

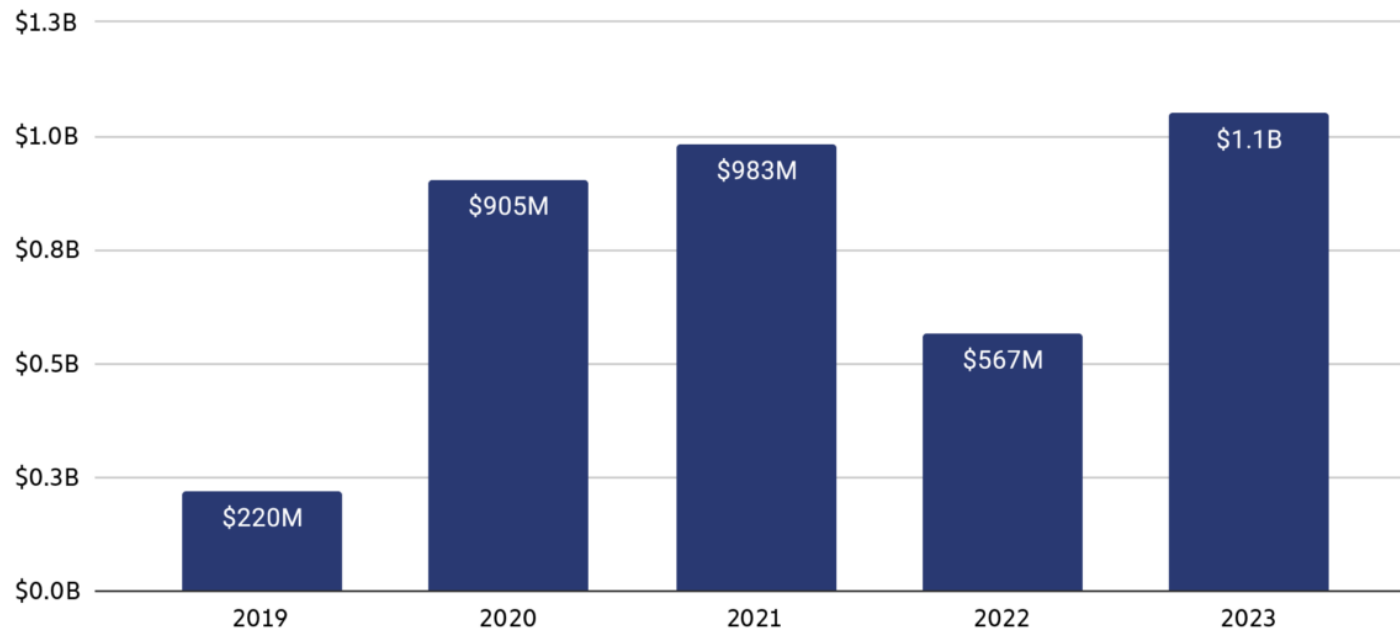
Small and Medium Organisations : Paving the way for effective resilience



SSCC webinar
6th of June 2024
Nicolas Frey

Dangers

Total value received by ransomware attackers, 2019 - 2023



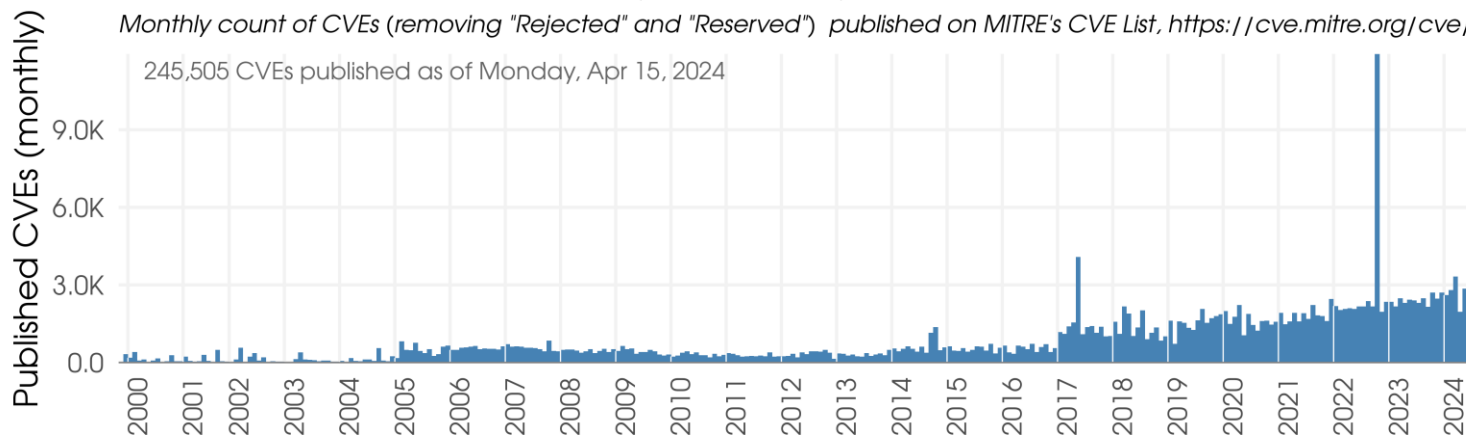
© Chainalysis

- Average ransom in 2023 : **700'000\$**
- **2022 : war in Ukraine and collapse of Conti Group**

Vulnerabilities

Monthly counts of CVE publications (MITRE CVE List)

Monthly count of CVEs (removing "Rejected" and "Reserved") published on MITRE's CVE List, <https://cve.mitre.org/cve/>



Source: https://first.org/epss/data_stats, 2024-04-15



Have been exploited in 2023/2024 :

- Fortinet
- Palo Alto
- 1Password
- Microsoft
- Sonicwall
- SSH / XZ
- To be continued ...

