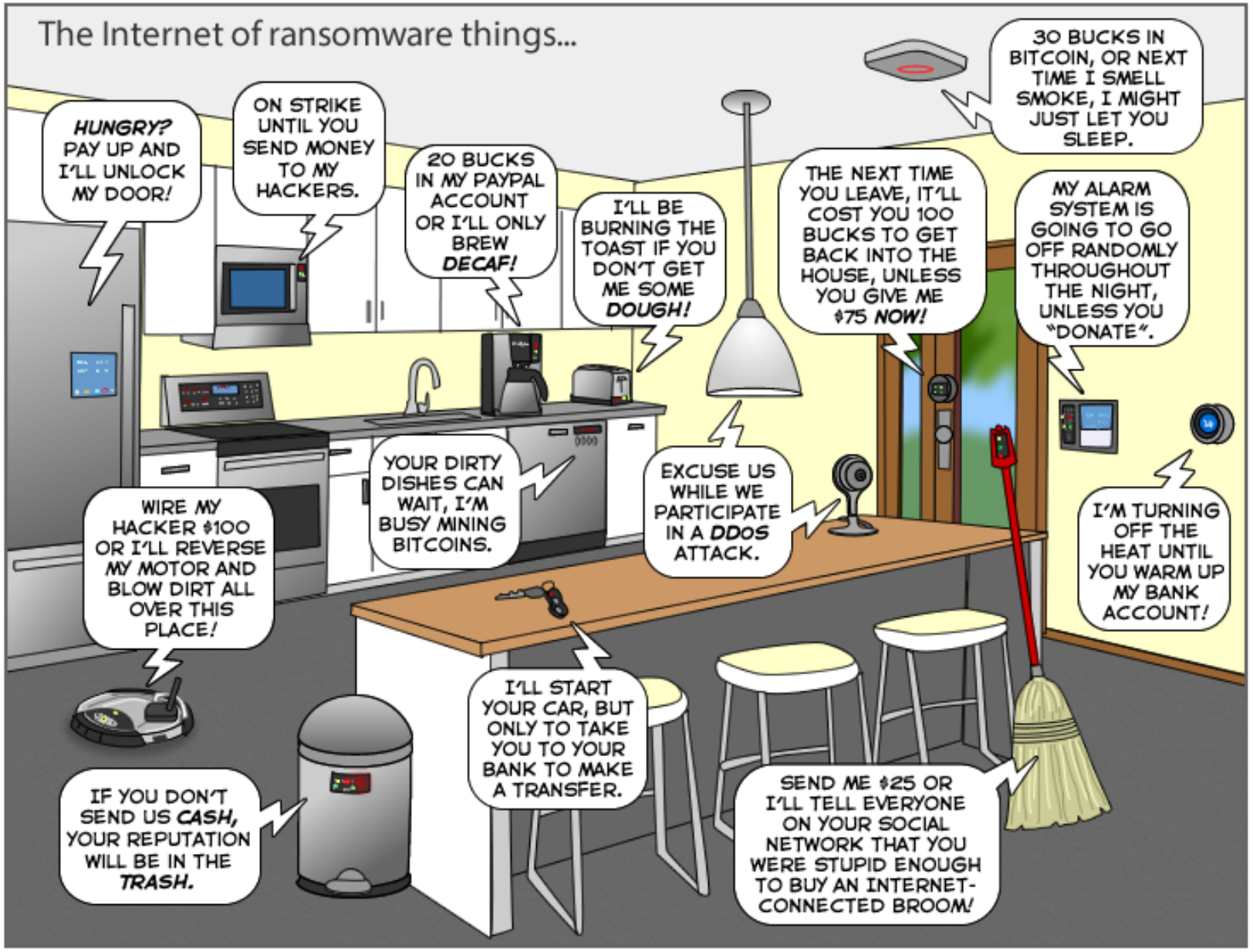
Information
Security Society
Switzerland
> vormals FGSec

~~Cyber~~ Information Security Quo Vadis?

