Cybersecurity & Human Rights:
Technical Measures and the Private Sector

Eve Hunter
Cybersecurity East Project Expert
17.12.2020

EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Cybersecurity EAST

DETECON CONSULTING

Cybersecurity goals aim to protect organizations, but can also be important for the protection of human rights.

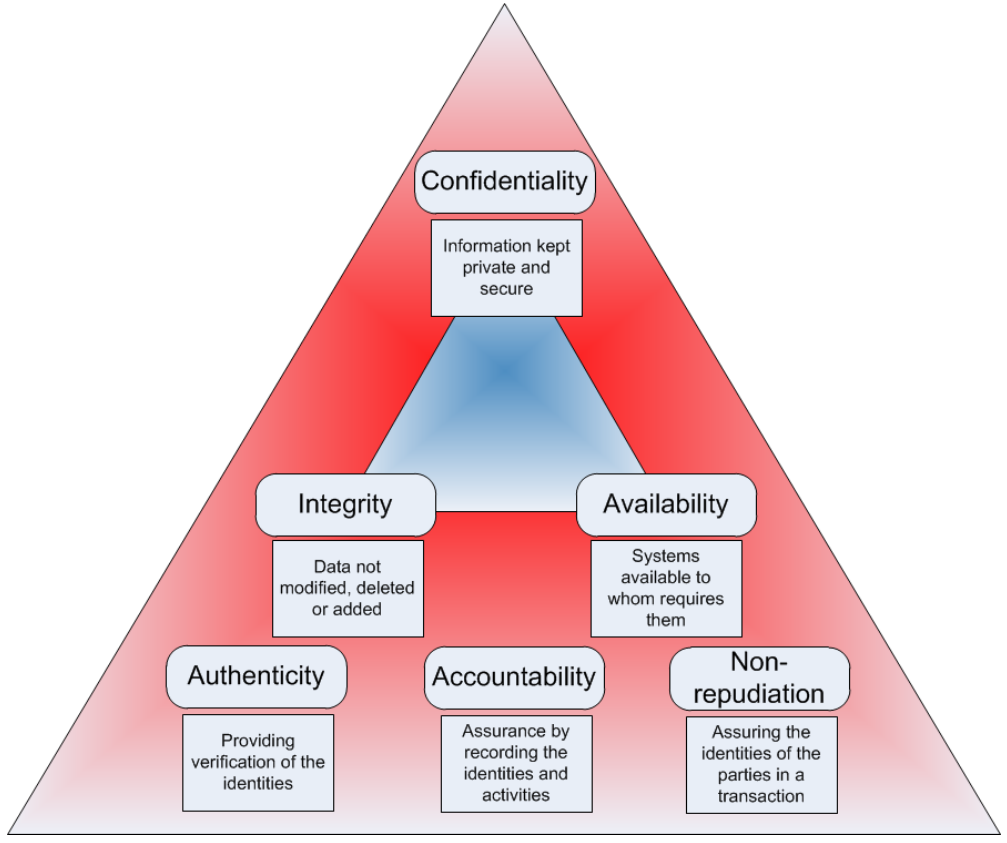
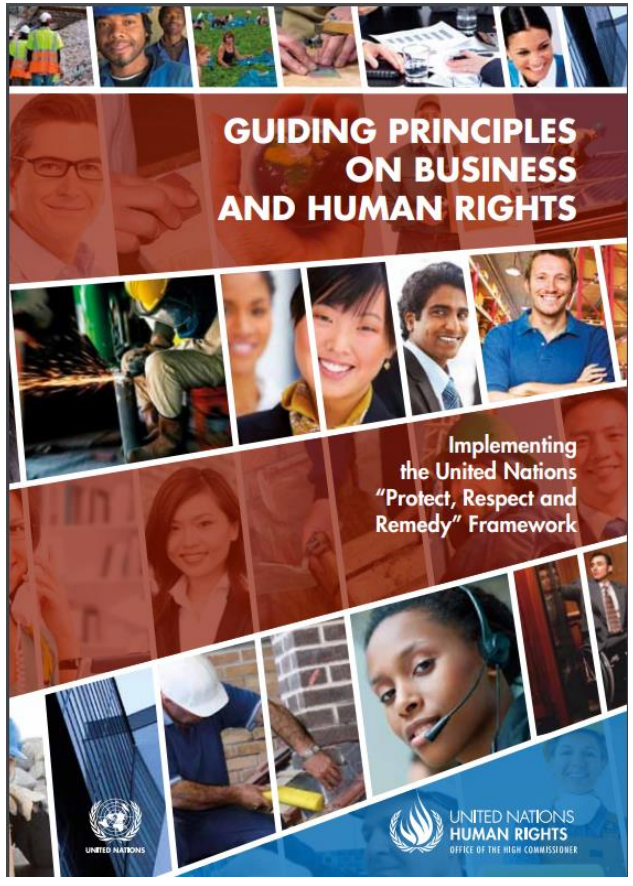


