


Political solutions to technical problems?

Linus Neumann <linus at berlin.ccc.de>

Agenda

-
-  **1. Tech problems**
 - 2. Political approaches
 - 3. What would actually make sense?
-

We recently discovered devastating and embarrassing security issues

Goto fail;	Heartbleed	Shellshock
Discovered: February 2014	Discovered: April 2014	Discovered: September 2014
Age at discovery: <ul style="list-style-type: none">▪ 1.5 years (iOS)▪ 5 months (Mac OS)	Age at discovery: 2 years	Age at discovery: 25 years
Time till fix: <ul style="list-style-type: none">▪ Same day (iOS)▪ 5 days (Mac OS)	Time till fix: Same day	Time till fix: <ul style="list-style-type: none">▪ Same day▪ 5 days (Mac OS)
Special feature Only the latest U2 album was pushed to Apple users even faster	Special feature First bug with its own logo	Special feature So far the oldest CVSS 10 known to mankind (older than Windows' IP stack)

The often proclaimed self-healing powers of OSS failed – and so did economic incentives

Example companies & Industries affected by heartbleed

Company	Industry	Annual turnover
Facebook	Social “network”	8 billion
Google	Web search	60 billion
Deutsche Bank	Banking	35 billion
Amazon	Shopping	75 billion
Dropbox	Cloudy storage	<1 billion
...		

Social dilemma:

Investments into open source security software audits and improvements are costly, yet benefit everybody:
Parasitizing is incentivized

Agenda

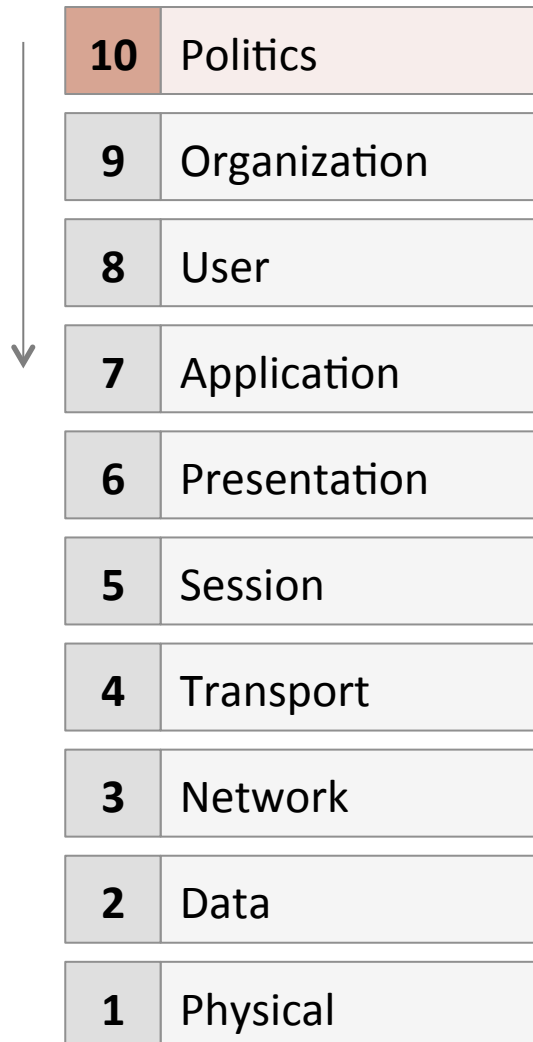
1. Tech problems

 **2. Political approaches**

3. What would actually make sense?

Naturally, political solutions are high-level by nature, but we should still evaluate them

OSI-layer



Lack of competence

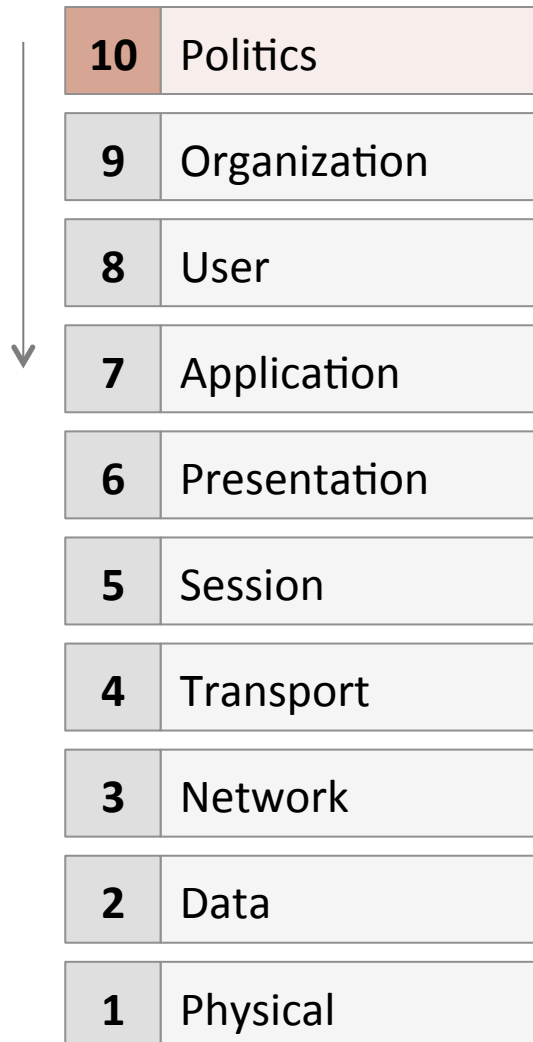
If politicians could fix the buffer overflow, they probably would not be politicians.

Strong pressure to “finally do something”

As the solution must be visible, “Security Theater” is the most tempting option.

Naturally, political solutions are high-level by nature, but we should still evaluate them

OSI-layer



Lack of resources

State of the art security research requires strong

Dysfunctional KPIs

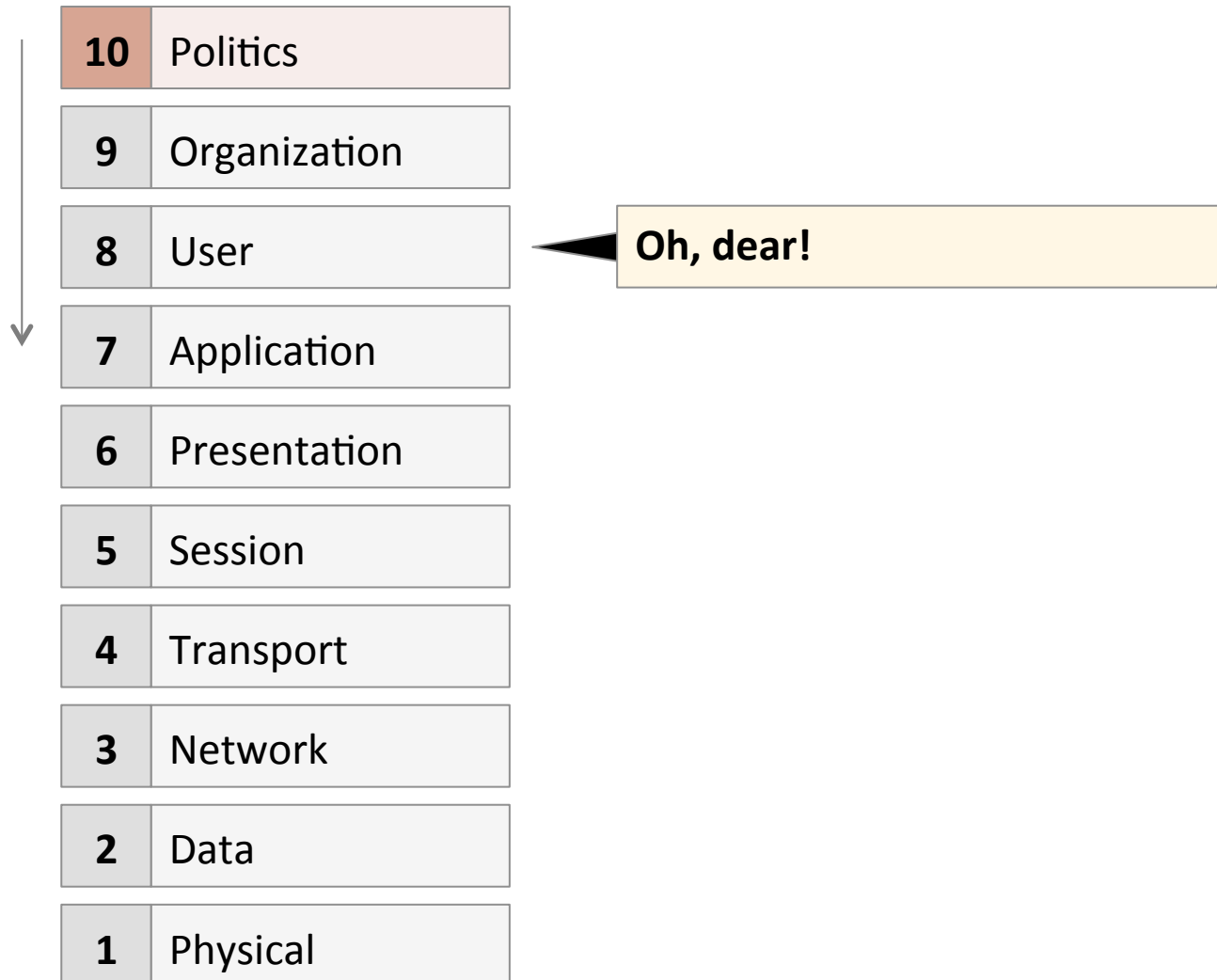
Strongest incentive is to cover one's own ass by fulfilling regulations.