Cyber risk 101



How to protect an organisation should depends on what it has to lose :

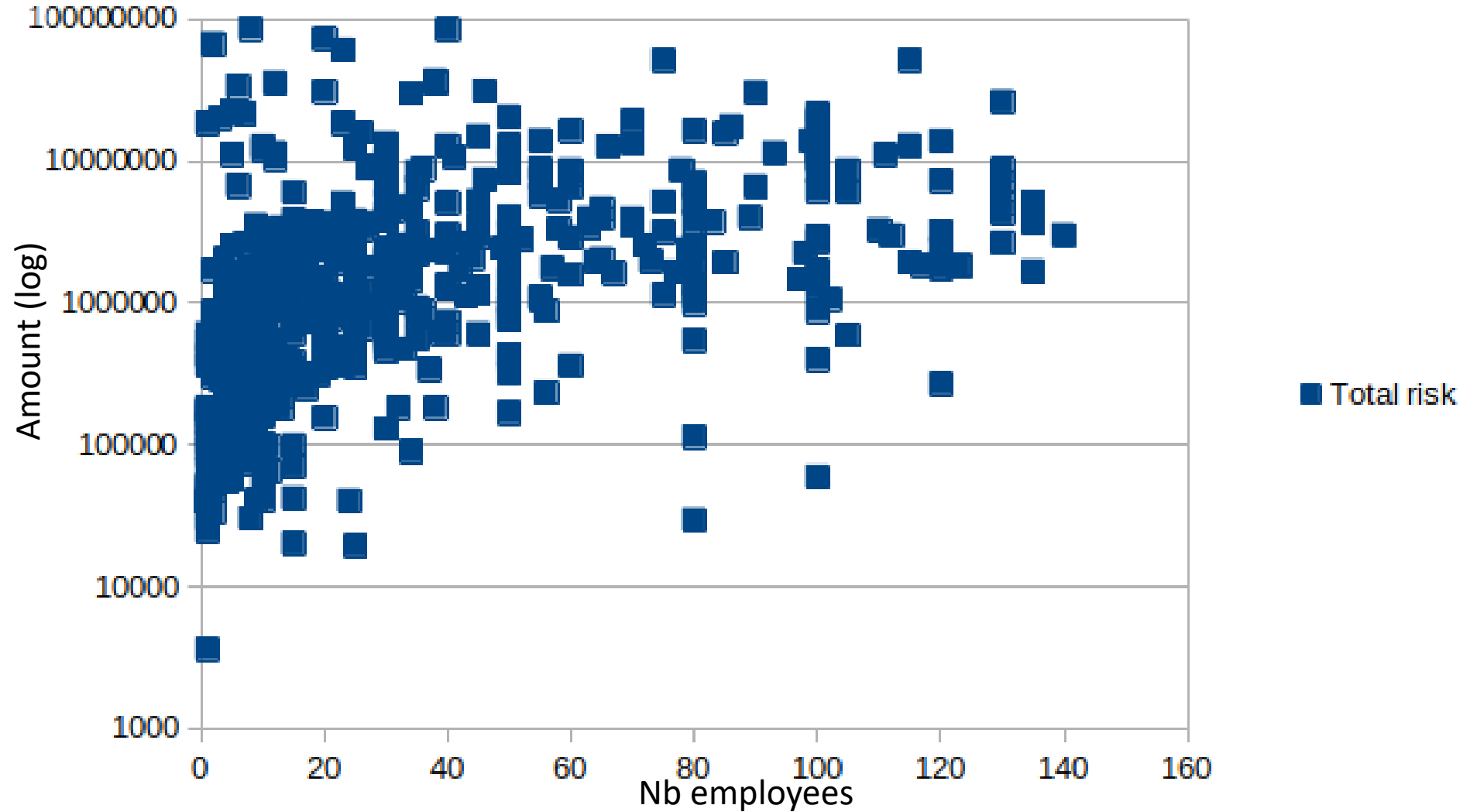
Which impacts in case of cyber incident ?