Image Source: GeraintW Photography

How can the private sector protect digital human rights by implementing cybersecurity measures?

“Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.”
– UN Guiding Principles on Business and Human Rights



Resources for Cybersecurity Implementation

- Standards – NIST, ISO
  - Voluntary
  - Mandatory (Regulated)
- Regulations
  - E.g. GDPR, NIS Directive
- Guidelines / Best Practices
  - Voluntary, driven by industry norms

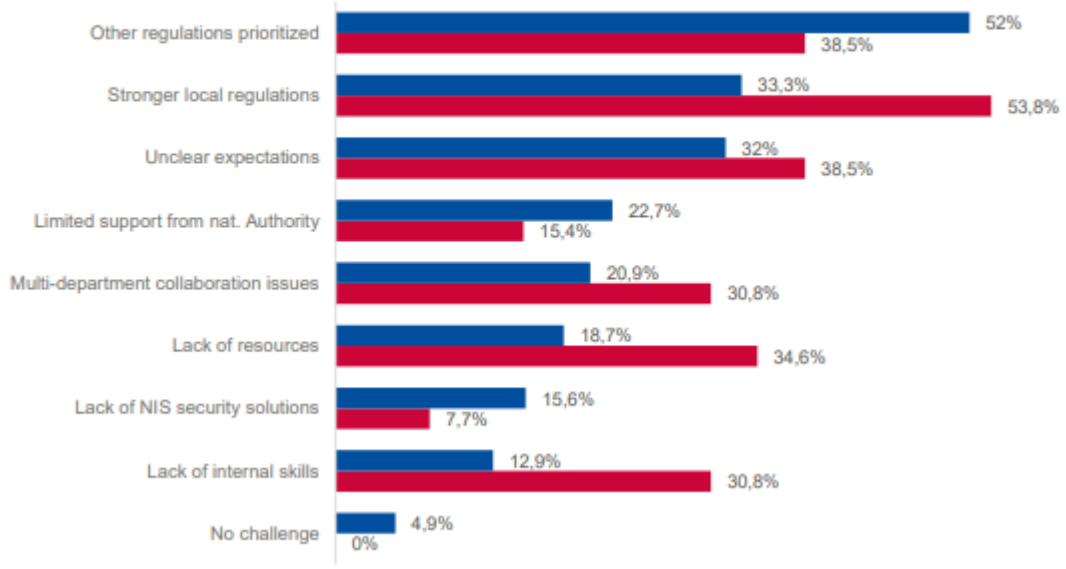
Regulation moves the private sector away from the bare minimum of cybersecurity towards best practices.

Use Case: NIS Directive for OES / CIP

- 80% of companies surveyed have completed or are in the process of implementing the NIS directive.
- Average budget - 175k €
- Clear benefit – 60% of surveyed organizations experienced a major security incident
- Most cited challenges:
  - The prioritization of other regulations e.g. GDPR.
  - The existence of stronger local regulations e.g. France's "Loi de Programmation Militaire" (LPM).
  - The lack of clarity of the NIS Directive expectations after transposition into national law.

