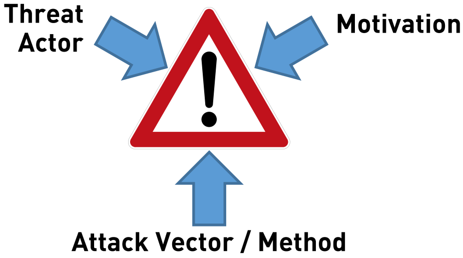
CORPORATE TRUST
business risk & crisis management

Threat Actors

Your Way to Threat-Driven Security (I)

It could hardly be clearer: The world of Cyber Security has fundamentally changed. But how exactly? Are the vulnerabilities worse than before? Has software become less secure? The fact is: Even 30 years ago, technology offered enough possibilities for attackers. Nevertheless, the digital threat situation today is different than in the past. But what makes it different?



A threat consists of three components: Threat actor, motivation and attack vector/method. Only if all three elements are present, a threat can genuinely occur. If one of the three elements is missing, an attack is at best hypothetically conceivable. Taking this model into account, the difference in today's security situation quickly becomes clear: We now face completely new threat actors with different motivations.

Your Way to Threat-Driven Security (II)

In this deck of cards you find a selection of typical threat actors from the perspective of Corporate Trust. The typical motivations are also depicted, together with some criteria of how the threat actors can be classified. But why should you concern yourself with this?

Those who protect everything, protect nothing.

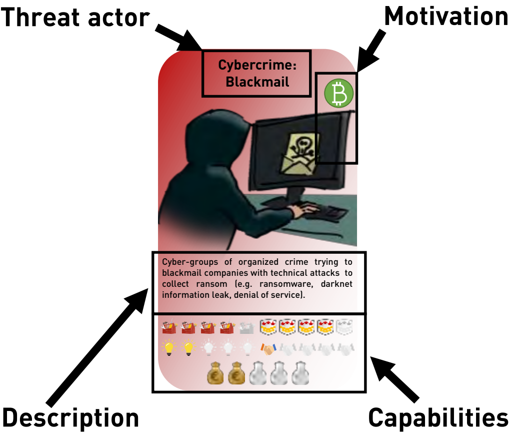
Years ago, the conviction was established that it is not an ideal use of resources to secure everything equally. Instead, the motto should be to protect some things less, but others more. The goal:

Cyber security tailored to your needs

In times of industry 4.0 and internet of things an inward-looking analysis of security requirements driven by one's own values is no longer sufficient as a basis. All security effort must begin with a systematic analysis of the threat situation. So the credo is: asset-driven security is yesterday's approach, threat-driven security is the future.

Your Way to Threat-Driven Security (III)

The focus on possible threat actors automatically leads to an integrated defense strategy. This not only includes preventive technical measures but also reactive elements (e.g. emergency plans) as well as organizational and personnel measures (e.g. maintaining contact with authorities, offering bug bounty programs, monitoring relevant forums). Simply flip through the card game.



Threat actor

Motivation

Cybercrime: Blackmail

Cyber-groups of organized crime trying to blackmail companies with technical attacks to collect ransom (e.g. ransomware, darknet information leak, denial of service).

Description

Capabilities

Instructions for Use
Part I: Prioritization

1. Place the colored cards in a row on a large table. Remove the blank cards and the unintentional threat actors (gray cards) for now.
2. Optional: Pre-sort the cards by their general threat level. Background is available at tools.corporate-trust.de/store.
3. Get your management and the key players from your business, production, digital product development and IT to the table for 1-3 hours. Together they should now sort the cards: On the left are the threat actors against whom you are willing to spend the most money on defense. On the right are the threat actors for whom lower investments in defense are justified or for whom one already feels well prepared.
4. If a threat actor is irrelevant from the participants' perspective, the card is removed. If a new threat actor or a new variation should be needed, use one of the blank cards.
5. During the ensuing discussion, the possible damage that could result from a successful attack must be taken into account. Furthermore, the participants may already be debating existing measures and their effectiveness. Assign an uninvolved person to keep the minutes of the meeting.