=> The starting point

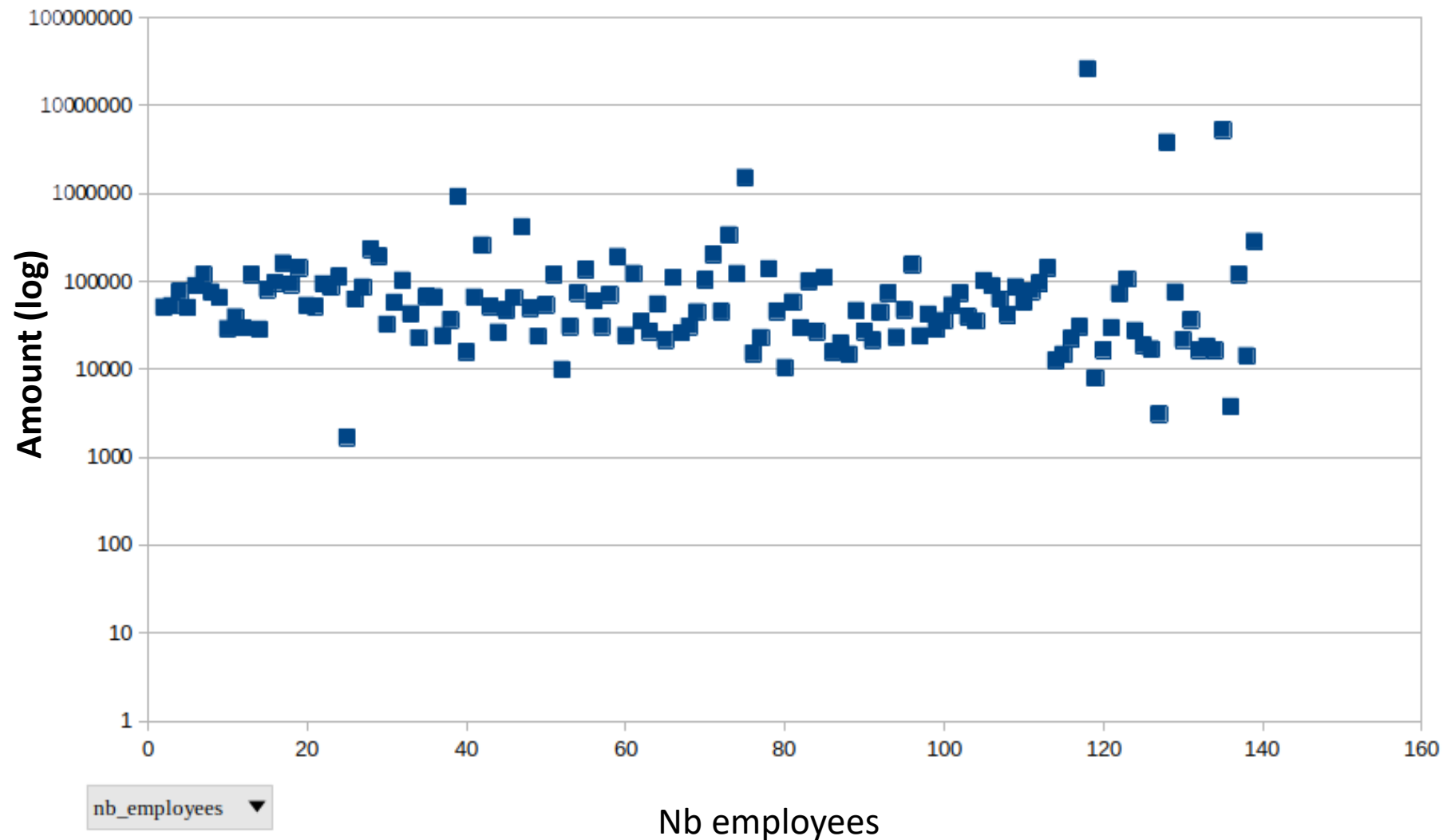
Data types :