ENISA NIS Investments Report – Dec. 2020

Figure 38: Main challenges in implementing the NIS Directive amongst surveyed organisations



Note: The red color indicates that the organization had no dedicated NIS Directive implementation program.

What technical measures are available to prevent digital human rights abuses?

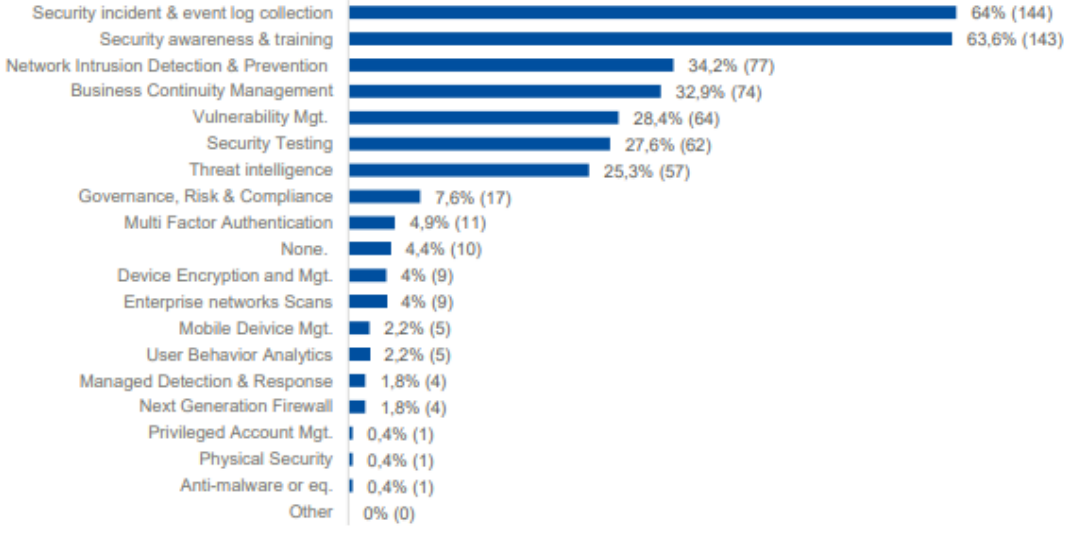
Unique Requirements for ISPs

The following are prohibited in order to protect human rights:

- Cutting access to individual customer accounts
- Revealing the identity of a user
- Actively monitor the content of communications or messages
- Removing content without verifying its illegality
- Blocking or filtering devices without a legitimate, transparent reason
- Actively seeking facts or circumstances indicating illegal activity on their own
- Not ensuring users to be able to use, adjust and control internet filters according to their needs

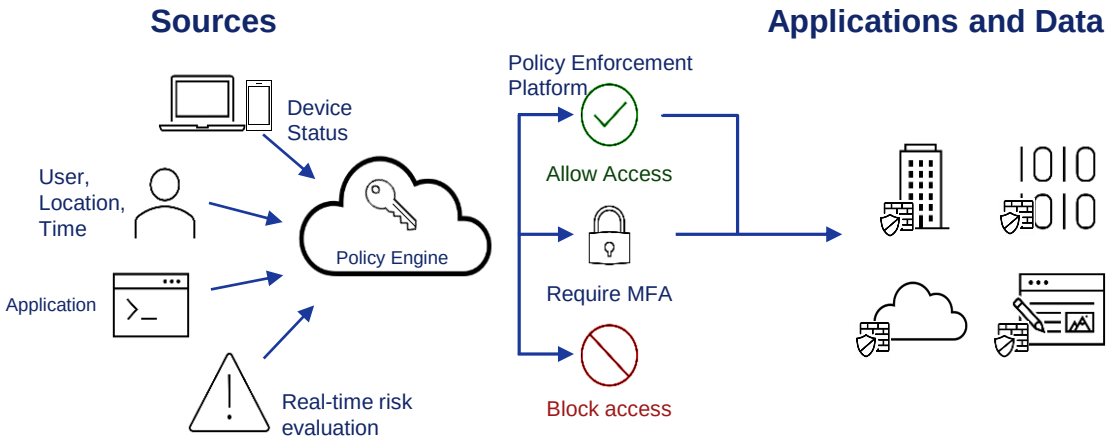
ENISA NIS Investments Report – Dec. 2020

Figure 35: Technologies and services procured to implement the NIS Directive



Security technologies also collect data that could identify an individual.