Social dilemma

As long as we're as good as the others, we're fine.

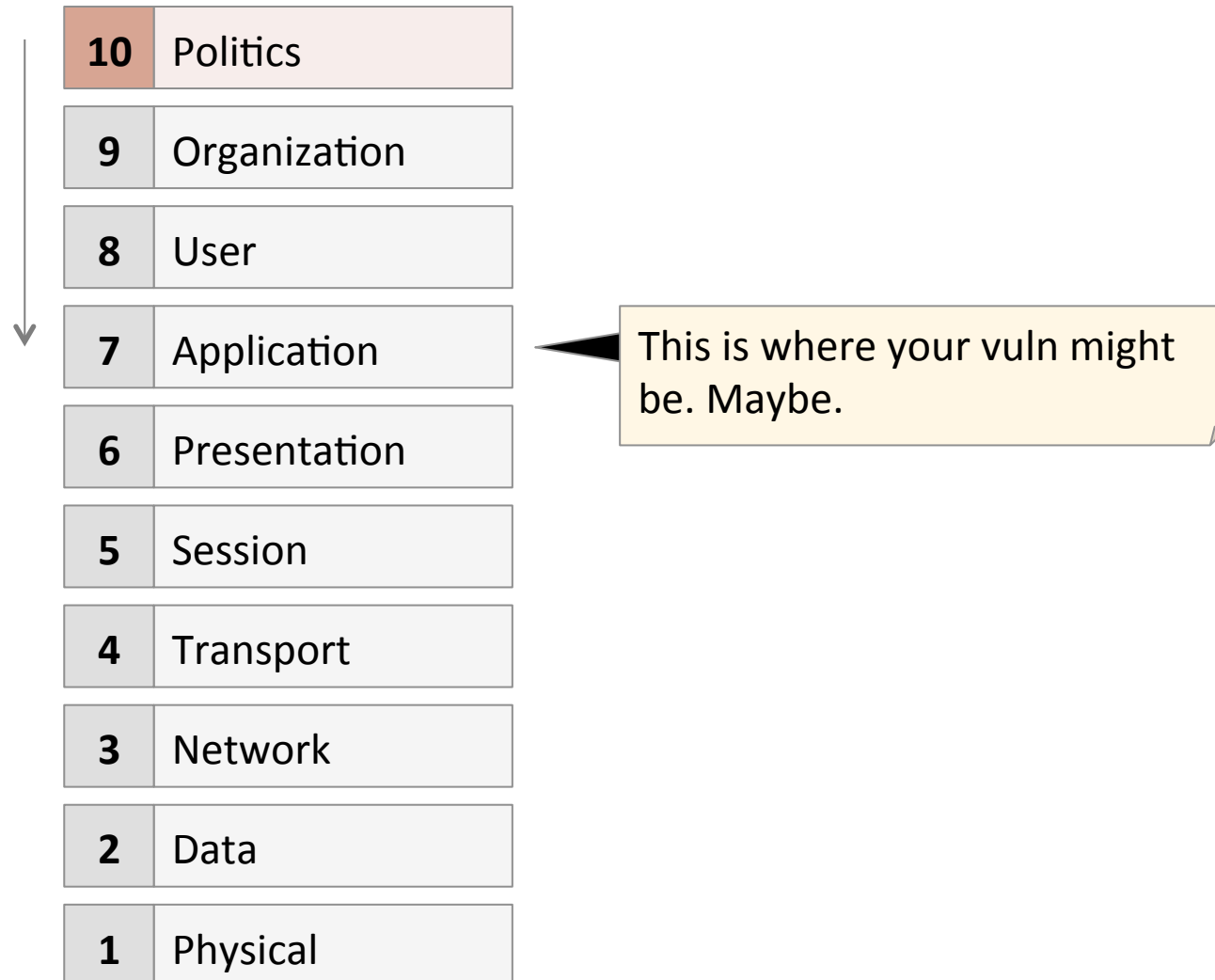
Naturally, political solutions are high-level by nature, but we should still evaluate them

OSI-layer



Naturally, political solutions are high-level by nature, but we should still evaluate them

OSI-layer



The German IT security law makes changes in 5 legal domains

Law

Core changes

A
BSI

- Critical infrastructure: Mandatory reporting to BSI
 - Minimal baseline security standards
 - SPOCs for security issues
-

B
Online services

- Minimal baseline security standards
 - Adequate authentication methods
 - Data retention for diagnostic purposes
-