IHK Business Outlook, 25.04.2018

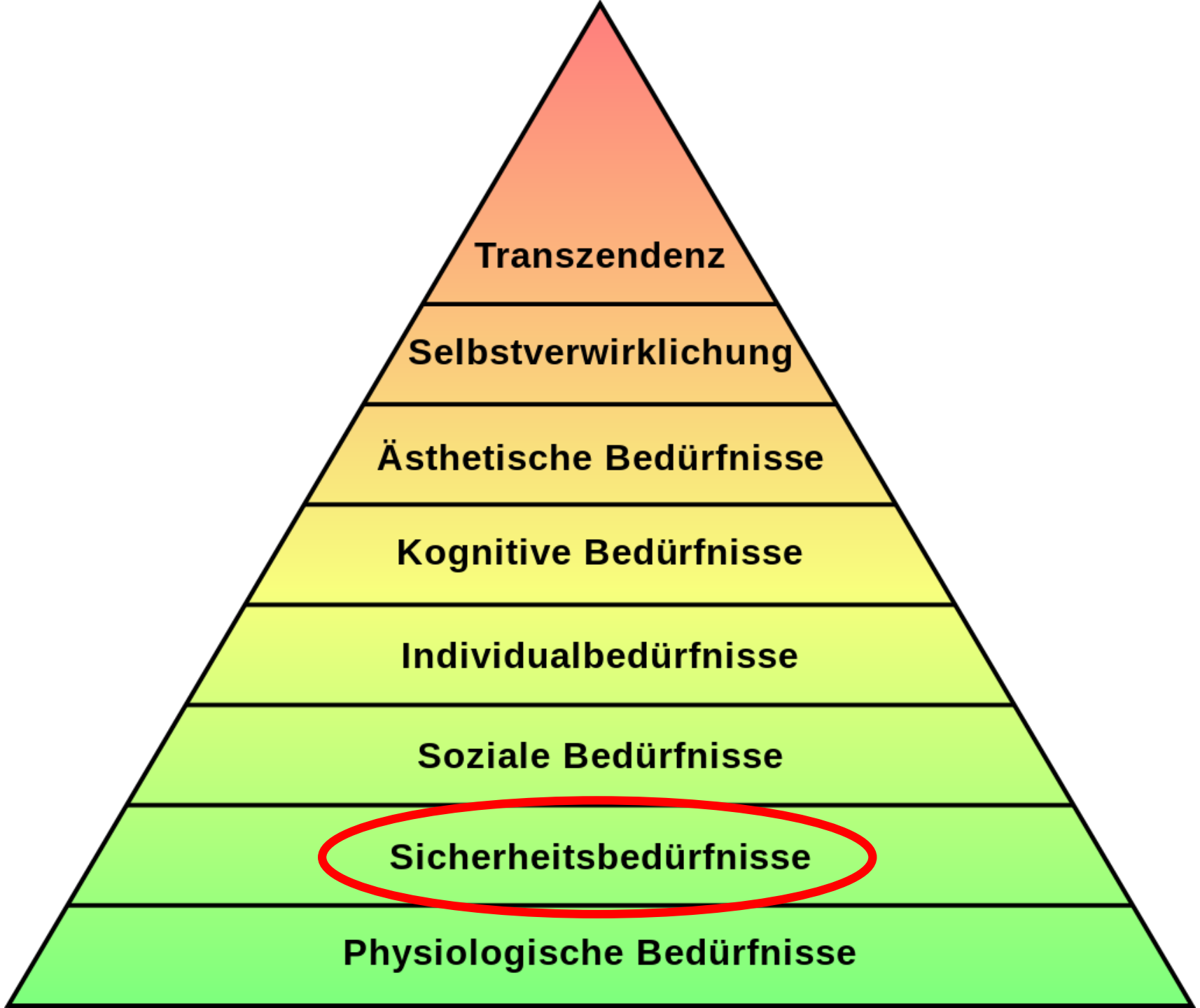
Umberto Annino, Präsident ISSS

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com



ISSS Information Security Society Switzerland

Security – Sicherheit

- Frei von unvertretbaren Risiken

ICT Security

- Sicherheit von IT-Systemen und Daten

Cyber Security

- Sicherheit von vernetzten Systemen
- (moderne, aktuelle Bezeichnung für ICT Security)

Information Security

- Sicherheit von Informationen (unabhängig von deren Bearbeitung in ICT)

People

- Umsetzung der Sicherheit, Verantwortung
- Personelle Sicherheitsmassnahmen

Process

- Business Case, Use Case → Anforderungen
- Organisatorische Sicherheitsmassnahmen

Technology

- Umsetzung der Sicherheit (in/mit Technologie)
- Technische Sicherheitsmassnahmen

Probleme und Herausforderungen

Komplexität und “time to market”

- The smarter to use, the more complex to build
- Sell now, secure later… (IoT anyone?)

