itopia
corporate information technology

Cyber risks in the financial industry

Costs and effects

Zurich, 31 May 2024

daniel.zuber@itopia.ch

benjamin.schlup@itopia.ch

Summary

– The mean value of **total costs** to **mitigate cyber risks** lies between **7% and 8% of IT budget** of all participating institutes.

– **At 3 institutes**, these costs are - in some cases significantly - **above the perceived maximum acceptable costs** of around **10-15% of the IT budget**; for **all other participants**, **95%** of this maximum **is utilised** on average.

– Over the **next five years**, the participants expect costs to **increase by 10% p.a**. In the **last five years** - depending on the institution - **cost growth** of between **5% and 20% p.a.** was reported.

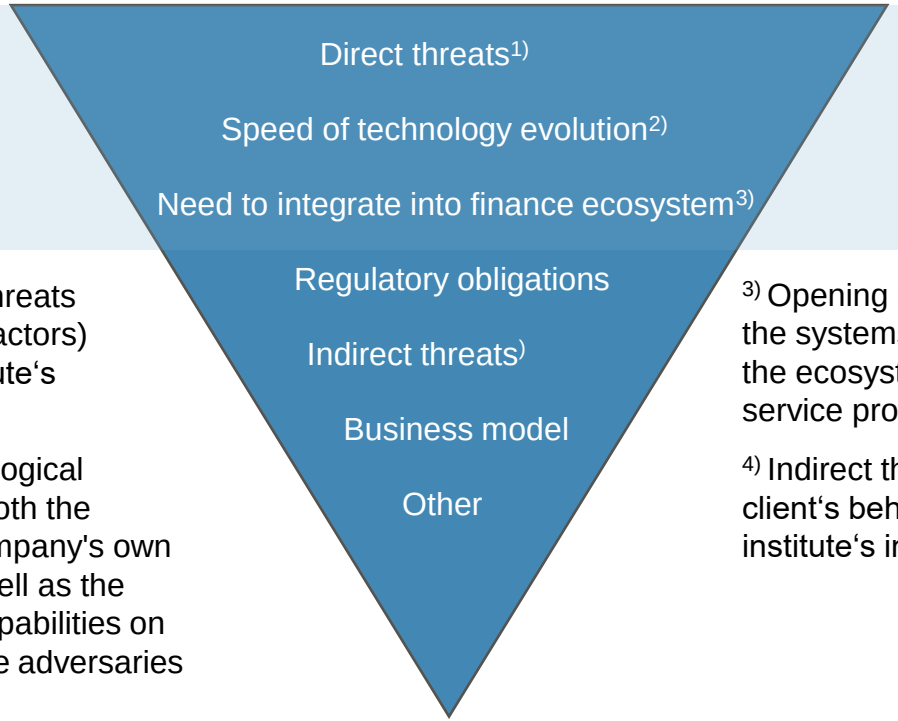
– **Direct threats** to the infrastructure of the participating institutes are reported as the main cost driver. **Technological development** is likely to be responsible for driving the cost increase. The third main driver is the importance of **integration into the ecosystem** of financial service providers.

– The reported **investment priorities** primarily show investments in **risk management of the IT supply chain** and in **improving detection**, thus addressing some of the main drivers.

– **Risk assessment** is carried out for all participants according to the **widely used procedure,** i.e. with the product of probability of occurrence and impact.

Ranking of cost drivers

Top 3 cost drivers for banks



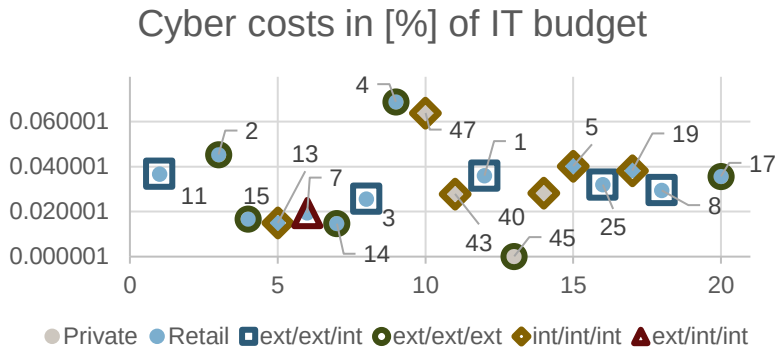
1) Direct threats= threats (and professional actors) targeting the institute‘s infrastructure