- **Administrative**
- **Financial**
- **Personal data**
- **...**

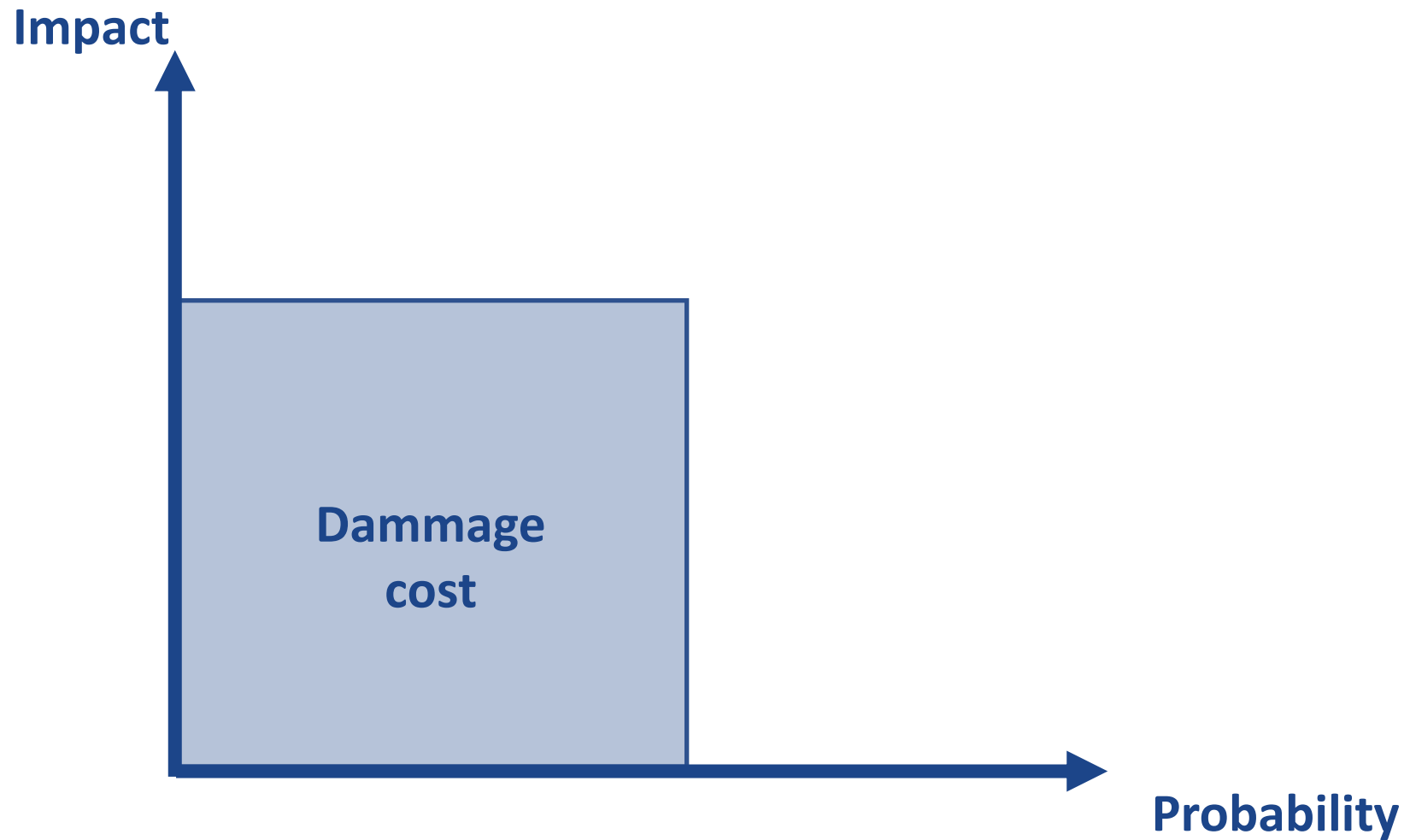
SME evaluated risks



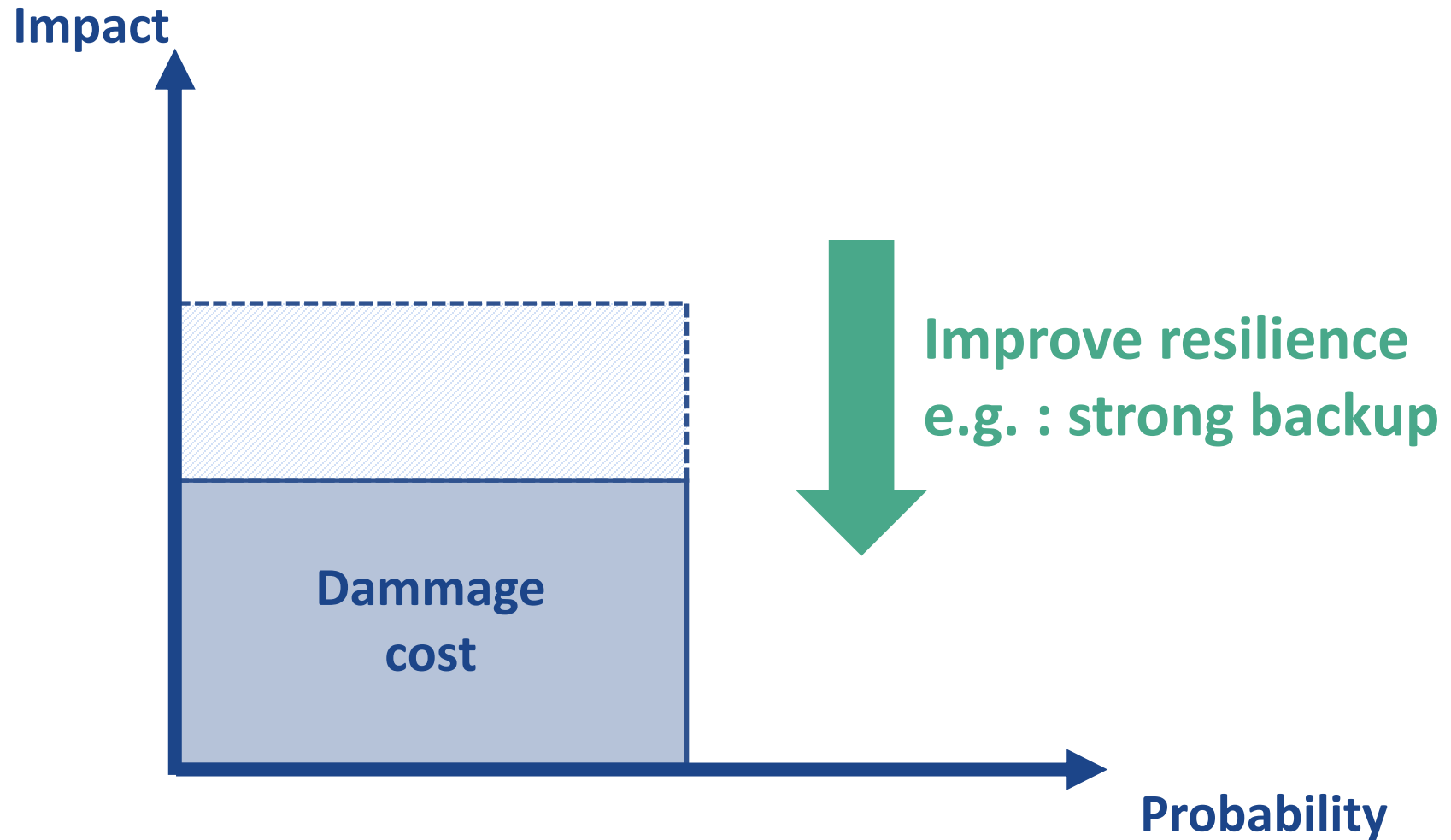
SME evaluated risks / employee



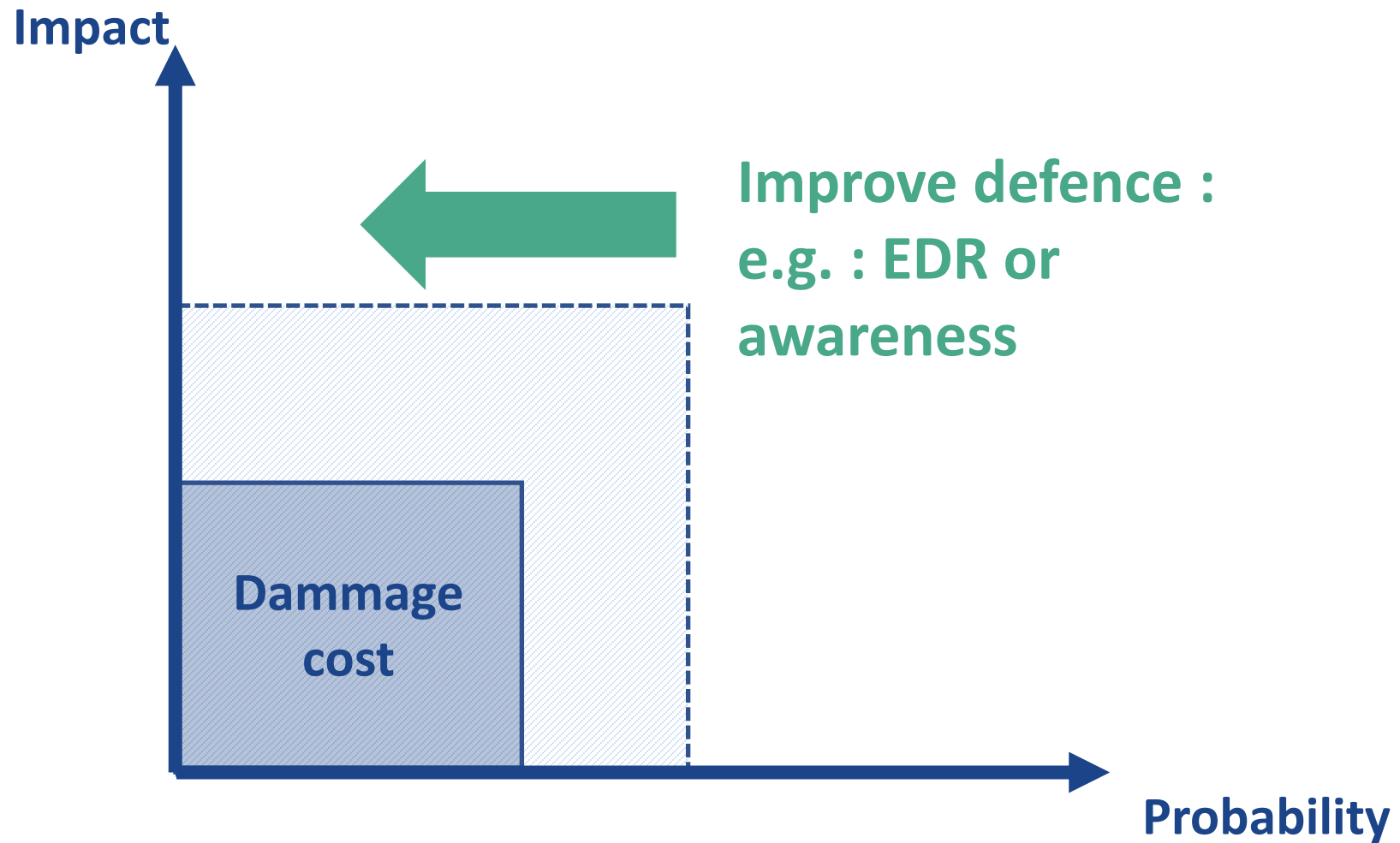
Cyber risk reduction