History of doing nothing

- If it “works”, why bother?
- Keine statistische Basis, wenig geeignete Risk-Assessment Methoden

Geheimagent-Mentalität, falsches Vertrauen

- I am security, therefore I am invisible keine “sharing-mentality”
- Nein as a service → disable, not enable

Problem der Haftung

- Software (Produkt)-Haftung, eines der grossen ungelösten Probleme der ~~IT~~ Menschheit
- Compliance-Kultur
  compliance: yes please, real security: don’t care

Secure Software

- Resultat aus Komplexität, History of doing nothing, Problem der Haftung
- Kostet (viel), kein unmittelbarer Nutzen

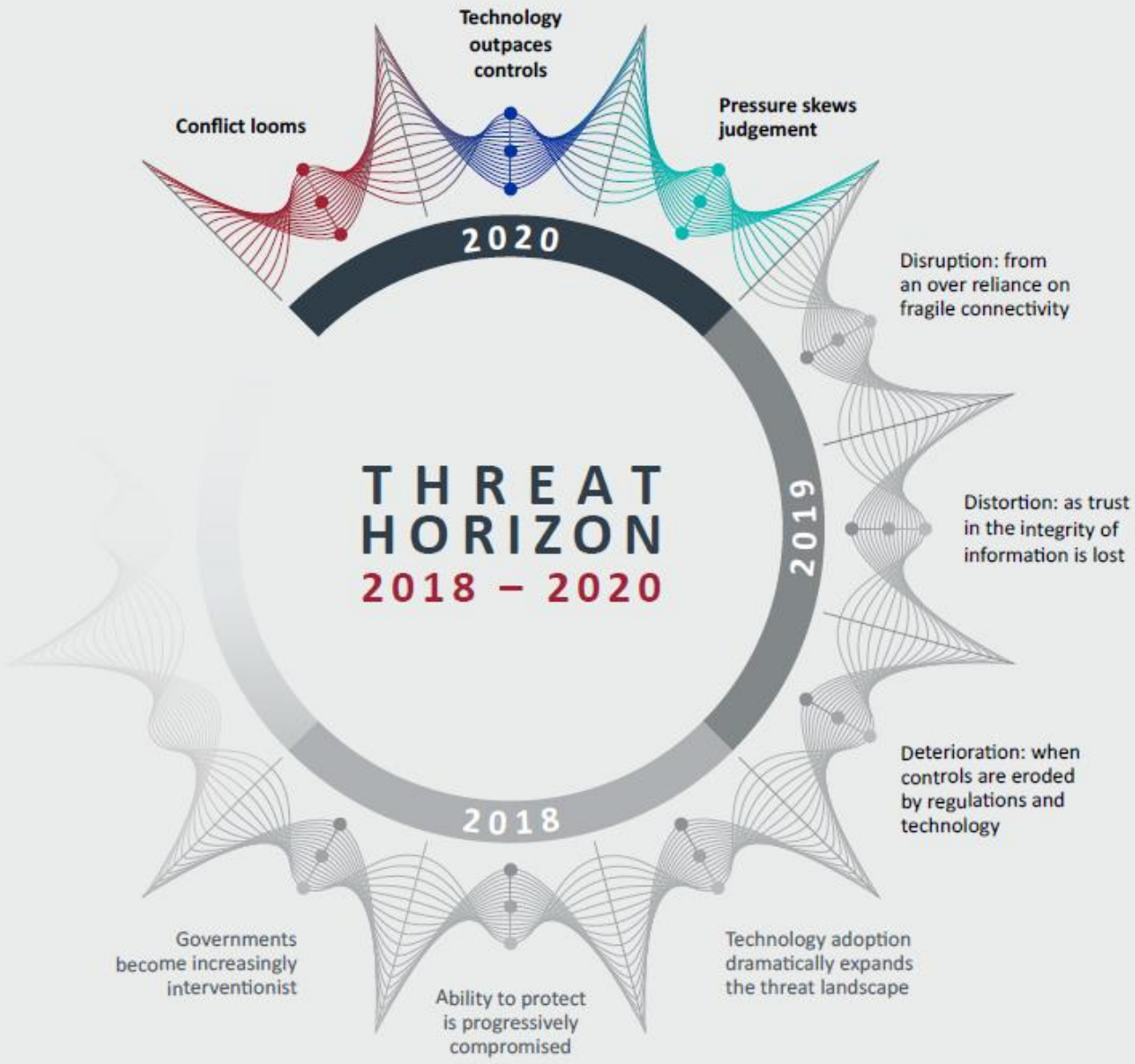
Ubiquity of Smart Technology

- Everything is smart, everything is cyber

© ISF – Information Security Forum

THREAT HORIZON 2020

FOUNDATIONS START TO SHAKE



Information Security Society Switzerland

© ISF – Information Security Forum

2018

1.1 The IoT leaks sensitive information
1.2 Opaque algorithms compromise integrity
1.3 Rogue governments use terrorist groups to launch cyber attacks

2.1 Unmet board expectations exposed by a major incident
2.2 Researchers silenced to hide security vulnerabilities
2.3 Cyber insurance safety net is pulled away

3.1 Disruptive companies provoke governments
3.2 Regulations fragment the cloud
3.3 Criminal capabilities expand gaps in international policing

2019

1.1 Premeditated internet outages bring trade to its knees
1.2 Ransomware hijacks the Internet of Things
1.3 Privileged insiders coerced into giving up the crown jewels

2.1 Automated misinformation gains instant credibility
2.2 Falsified information compromises performance
2.3 Subverted blockchains shatter trust

3.1 Surveillance laws expose corporate secrets
3.2 Privacy regulations impede the monitoring of insider threats
3.3 A headlong rush to deploy AI leads to unexpected outcomes

2020

1.1 Cyber and physical attacks combine to shatter business resilience
1.2 Satellites cause chaos on the ground
1.3 Weaponised appliances leave organisations powerless

2.1 Quantum arms race undermines the digital economy
