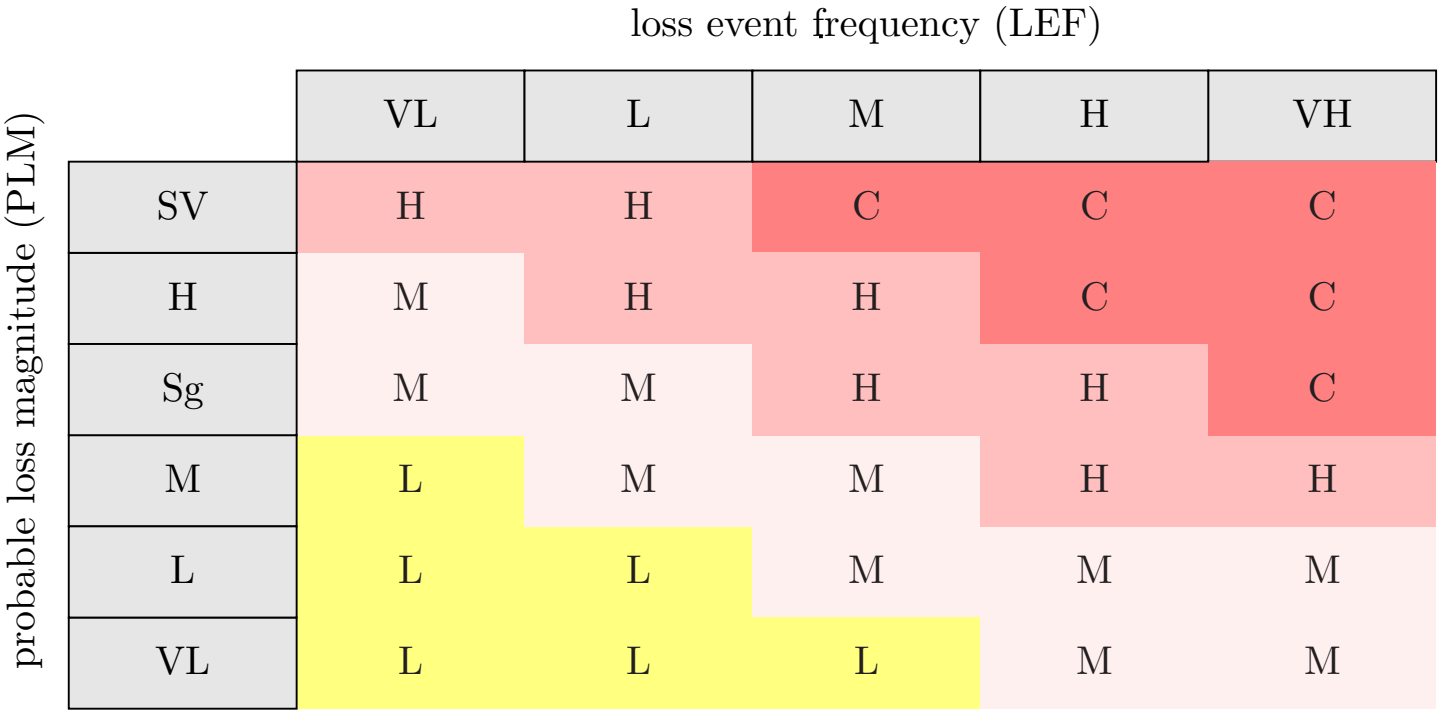

Figure 15: risk magnitude matrix

result: “high” (H)

risk management

- T1 (**LOW**): an attacker could pretend to be a paying customer and get free access to the extended search functionality
- T4 (**MEDIUM**): an attacker could pretend to be a technician working remotely and get full administrator access to the production servers
- T5 (**HIGH**): an attacker could pretend to be the software supplier and send a compromised code update to the agency
- T9 (**HIGH**): an attacker could perform an APT attack to get access to the internal network, and subsequently tamper with the data flow between the data broker and the data processing server in order to inject errors into the data and in this way break the integrity of the published AIS data

risk management

recommendations

- T1: accept the risk
- T4: implement strong authentication (multi-factor)
- T5: immediately stop installing new releases until a structural solution is found
- T9: urgently redesign network architecture to protect the integrity of the data processing

To be developed in more detail in a *"Risk Treatment Plan"* (RTP).

risk treatment

risk mitigation

threats that require immediate action

- T5 (**HIGH**): an attacker could pretend to be the software supplier and send a compromised code update to the agency
- T9 (**HIGH**): an attacker could perform an APT attack to get access to the internal network, and subsequently tamper with the data flow between the data broker and the data processing server in order to inject errors into the data and in this way break the integrity of the published AIS data

threats that require planned action

- T4 (**MEDIUM**): an attacker could pretend to be a technician working remotely and get full administrator access to the production servers