C
Telecommunication

- Mandatory reporting to BNetzA
 - Data retention for diagnostic purposes
-

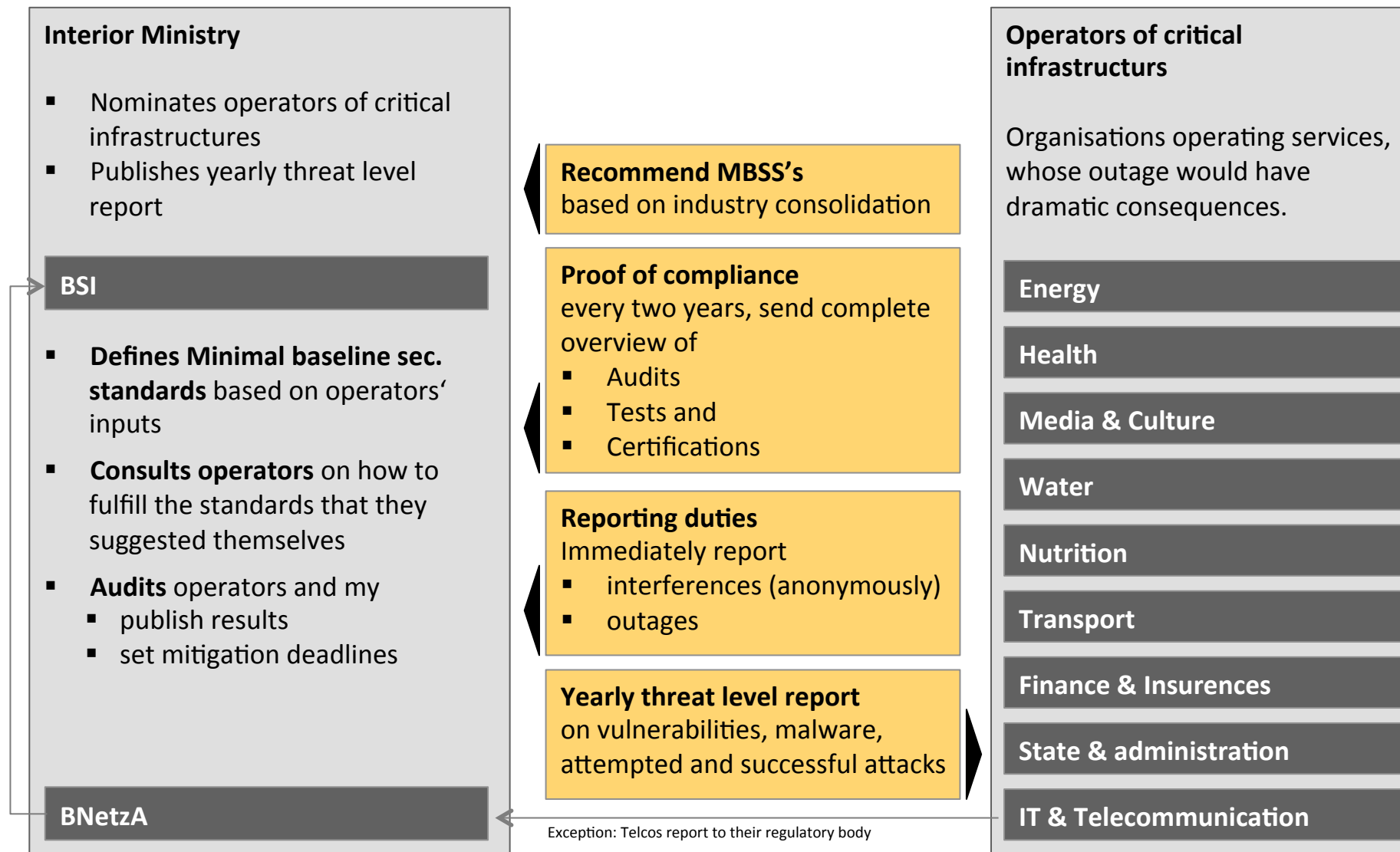
D
Exports

- Export regulations similar to military products
-

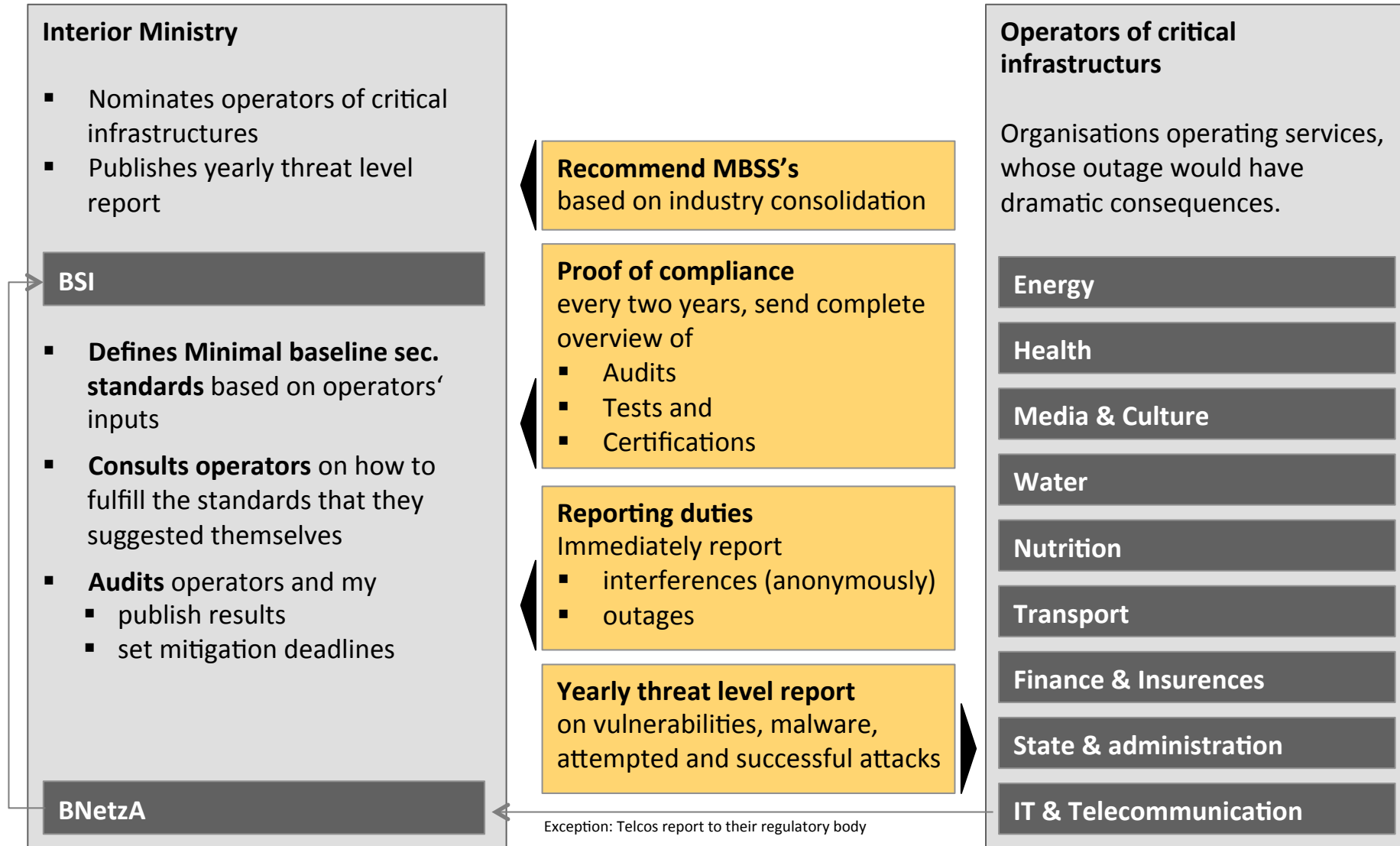
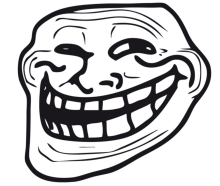
E
Law enforcement

- Federal LEA authority over cybercrime
- Federal LEA authority for attacks on federal institutions

A Operators of critical infrastructures will be subject to strict overview and regulation



A Operators of critical infrastructures will be subject to strict overview and regulation



A Self-regulation lacks incentives to step beyond current standards

Comparability:

Different incompatible MBSS's must be aligned

Corp. A		Corp. B		Corp. C	
Rule 1	<input checked="" type="checkbox"/>	Rule 1	<input type="checkbox"/>	Rule 1	<input checked="" type="checkbox"/>
Rule 2	<input type="checkbox"/>	Rule 2	<input checked="" type="checkbox"/>	Rule 2	<input type="checkbox"/>
Rule 3	<input type="checkbox"/>	Rule 3	<input type="checkbox"/>	Rule 3	<input checked="" type="checkbox"/>
Rule 4	<input checked="" type="checkbox"/>	Rule 4	<input checked="" type="checkbox"/>	Rule 4	<input checked="" type="checkbox"/>
Rule 5	<input type="checkbox"/>	Rule 5	<input type="checkbox"/>	Rule 5	<input checked="" type="checkbox"/>
Rule 6	<input checked="" type="checkbox"/>	Rule 6	<input type="checkbox"/>	Rule 6	<input checked="" type="checkbox"/>
...		

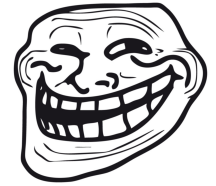
Consolidation:

A unified MBSS must be agreed on

Option A		Option B	
		Rule 1	<input type="checkbox"/>
		Rule 2	<input type="checkbox"/>
		Rule 3	<input type="checkbox"/>
Rule 4	<input checked="" type="checkbox"/>	Rule 4	<input checked="" type="checkbox"/>
		Rule 5	<input type="checkbox"/>
		Rule 6	<input type="checkbox"/>
		...	

Which outcome do you expect in a semi-democratic consolidation process?
Either way, the bureaucratic cost for this slight increase in security is enormous.

B Online service providers are now obliged to be secure



Online service providers

ARE: Content- und Hosting-Providers

MUST:

- Apply appropriate **organizational & technical measures** to protect systems, components and processes
- Use appropriate **authentication procedures**

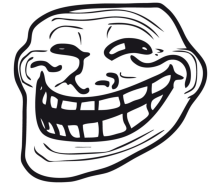
MAY:

- Store usage data to diagnose and detect abuse.
For 6 months.
→ New § 15 (9) TMG, similar to § 100 (1) TKG

Sounds good.

At least, it introduces liability for careless security.

B Online service providers are now obliged to be secure



Online service providers

ARE: Content- und Hosting-Providers

MUST:

- Apply appropriate **organizational & technical measures** to protect systems, components and processes
- Use appropriate **authentication procedures**

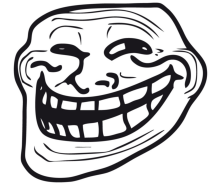
MAY:

- Store usage data to diagnose and detect abuse.
For 6 months.
→ New § 15 (9) TMG, similar to § 100 (1) TKG

Sound good, or does it?

This is not about 2FA,
this is about showing
your ID when signing up.

B Online service providers are now obliged to be secure



Online service providers

ARE: Content- und Hosting-Providers

MUST:

- Apply appropriate **organizational & technical measures** to protect systems, components and processes
- Use appropriate **authentication procedures**

MAY:

- Store usage data to diagnose and detect abuse.
For 6 months.
→ New § 15 (9) TMG, similar to § 100 (1) TKG

6 months?

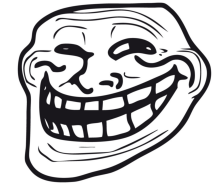
This is not about threat detection, this is about law enforcement.

B Data retention: Where there's a trough, the pigs ain't far...

New § 15 (9) TMG	Former EU policy 2006/24/EG *
Motivation: To diagnose and detect issues	Motivation: Law enforcement
Extent: <ul style="list-style-type: none">▪ Unscharf definiert als „Nutzungsdaten“▪ Daten, die über den für Betrieb und Funktionalität notwendigen Umfang hinausgehen	Extent: <ul style="list-style-type: none">▪ All metadata of [mobile,online] telephony services
Length: 6 months	Length: 6 months
Access: <ul style="list-style-type: none">▪ Data collected in accordance with § 100 (1) TKG is regularly used for prosecution and copyright infringements cease-and-desist orders.	Access: <ul style="list-style-type: none">▪ Criminal prosecution▪ LEA immediately demanded to use data for prevention as well

*) German data retention laws were ruled unconstitutional by BVerfG in March 2010; EU-policy was dropped by EuGH in April 2014

B Data retention: Where there's a trough, the pigs ain't far...



New § 15 (9) TMG

Motivation:

To diagnose and detect issues

Extent:

- Unscharf definiert als „Nutzungsdaten“
- Daten, die über den für Betrieb und Funktionalität notwendigen Umfang hinausgehen

Length: 6 months

Access:

- Data collected in accordance with § 100 (1) TKG is regularly used for prosecution and copyright infringements cease-and-desist orders.