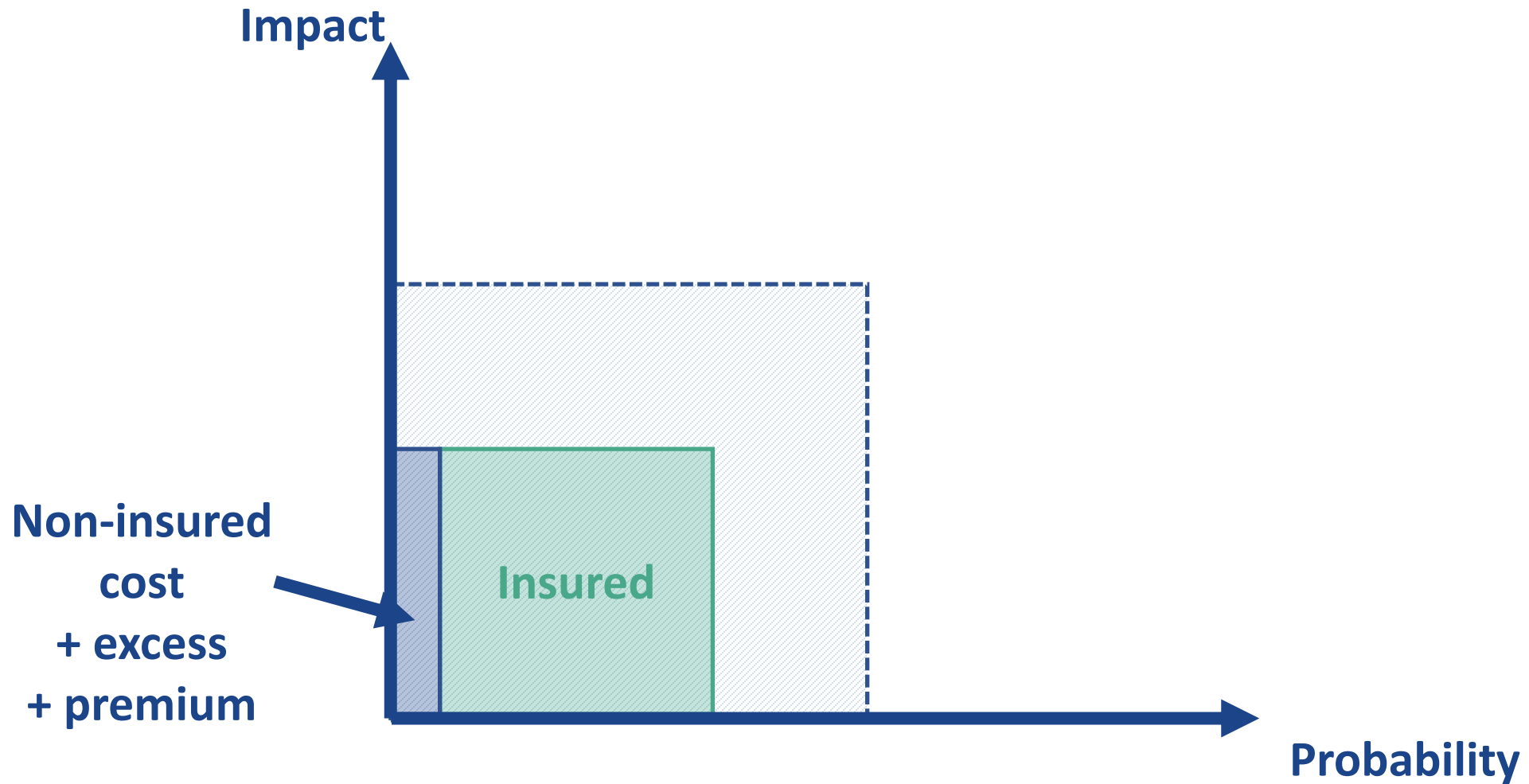
Cyber risk reduction



Cyber risk reduction



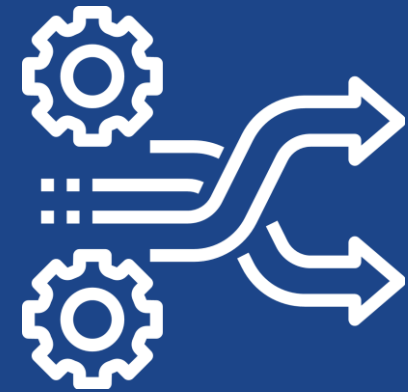
Cyber risk reduction



Results from the ground

- **Next come statistics of the status of organisations which started the Labelling process.**
- **Pool size : ~550 organisations in Switzerland, from 2 to 1000 employees.**
- **The organisations that finished the process had all been checked as compliant.**

This is not entirely representative of Swiss organisations, since these are the ones that have undertaken such a process.