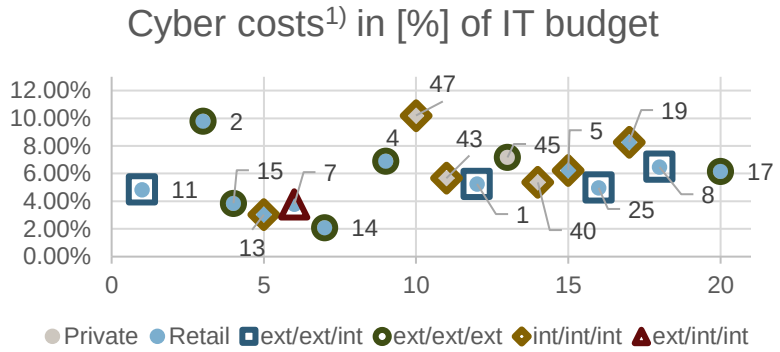
2) Speed of technological evolution affects both the changes in the company's own infrastructure as well as the development of capabilities on the side of possible adversaries

3) Opening up and connecting the systems for integration into the ecosystem of financial service providers

4) Indirect threats = threats (e.g. client‘s behaviour) impacting the institute‘s infrastructure

Total costs for cyber

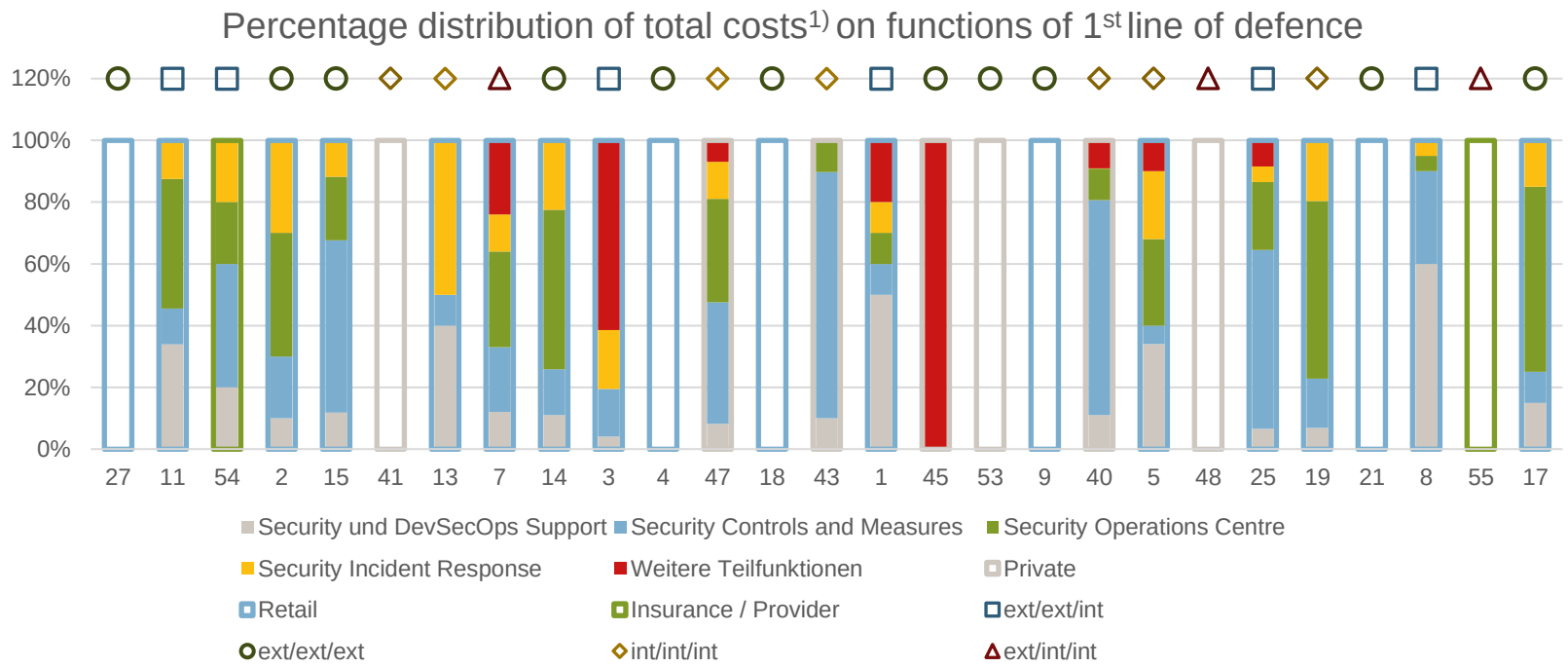




- Total costs for cyber (including costs for personnel) are close to the average maximum limit of 10-15% of the IT budgets, in 3 cases above the individually specified limit.
- Costs tend to be higher for private banks (median: 6.4%) than for retail banks (median: 5.7%).
- The sourcing model does not appear to have a major effect on the overall costs, but does have an influence on the specific cost distribution within the 1st, 2nd and 3rd line of defence functions.