Former EU policy 2006/24/EG *

Motivation:

Law enforcement

Extent:

- All metadata of [mobile,online] telephony services

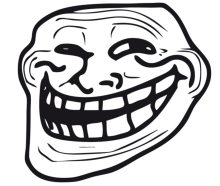
Length: 6 months

Access:

- Criminal prosecution
- LEA immediately demanded to use data for prevention as well

*) German data retention laws were ruled unconstitutional by BVerfG in March 2010; EU-policy was dropped by EuGH in April 2014

C TelCos get the same „security“ regulations, plus additional reporting duties to their dedicated regulatory body



Telecommunication service providers

ARE: Landline and mobile phone operators

MUST:

- Apply appropriate **organizational & technical measures** to protect systems, components and processes
- Use appropriate **authentication procedures**
- **Report issues** to their regulatory body (BNetzA)

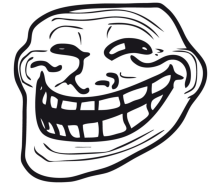
MAY:

- Store usage data to diagnose and detect abuse.
For 6 months.
→ well established § 100 (1) TKG

BNetzA

- Can force operator to inform public about probable breach
- Forward security issues to BSI or European Agency for Network and Information Security (ENISA)
- Issues a yearly report to BSI & ENISA

D Surveillance equipment will be subject to export regulations



Extension of § 4/5 Außenhandelsgesetz

Extended to cover Lawful Intercept equipment:

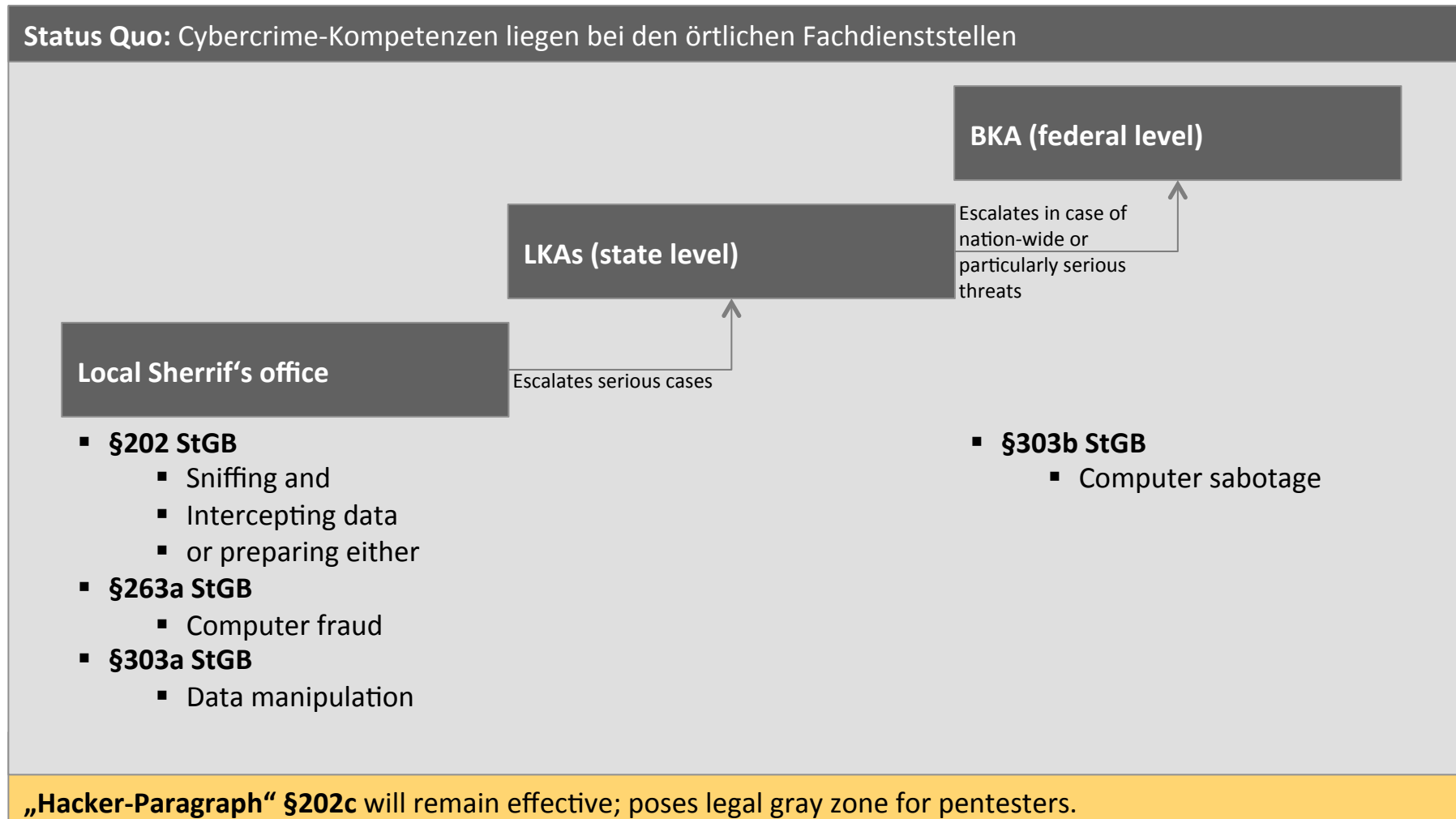
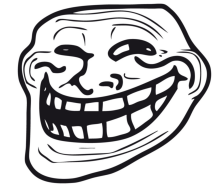
Vendors and Service providers of LI equipment according to § 110 TKG

Allows government to issue legal decrees

Limitations and shall ensure confidentiality in lawful intercept.

Possible restrictions are analogous to the export of weapons and military goods.

E Federal law enforcement will have Cybercrime jurisdiction



Agenda

-
1. Tech problems
 2. Political approaches

 **3. What would actually make sense?**

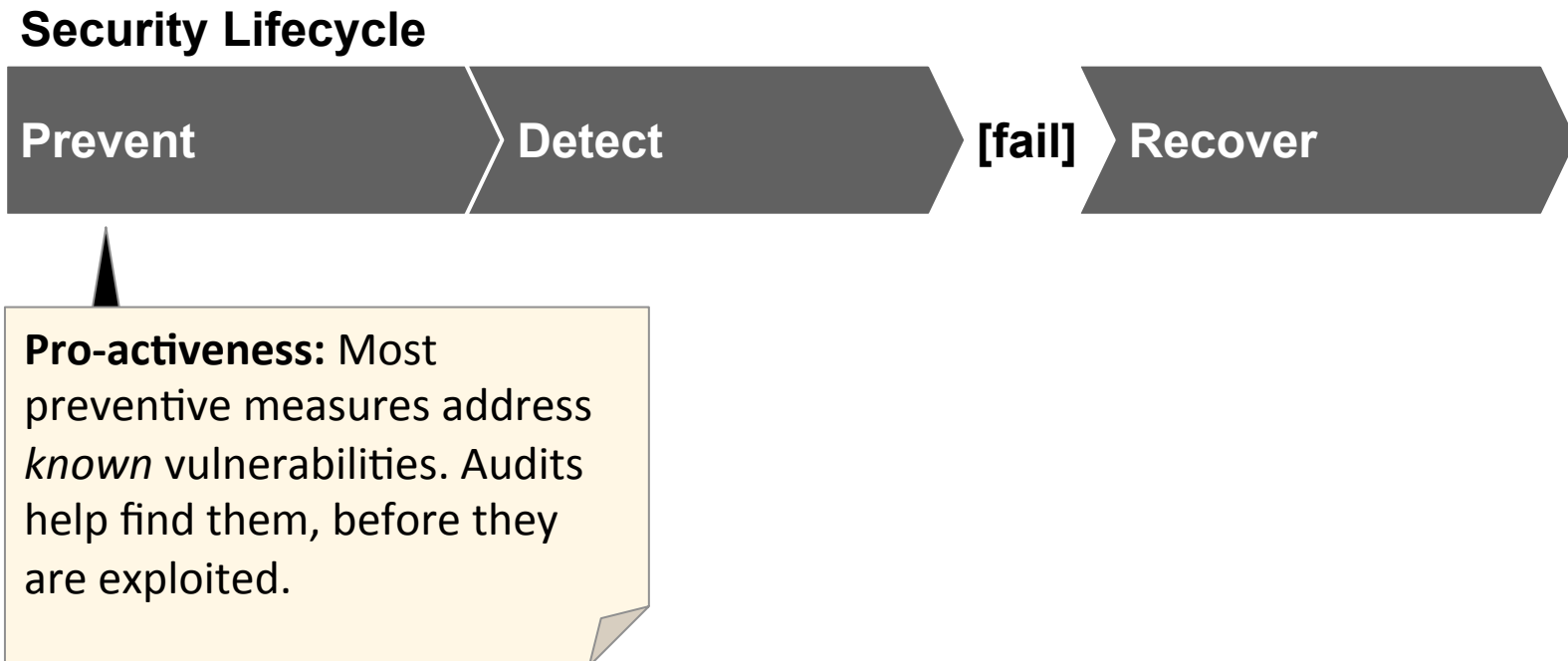
The CCC recommends a carrot-and-stick approach to IT security regulation

I Software quality	II Secure infrastructure	III Independent bodies and evidence-based laws
<ul style="list-style-type: none">▪ Regular independent audits▪ Bug bounties▪ Liabilities	<ul style="list-style-type: none">▪ Decentralize infrastructure▪ Apply strong standards▪ Require e2e-crypto	<ul style="list-style-type: none">▪ Assess effectiveness of surveillance laws▪ Provide independent IT security body

Will these signs make coders code better keep attackers from attacking?



