The 116 Best Cybersecurity Tools & Tactics (2021)

By Benjamin Eidam

Proudly presented by the
Global Cyber Security Forum

If you want the best cybersecurity tools and tactics all in one place, you will love this guide.

Below are the best 116 tools and tactics to keep your business digitally secure.

Let's get started:

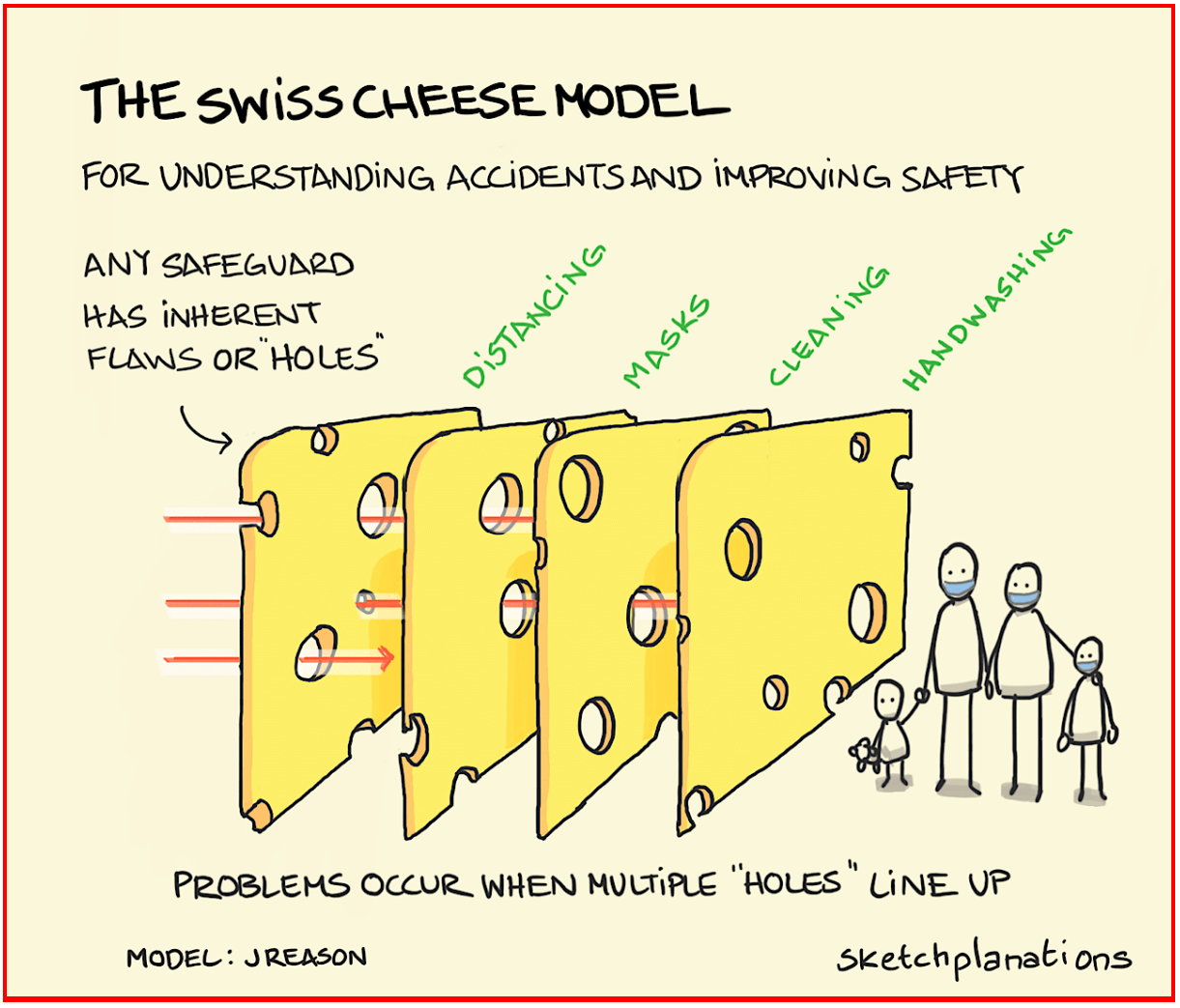
1. **Software**
2. **Hardware**
3. **Employees**
4. **Management**
5. **Company**
6. **Corporate culture**
7. **Suppliers**
8. **Environment**
9. **Artificial intelligence**
10. **Habits**

What is cybersecurity?

For most people, cybersecurity sounds quite abstract. Just as “security measures” can mean anything and everything in the “real” world.

Roughly speaking, cybersecurity consists of three interlinked and coordinated areas; Human, Hardware and Software.

Cybersecurity is more than the sum of its parts. You can imagine cybersecurity as the "digital immune system" like a sliced onion or a stack of Swiss cheese slices:



Source and more: https://sketchplanations.com/the-swiss-cheese-model

This e-book is about these layers, the components of cybersecurity. And about the most practical and immediately applicable components of it. Because cybersecurity is such an incredibly complex field that no side in the world can completely map it.

That is why I am showing 116 facets and immediately tangible possibilities that the big term cybersecurity for every section will fill with life.

Why is cybersecurity important?

The greatest digital Threads are:

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	---	---
2	Web-based Attacks	---	↗
3	Phishing	↗	↗
4	Web application attacks	---	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	---	---
9	Insider threat	↗	---
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	---	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Source: https://www.enisa.europa.eu/publications/year-in-review

Every company is attacked, no matter what size or sector, and this table is as impressive as it is meticulous.

According to ENISA, the most common attack strategies are:

The most common attack strategies:

- Attacks on the human element
- Web and browser-based attack vectors
- Internet Exposed objects
- Exploitation of weak points / misconfigurations and errors in cryptography / networks / security protocols
- Attacks via supply chain attacks
- Network spread / lateral movement
- Active network
- Abuse / escalation of privileges or userinformation
- Fileless or memory-based attacks
- Misinformation / disinformation

Source: https://www.enisa.europa.eu / topics / threat-risk-management / threats-and-trends

Tips for optimal implementation

In order to get the most out of the tools and tactics mentioned here, it makes sense to:

1. Double check and deal with the tool / tactic to evaluate which and which Shape works best.
2. Consultation / questions to the relevant responsible. It's not about competencies or paternalism, it's about optimal security. If he can say out of hand how this has already been implemented, great. If not, this can be a good starting point for further security.
3. Each of these notes has been created to the best of our knowledge and belief, however, successes in the individual application must be individually weighed and, if necessary, supervised.

I wish you success!