1) Including estimation of costs for personnel

Cost distribution within 1st line of defence



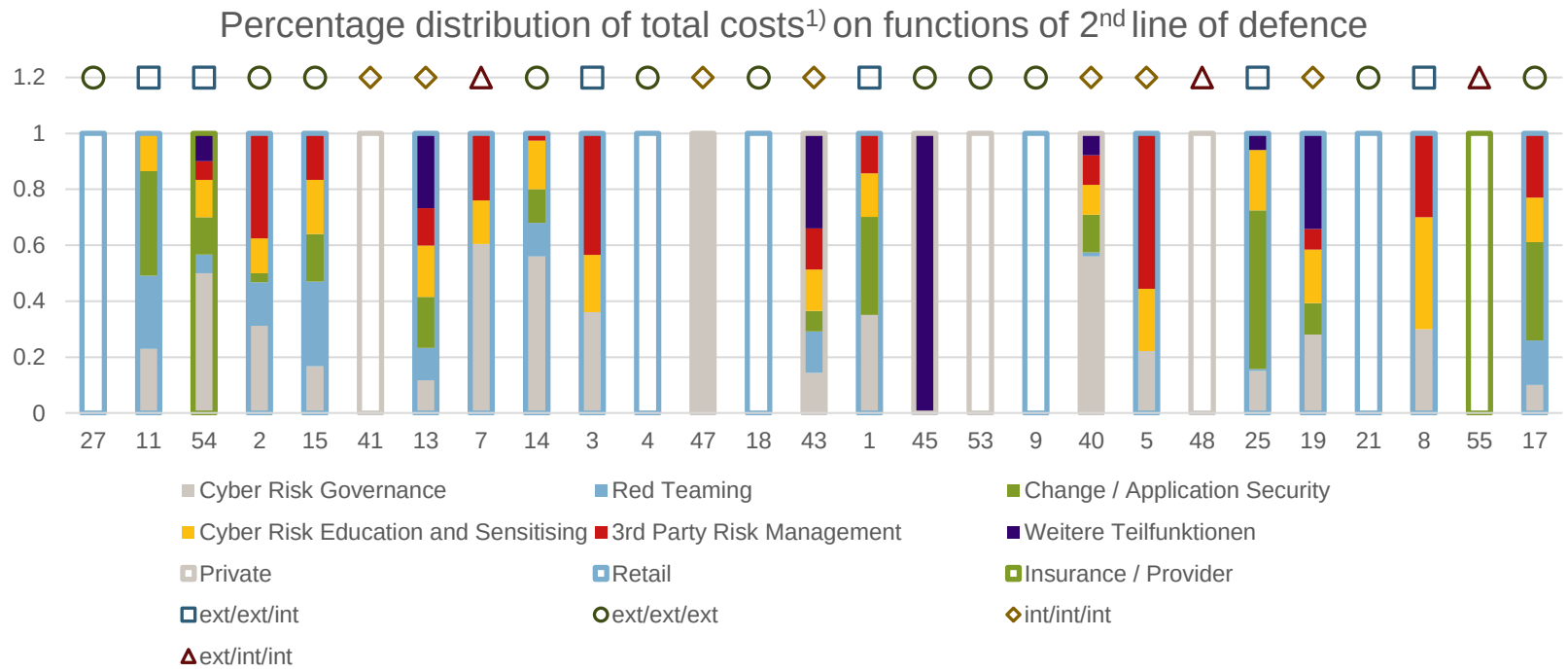
1) Total costs of the 1st line of defence incl. estimated personnel costs

Cost distribution within 1st line of defence

Findings

- The *DevSecOps support* spend is highly dependent on the sourcing model; main drivers of this spend being security architecture and vulnerability scanning. Investment priorities are moving towards automation of DevSecOps and security testing. Other aspects are cloud and network security, red teaming and bug bounties.
- The proportion of operational expenditure for *Security Controls and Measures* is considerable for in-house operations; the main drivers being intrusion detection and prevention systems. Investment priorities are set for data leakage prevention.
- The costs for *Security Operations Centres* and *Security Incident Response* are driven by external services. Their optimisation is the top investment priority. Investment in the automation of incident response is prioritised heavily by retail banks.
- Other sub-functions that are performed in the 1st line of defence organisation of the participating institutes include IT security lead, supply chain risk management and operational tasks (e.g. authorisations).