I Open source software audits drive security evolution



I Current bug bounty programs do not match black market's financial incentives



[Home](#) | [VUPEN Products](#) | [Industry Solutions](#) | [Vulnerability Research](#) | [Contact Sales](#) | [Company & Events](#)

Products by Name


- VUPEN Products Overview
- Binary Analysis & Exploits
- Threat Protection Program
- Exploits for Offensive Sec.

[Contact Sales](#) ▶▶

VUPEN Vulnerability Research Videos and Demonstrations

Google Chrome Pwned by VUPEN aka Sandbox/ASLR/DEP Bypass

Published on 2011-05-09 17:35:41 UTC by VUPEN Vulnerability Research Team

 Hi everyone,
We are (un)happy to announce that
The exploit shown in this video is one that bypasses all security features including (vulnerability), it is silent (no crash after exploit discovered by VUPEN and it works on all Windows 7 SP1 (x64). The user is tricked into execute various payloads to ultimately down the sandbox (at Medium integrity level).


The video shows the exploit in action with Windows 7 SP1 (x64). The user is tricked into execute various payloads to ultimately down the sandbox (at Medium integrity level).


While Chrome has one of the most secure sandboxes in three years, we have now uncovered a reliable exploit despite its sandbox, ASLR and DEP.

For security reasons, the exploit code and technical details of the underlying vulnerabilities will not be publicly disclosed. They are available to our customers as part of our vulnerability research services.

Note: The exploit works on both Windows 7 and Windows 8.

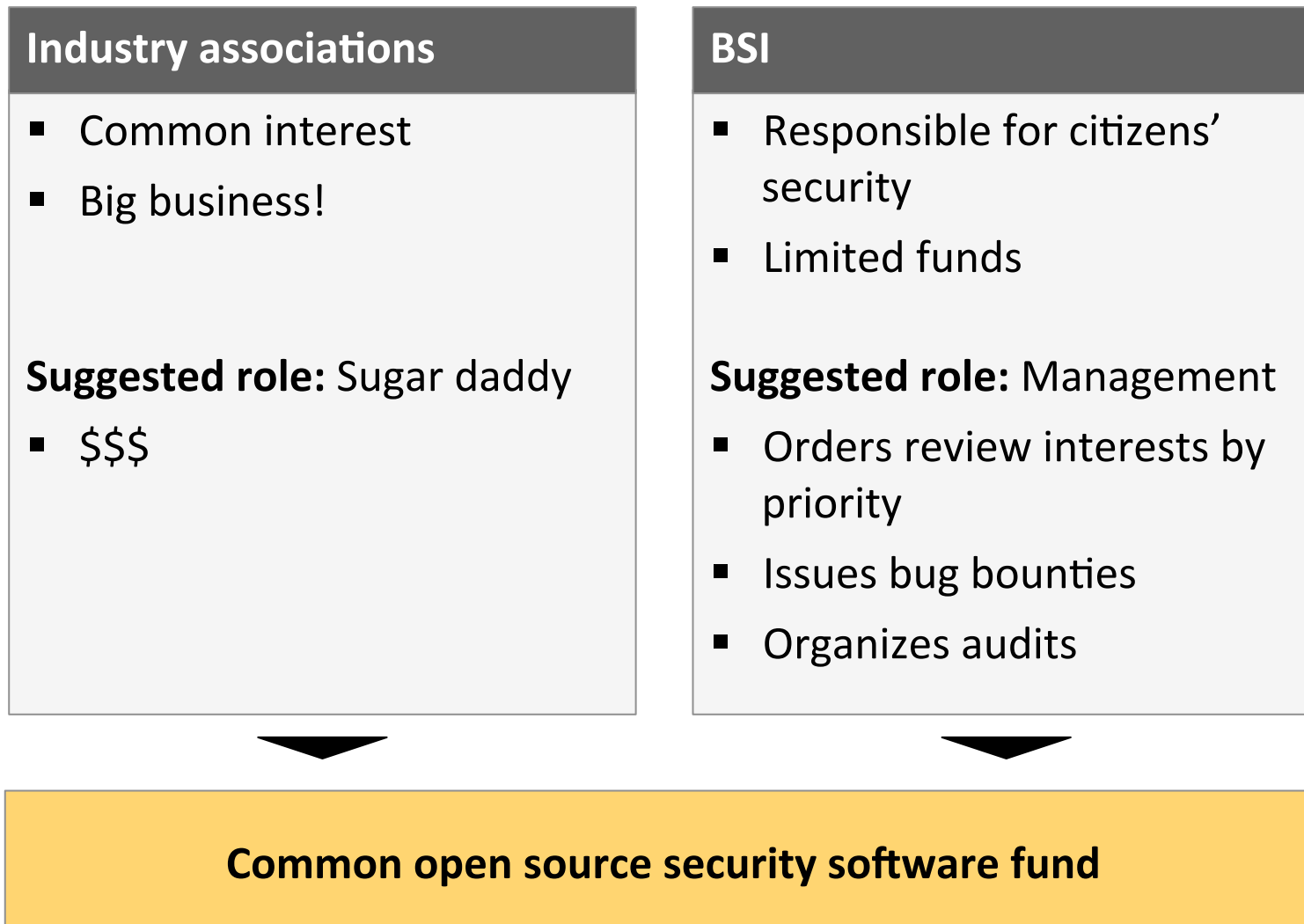
VUPEN Solutions

 [Contact Us](#)



“For security reasons, the exploit code and technical details of the underlying vulnerabilities will not be publicly disclosed. They are available to our customers as part of our vulnerability research services.”

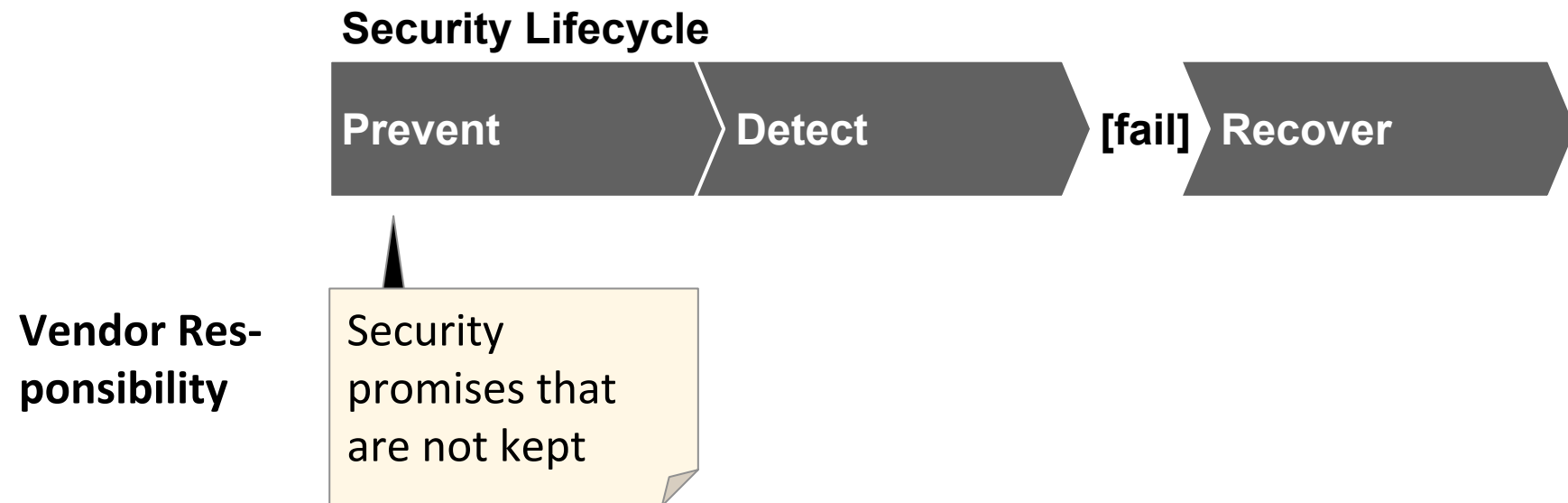
I If everybody benefits, why shouldn't everybody pay their share?