2.2 Artificially intelligent malware amplifies attackers' capabilities
2.3 Attacks on connected vehicles put the brakes on operations

3.1 Biometrics offer a false sense of security
3.2 New regulations increase the risk and compliance burden
3.3 Trusted professionals divulge organisational weak points

Security ist ein Zyklus, kein Zustand

Mission & Objectives

- Warum Sicherheit, welche, wer und wie Sicherheit

PLAN

- *Inventar* → Schutzobjekte (Informationen)
- Sicherheitsanforderungen definieren (sec req)
- *Risiken identifizieren* und bewerten
- Sicherheitskonzept → Risiken verwalten

DO

- Gap Analysis / IST vs SOLL
- *Umsetzung planen und durchführen*

Compliance & Closing the Loop

- Validate, verify, comply

CHECK

- *Technical Audit* (security audit)
- Security Prozess-Maturität Assessment
- Compliance ggü.
  regulatory, legal, contractual requirements

ACT

- Re-act (reality!) → assume compromise, Notfallplan, Notifikations-Prozess
- Security Prozess optimieren

ISSS / SECO KMU – 10-Punkte-Programm

- Pflichtenheft für IT-Verantwortlichen
  AKV für Sicherheitsverantwortlichen
- Backups
  auch von Cloud-Daten!
- Anti-Malware aktuell und ohne Ausnahmen
- Firewall am Internet
- Software regelmässig aktualisieren
- Starke Passwörter, 2-Faktor auth
  keine Passwort-Mehrfachverwendung!
- Mobile Geräte schützen
- IT-Benutzer Richtlinien
- IT-Umgebung schützen
- Ordnung in Daten und Dokumenten

https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/infrastruktur-und-it/it-sicherheit.html

ISSS / SECO KMU – erweitert

- Vorgaben (gesetzliche, vertragliche) erfüllen
- Zugriffsschutz auf Daten regeln
- Datenträger und Daten verschlüsseln
- Auch nicht-elektronische Daten sind vertraulich
- Mitarbeitende sensibilisieren
- Unterbruchfreie Stromversorgung
- Systeme überprüfen
- Redundanz wichtiger Elemente
- Notfallvorsorge planen
- Know-how verteilen

https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/infrastruktur-und-it/it-sicherheit.html

Kontakt

Umberto Annino president@isss.ch