Cost distribution within 2nd line of defence



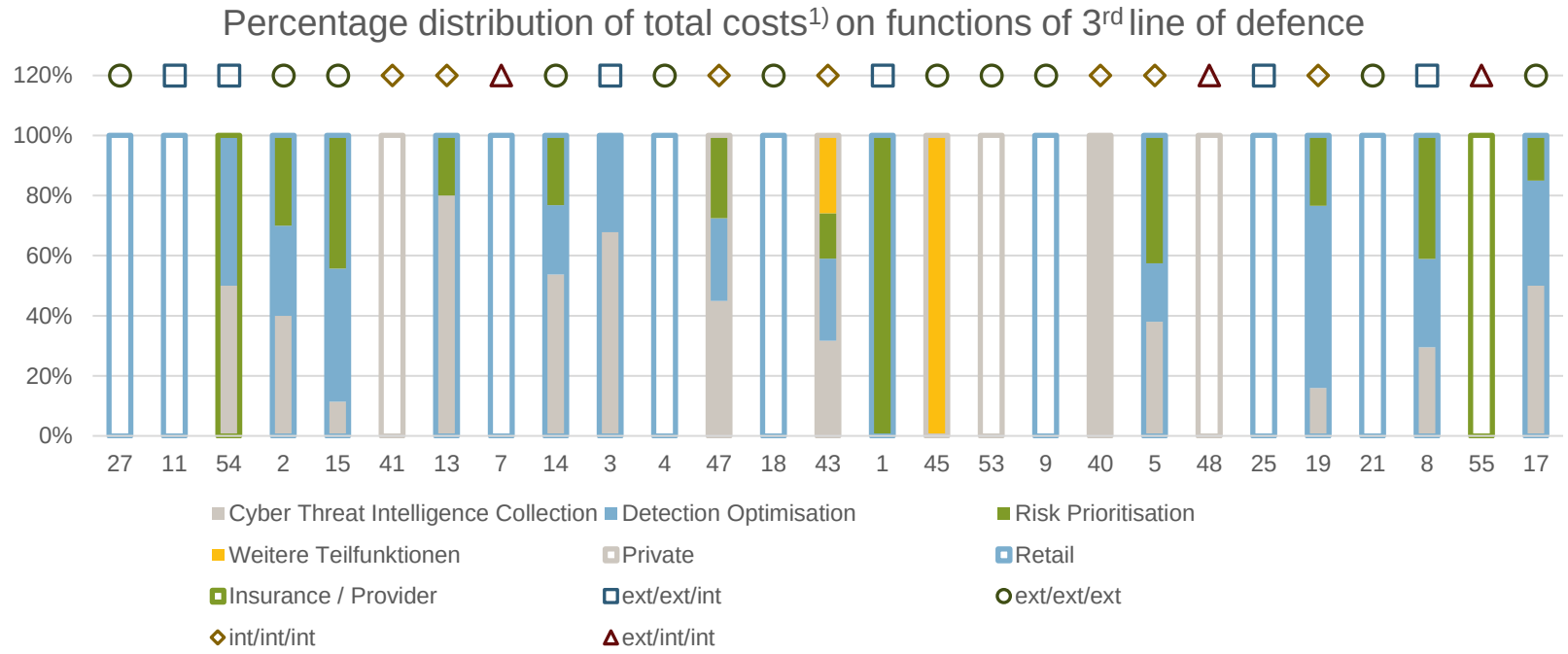
1) Total costs of the 2nd line of defence incl. estimated personnel costs

Cost distribution within 2nd line of defence

Findings

- *Cyber risk governance* currently generates the main cost burden across all banking institutions within 2nd line of defence, while *change and application security* are the main cost drivers for the participating other financial service providers.
- *3rd party risk management* and *cyber risk education and sensitizing* are just under 15% of 2nd line of defence costs on average.
- Investment priorities are *3rd* party risk management followed by cyber risk governance.
- Other sub-functions performed in the 2nd line of defence organisation of the participating institutions include BCM standardisation, IT security PL, IAM governance, IT risk management and penetration tests.

Cost distribution within 3rd line of defence



1) Total costs of the 3rd line of defence incl. estimated personnel costs

Cost distribution within 3rd line of defence

Findings

- Private banks tend to spend more overall on cyber threat intelligence (CTI) collection than retail banks.
- The cost driver of the 3rd line of defence across all institutions is clearly *cyber threat intelligence collection.*
- According to all participants, the investment priority is detection optimisation, i.e. improving detection capability, e.g. through optimised detection patterns.
- Risk prioritisation is not seen as the main driver of costs and is therefore not an investment priority.
- Other sub-functions that are performed in the 3rd line of defence organisation of the participating institutes were not specified.

Contact

itopia ag
corporate information technology
technoparkstrasse 1
ch-8005 zürich

tel. +41 44 355 56 00

www.itopia.ch