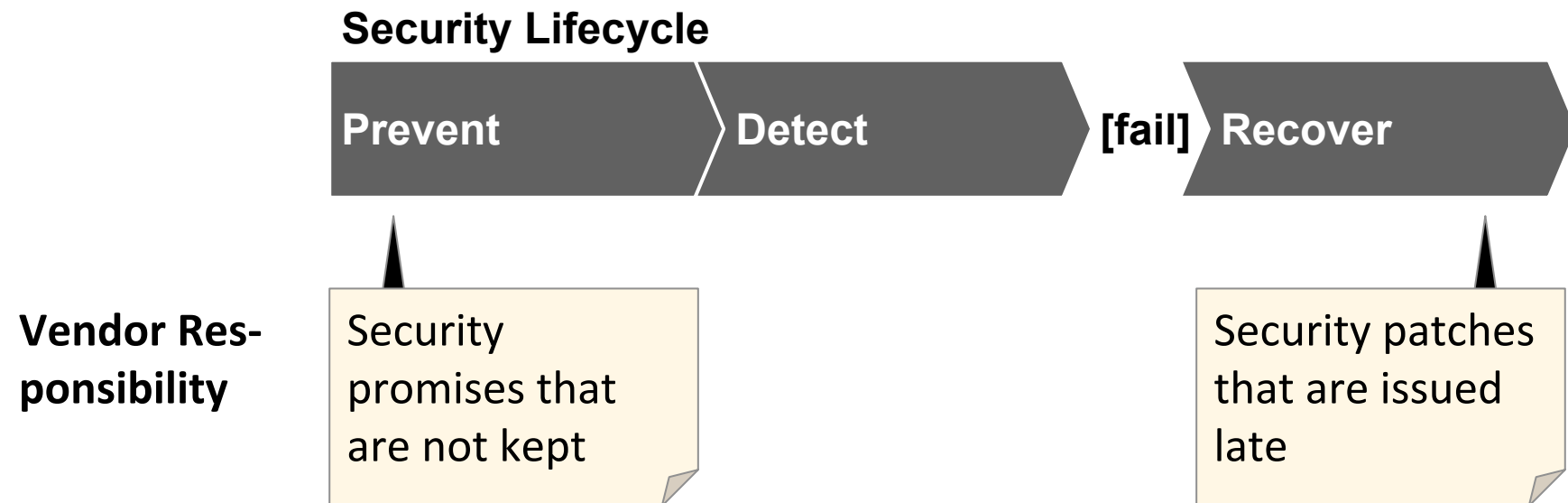
I Liabilities are strong economic incentives...



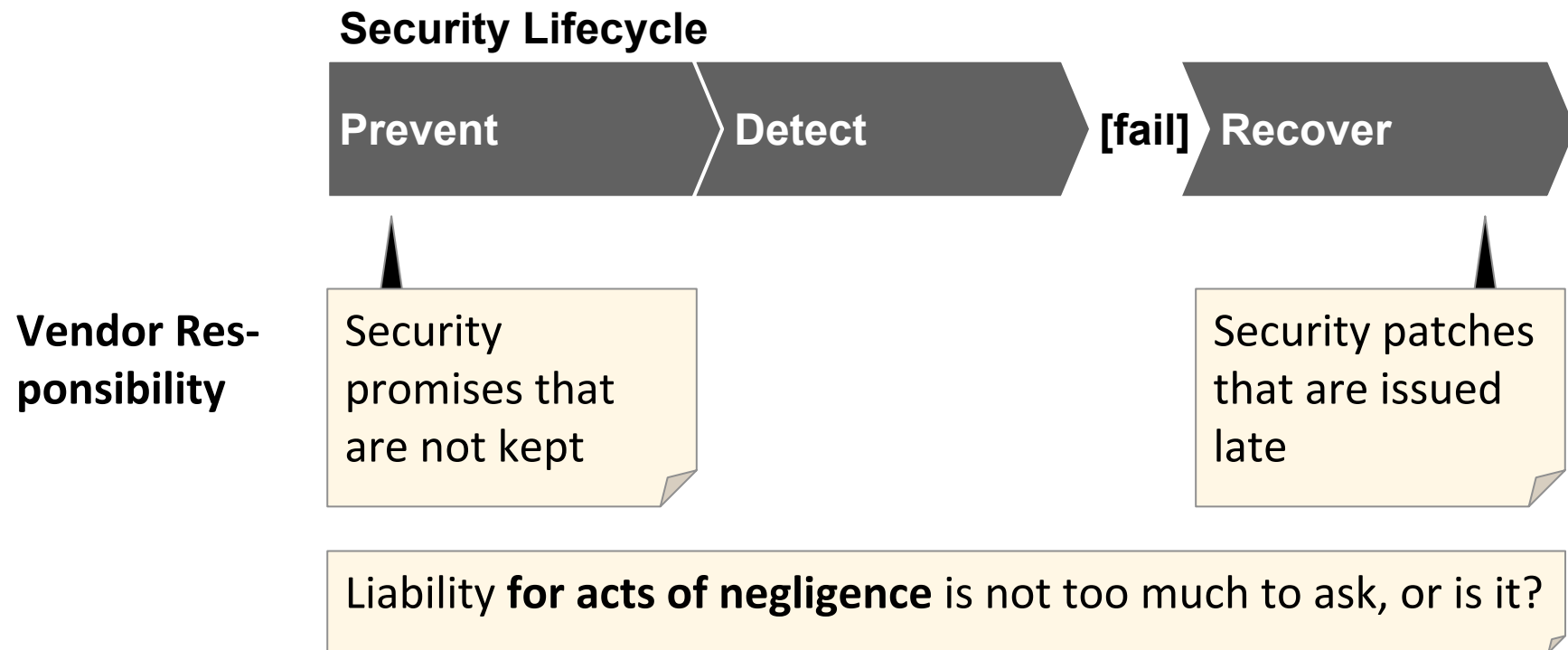
I Liabilities are strong economic incentives...



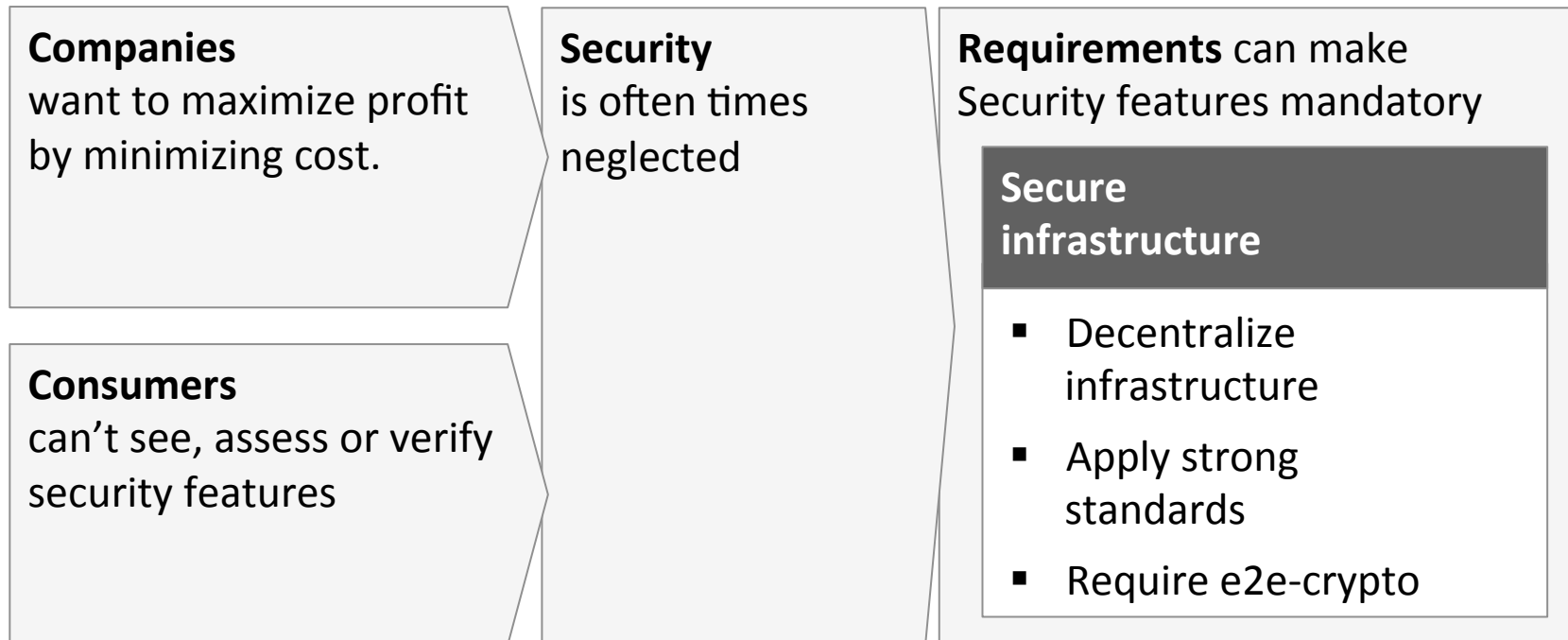
I Liabilities are strong economic incentives...