T5: software supply chain

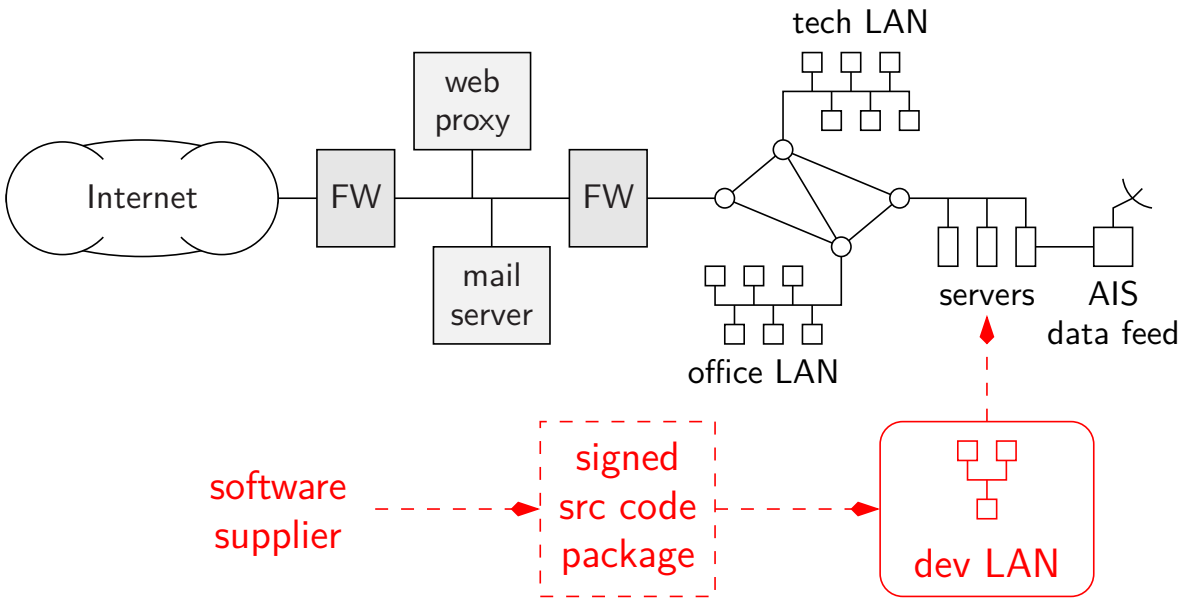

Figure 16: development LAN

- require software supplier to be certified (with periodic audits)
- updates delivered as signed source code packages
- all changes are audited by software experts
- extensive quality testing before transfer to production

T9: APT attack against AIS integrity

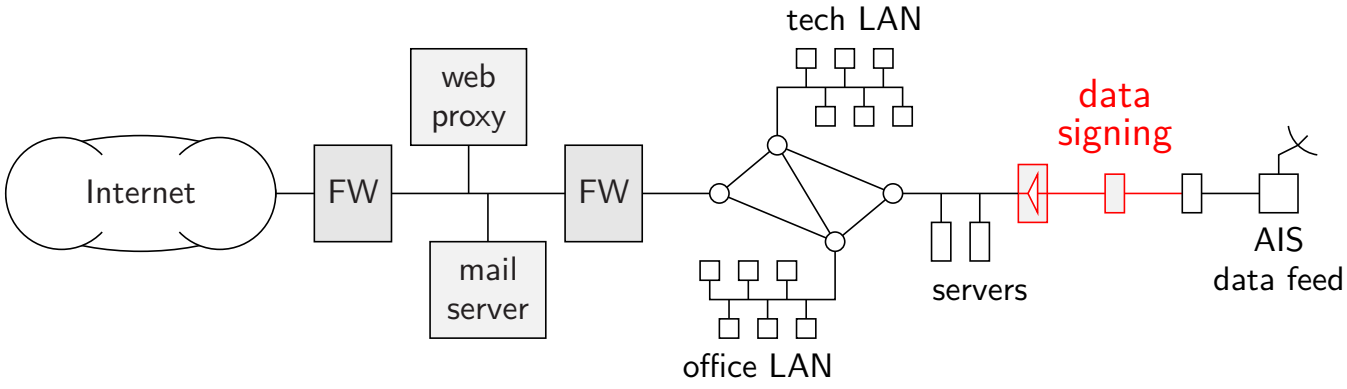

Figure 17: integrity protection

- protect Ops LAN from office and tech LAN
- no access from Ops LAN to the Internet
- integrity protection of Ops LAN through diode (Biba)
- integrity protection of AIS data through signing

T4: remote admin access

- use a dedicated laptop only for the remote admin work
  (to avoid APT compromises of multi-purpose device)
- strong two factor authentication for VPN
  (with separate hardware token)
- additional monitoring:
  - who connects from where
    (alert when connection from “new” country)
  - who performs which actions
    (alert when user perform “new” actions)
  - regular inspections of this audit trail
- quid servers behind diode ???
  (to be further discussed before implementation)

conclusions

what is expected from you

your project

- think about how you will implement the overarching meta-policy that you selected for GASEO in the form of:
  - a network architecture
  - building blocks and how they will be configured
- start writing down the network parts of your risk treatment plan

conclusions

Figure 18: questions or comments ?