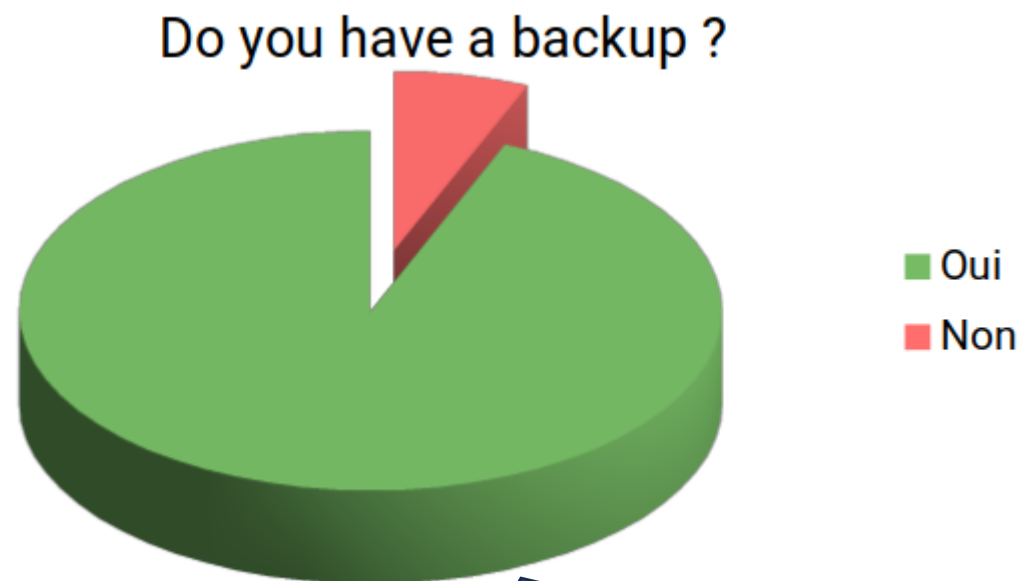
Results from the ground

Are antivirus alerts collected ?



When tested, the reaction time was often too long (sometime days).

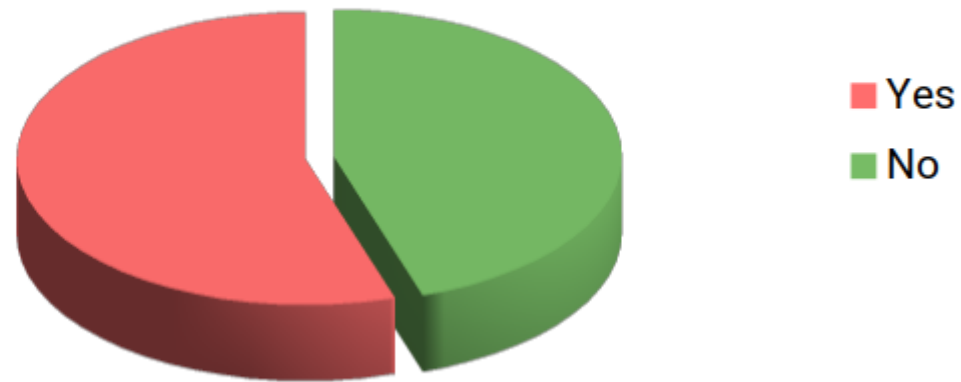
Results from the ground



Good news ! Quite every organisation has backups of their systems, but...

Results from the ground

Can admin account destroy all backups ?



Most of the time, an attacker can destroy them all simply by getting admin rights.

Results from the ground

Do you have a recovery plan ?



Finally, most organisations never thought about the recovery process....

Which requirements are related to resilience ?

Faster recovery

- Backups every day [3.3.5.1-9]
- Backups are unreachable for ANY account in the organisation [3.3.5.10]
- Recovery plan must exist, be tested and a minimal checklist should be completed [3.3.6.1-3]

Limit the malware spread :

- Internal contact point => faster reaction [3.1.1.1+2]
- Permission list => least privilege + easier forensics [3.1.1.4]
- Data matrix : Which data exists and where + sensitivity levels [3.2.1.1+2]
- Encrypt sensitive data [3.2.2.2+3]
- Use MFA [3.2.2.4]
- No high level vulnerabilities in internal network [3.2.5.1]
- AV on every device + check alerts [3.3.4.4+5]
- Passwords manager must be used [3.3.7.2]

Requirements published in
Creative Commons :
<https://www.cyber-safe.ch/exigences/>

Cyber-Safe Label

Diagnostic:



Cahier des charges exigences
V2.0 - 25 novembre 2019

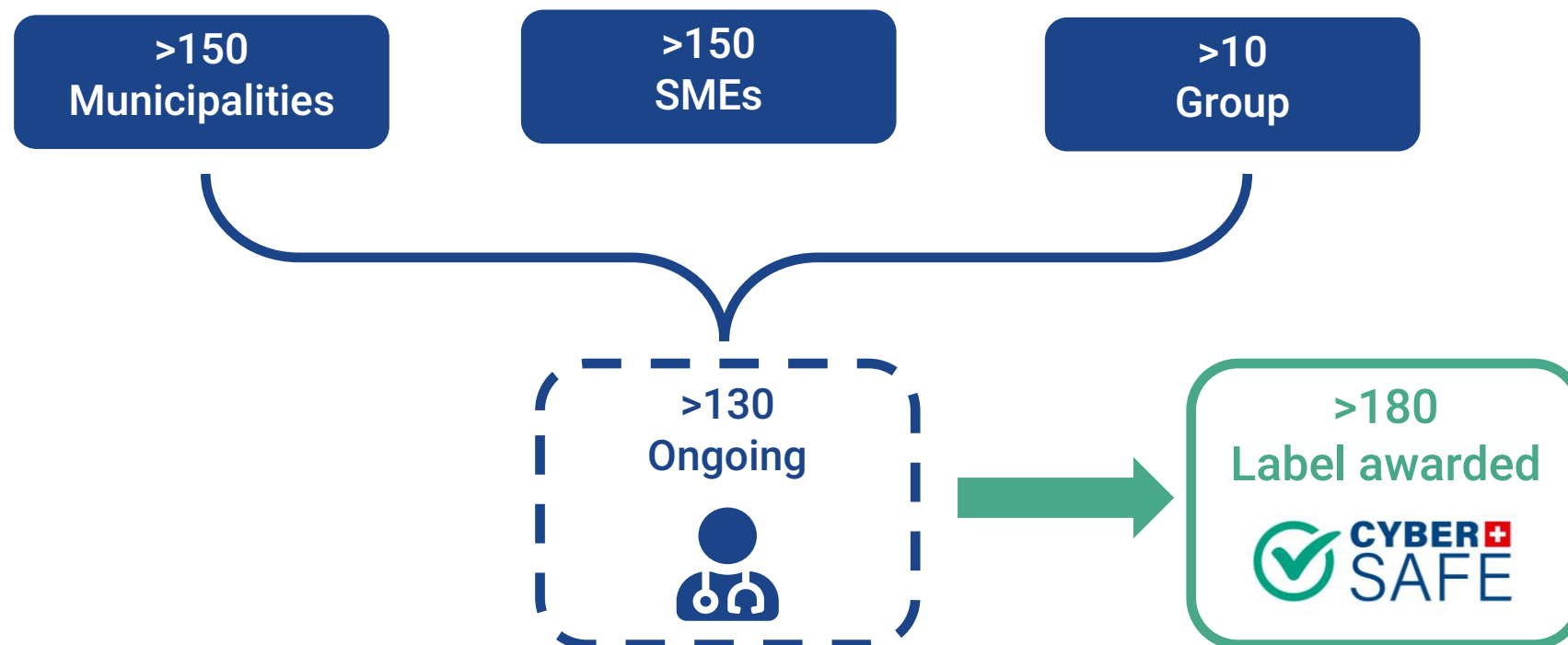
Table des matières

1 Introduction	2
1.1 Objectifs du document	2
1.2 Principes du Label cyber-safe	2
1.3 Terminologie	3
2 Conditions d'obtention du Label	5
2.1 Générales	5
2.2 Valeur des données	5
2.3 Catégories d'exposition	5
3 Exigences pour l'obtention du Label	6
3.1 Compétences et responsabilités	6
3.1.1 Ressources humaines	6
3.1.2 Test de phishing	7
3.2 Infrastructure IT	7
3.2.1 Inventaire	7
3.2.2 Chiffrement	8
3.2.3 WiFi	8
3.2.4 Accès physique	9
3.2.5 Scans internes	9
3.2.6 Scans externes	9
3.3 Organisation	10
3.3.1 Protection des données	10
3.3.2 Prestataires tiers	10
3.3.3 Ressources humaines	10
3.3.4 Procédures, routines	11
3.3.5 Sauvegardes	11
3.3.6 Nastices	12
3.3.7 Mots de passe	12
4 Annexe 1 - Principes en matière de protection des données	13

Checking:




Achievements (2024)



Who are we?

- Non-for-profit association
- Most of the umbrella organisations are part of the standardisation process
- Insurances recognise the Label
 - helvetia 
 - Allianz 
- Partner of :

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Defence,
Civil Protection and Sport DDPS
National Cyber Security Centre NCSC



sgvsusam

heig-vg
Haute école de gestion
Genève

ccig
Chambre de commerce, d'industrie
et des services de Genève

Trust4SMEs
Cybersécurité et confiance
numérique pour PME

FPE-CIGA
Fédération Patronale
et Économique

EPFL
C4DT
Center
for Digital
Trust

**Chambre Valaisanne
de Commerce et d'Industrie**
**Walliser Industrie-
und Handelskammer**

**Fédération des
Entreprises
Romandes**
Neuchâtel

Sicherheitsverbund Schweiz
Réseau national de sécurité
Rete integrata Svizzera per la sicurezza

UNION DES COMMUNES VAUDOISES

ISSS Information
Security Society
Switzerland

**SKO
ASC
ASQ** Association
suisse
des cadres

.!CON

Thank you for
your attention

[https://demo.
cyber-safe.ch](https://demo.cyber-safe.ch)

[nfrey@cyber-
safe.ch](mailto:nfrey@cyber-safe.ch)