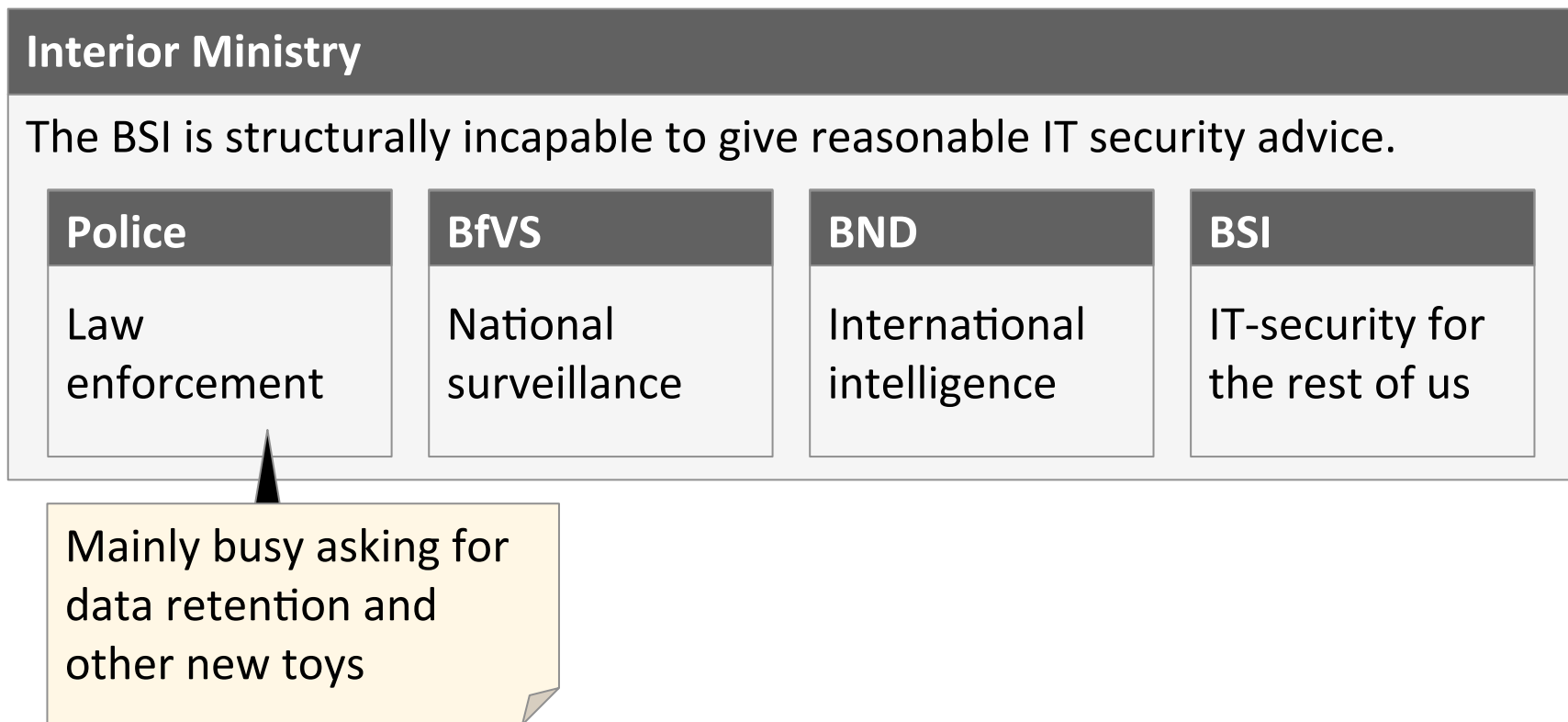
I Liabilities are strong economic incentives...



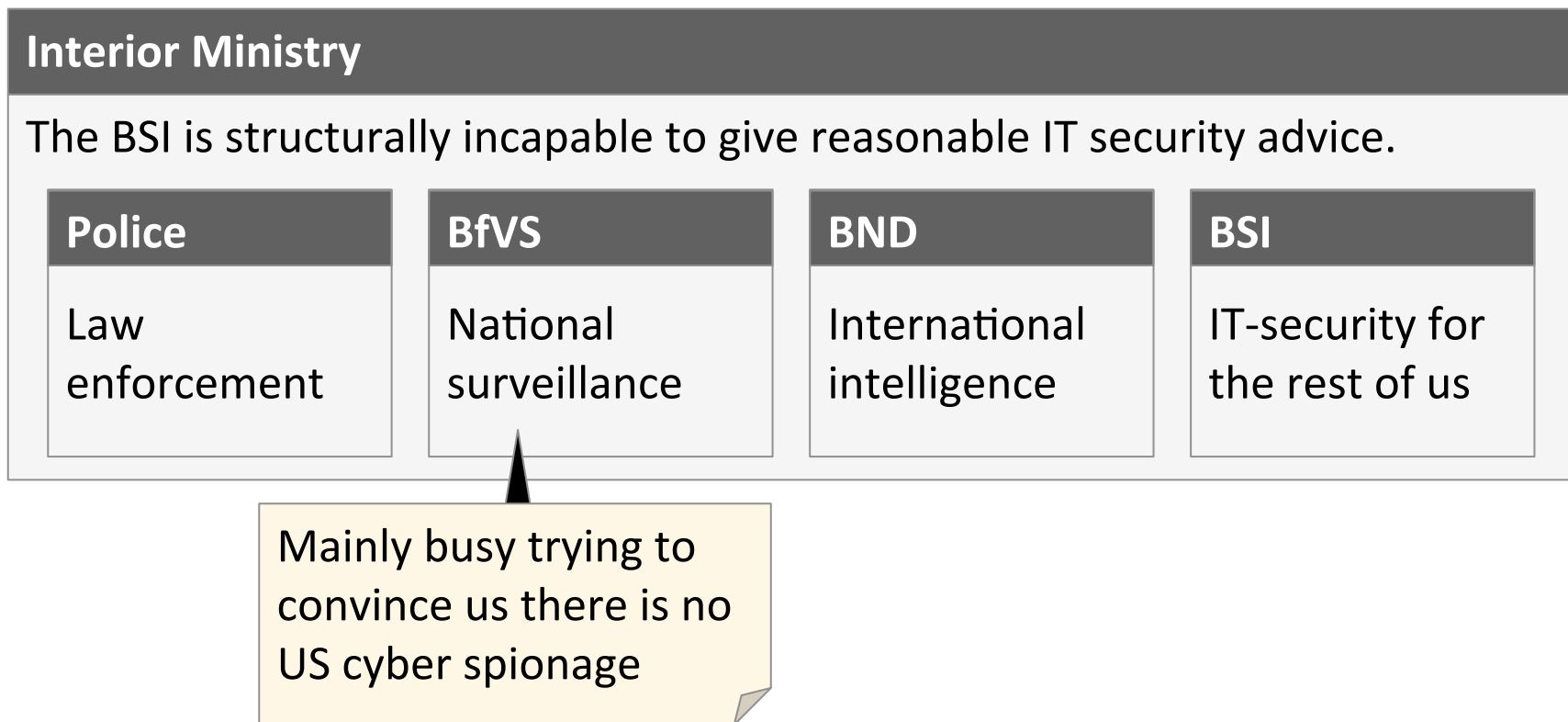
II Requirements should finally demand state-of-the art security instead of the bare minimum



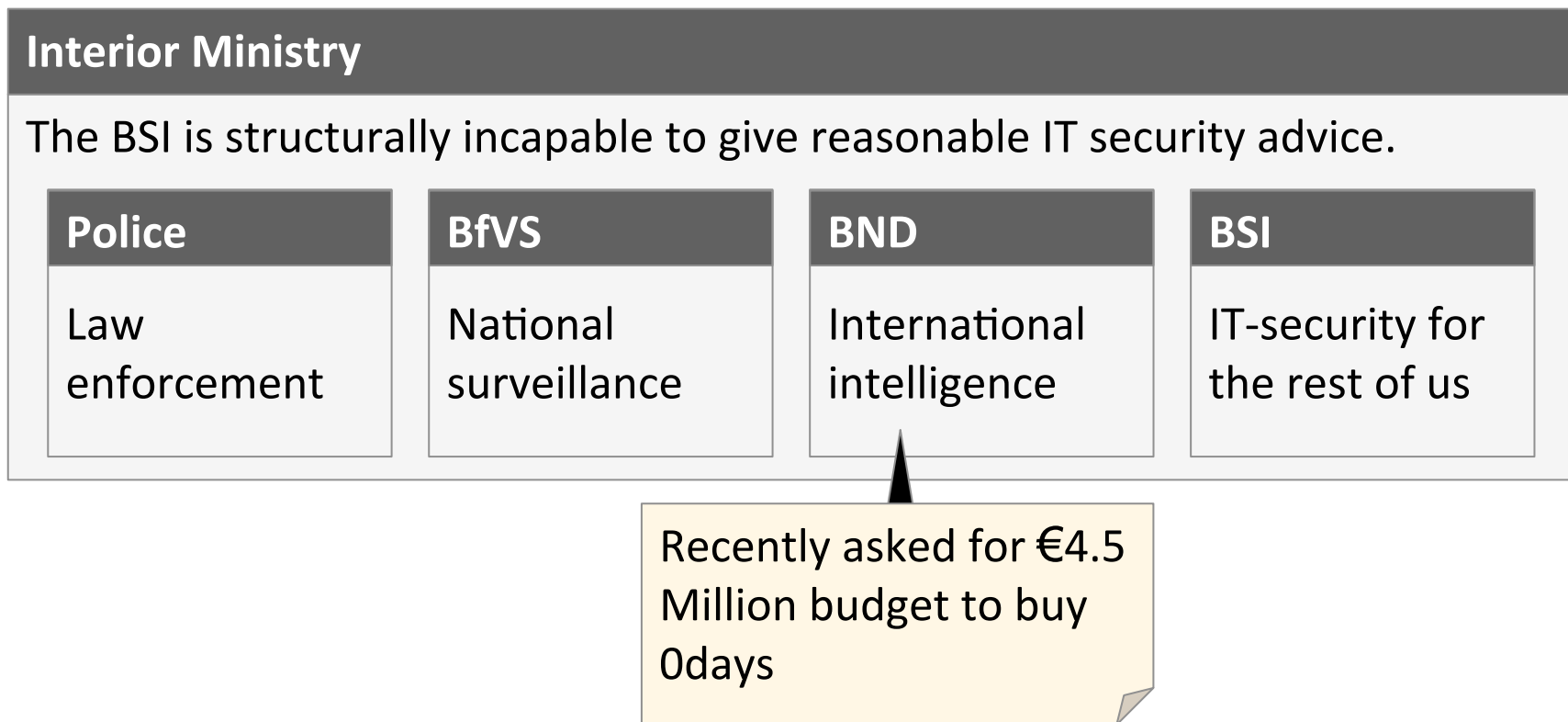
II The Interior Ministry's inherent conflict of interests must be resolved