Zero Trust Architecture



Use Case: User Entity Behavior Analytics

UEBA creates an individual digital footprint to detect potentially malicious behavior by using a dataset consisting of:

- IP addresses
- Location
- Operating system and browser types and versions
- Preferred screen resolution
- Typing speed

Despite the data collected as a means of authentication and threat detection, companies can:

- Select tools that provide anonymization and pseudonymization.
- Implement strong encryption
- Enforce the four eye principle
- Use behavior analysis only for users with admin privileges

Privacy Protection in a Health Emergency: Exposure Notifications

Decentralized Approach:

- Store exchange data locally on each person's smartphone
- Back end servers have no ability to identify individuals

Centralized Approach:

- Temporary IDs to be aggregated/analyzed by a trusted partner
- Temporary IDs can be linked back to a single user
- User privacy heavily reliant app infrastructure.

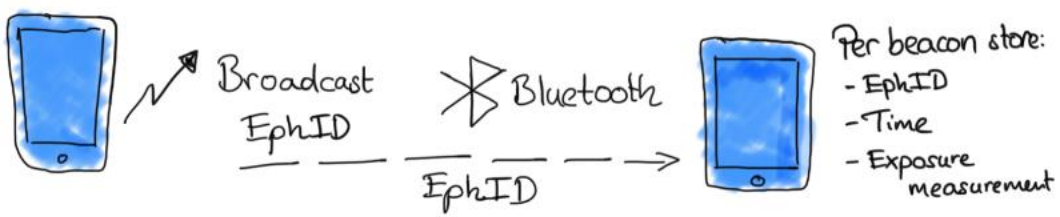
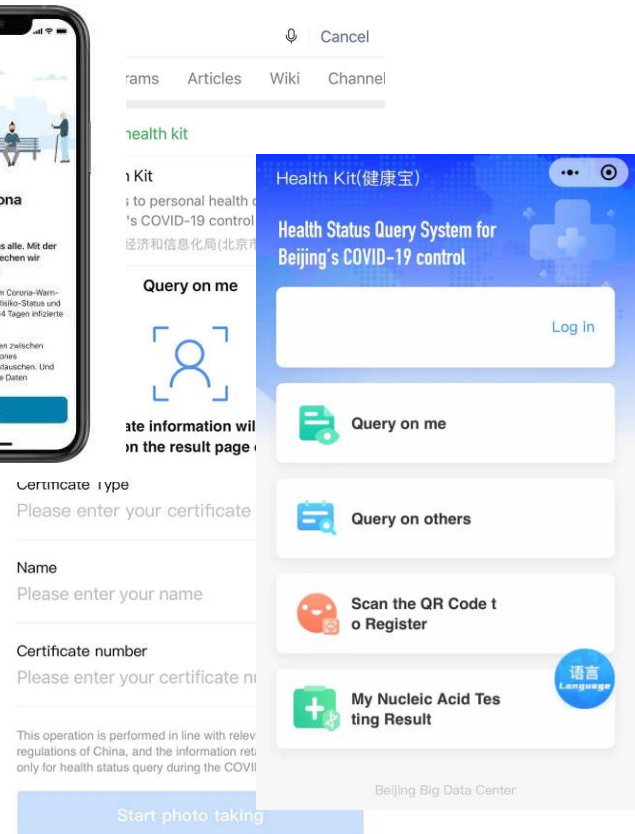


Figure AA: Processing and storing of observed beacons.

CORONA WARN-APP



Thank you!

Eve Hunter

Senior Cybersecurity Consultant
Detecon International GmbH
Digital Engineering Center

Winterfeldtstr. 21
10781 Berlin (Germany)
Phone: +49 151 27759934
Email: Eve.Hunter@detecon.com

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DETECON
CONSULTING

Cybersecurity EAST