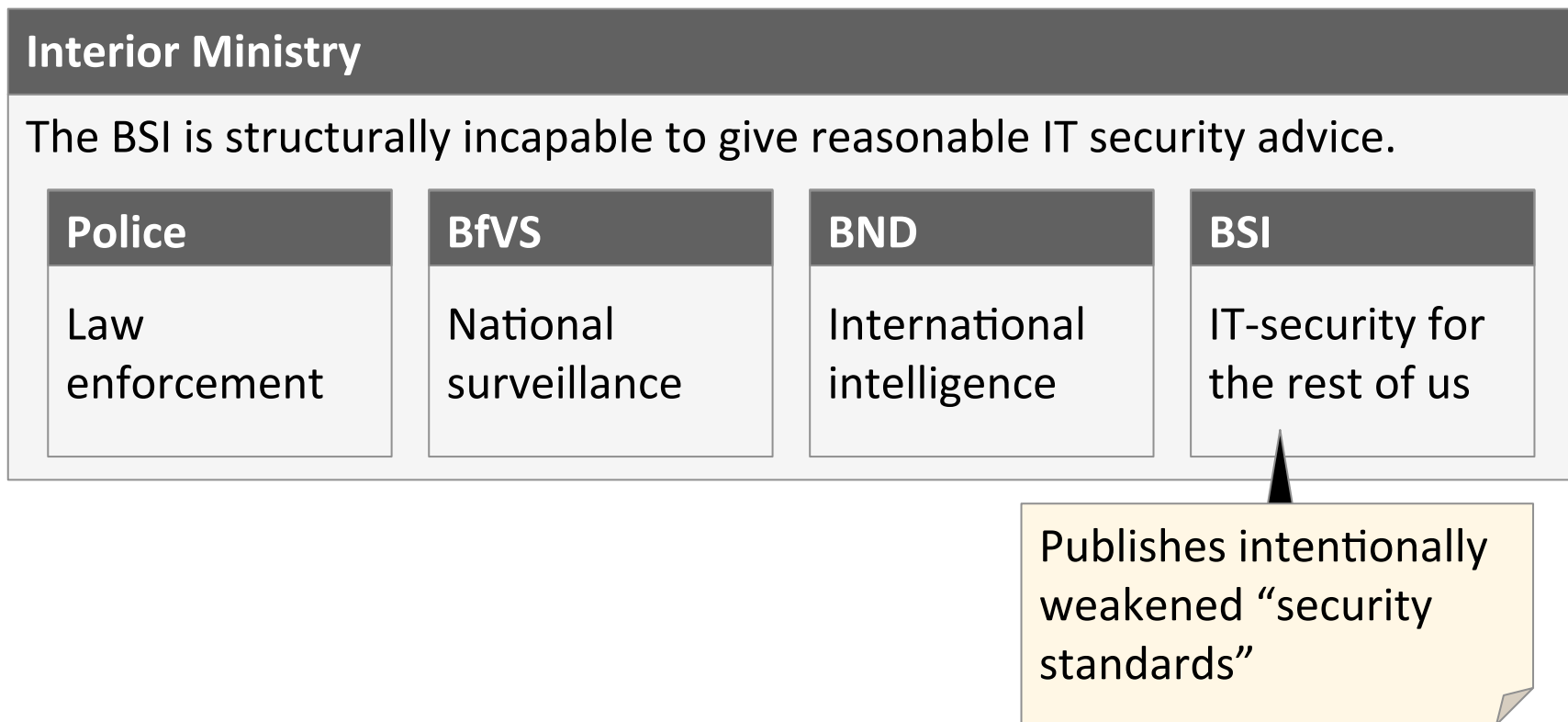
II The Interior Ministry's inherent conflict of interests must be resolved



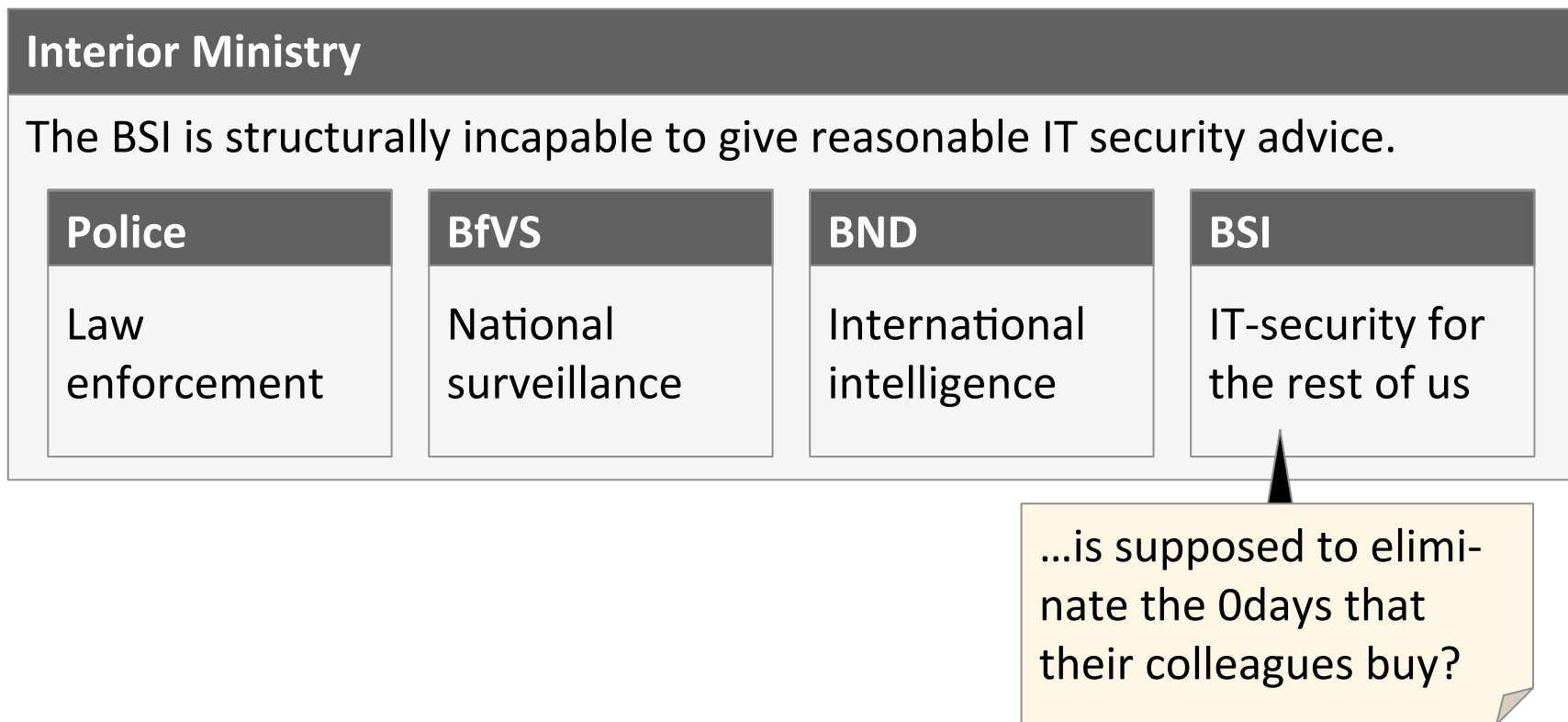
II The Interior Ministry's inherent conflict of interests must be resolved



II The Interior Ministry's inherent conflict of interests must be resolved



II The Interior Ministry's inherent conflict of interests must be resolved



II The Interior Ministry's inherent conflict of interests must be resolved