Instructions for Use
Part II: Plan your Defense

6. You now have a prioritized list of threat actors (take a photo for the record) and minutes of the discussion.
7. Gather the persons who are responsible for corporate security. For preparation, they are given the prioritized list of threat actors and the minutes.
8. Go through the threat actor cards with them, starting with the actor on the far left for whom the most investments in defense are necessary. Identify additional security measures, using the explanations on the individual motivation and skill levels on the cards.
9. After the meeting, create a prioritized plan of measures in relation to the discussed threat actors. Calculate the costs for each action and present the plan to the management. Begin with the implementation of approved measures.
10. At the same time, investigate existing measures, starting with those that have the highest running costs. Check each measure in context with the discussion and the prioritized list of threat actors. Evaluate whether it still contributes an added value to the company’s security.
11. Archive your results and repeat the process next year.

Motivation I: Glory & Money

On the upper right of each threat actor card is a symbol for the actor's motivation. This should play an essential role in planning the defense and incident response.

This threat actor wants to attract the attention of a community or the general public. His goal is to increase his personal reputation. „Bug bounty" programs and smart communication with potential threat actors can help prevent them. In a real incident, proactive communication plays a key role to limit the damage.

This threat actor wants money, usually in Bitcoins. Often short-term hit–and-run actions are executed to achieve a payment within a few weeks. The attacks are mostly random, i.e. the perpetrator chooses the easiest victim. A typical strategy is to install sufficient security defenses to avoid being an easy victim. Regardless of whether a company is willing to pay the ransom, professional communication with the perpetrator is recommendable.

Motivation II:
IP & Human Failure

The threat actor is pursuing the victim's intellectual property (IP), usually in planned long-term actions that are well concealed. The damage is often noticed much later. To limit the damage, it is helpful to closely involve the relevant business departments, and of course IT Forensics. For defense purposes, it is most important identify the information that an attacker may be targeting. This data must then be specially protected. Most often the base motivation of this threat actor is money, but with for the attack at hand the motivation is stealing IP.

An actor has unintentionally become an accomplice or accidentally facilitated an attack. In an actual incident, it is necessary to calm this person's distraught conscience. For defense purposes, trainings and awareness-raising are vital.

Motivation III: Business Disruption

The threat actor's goal is to sabotage machines, services and products. The most important defense is to have a well-prepared emergency plan, experienced crisis management and technical business continuity management. Attacks on companies that operate a critical infrastructure (CRITIS) are particularly dangerous.

The actor wants to eliminate a grievance. Often the victims are attacked as proxies in a larger conflict. Depending on the demand, professional communication with the perpetrator and his identification are important. Early detection is possible, e.g. through a whistleblower hotline or similar services.

The threat actor is looking for revenge or wants to harm his victim. The response is difficult; the actor's identification and the psychology of communicating with him are important. The most successful defense against this type of actor is to prevent feelings of ill will against the company. Potential perpetrators can usually be identified early through suitable "red flags".

Technical Expertise

The threat actor’s degree of general technical expertise

Threat actors with little expertise can be easily defended with technical measures. For actors with high technical expertise, log monitoring and security operating as well as trained and tested emergency procedures are important.

Examples:

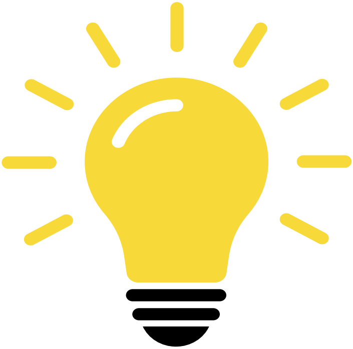
●○○○○: Amateurs with average expertise.

●●●○○: Skilled people with knowledge of the technology in general.

●●●●●: Experts who know the protocols, hardware and structures of the technologies as well as concepts, algorithms and principles of standard security technologies.

Insider Knowledge

The threat actor‘s special knowledge of his victim or his processes, systems and products.



Threat actors with little inside knowledge rarely adapt attacks to their victims and can therefore be repelled more easily with standard means. To defend against threat actors with a high level of inside knowledge, it is vital to have regular checks and to control instances of high-privilege access.

Examples:

💡○○○○: Threat actors have no special knowledge except for general information.

💡💡💡○◐: Has access to semi-public information (e.g. through personal contacts).

💡💡💡💡💡: Possesses sensitive information, such as passwords or internal documents.

Field Experience

The ability to reuse tried and tested attack methods and to evade defenses.

Threat actors with little operational experience are unpredictable. Attackers with a high level of operational experience, by contrast, are more difficult to identify and can only be repelled with great technical effort.

Examples:

●○○○○: First time threat actors without any field experience.

●●●○○: A repeat offender with experience from previous attacks.

●●●●●: Trained perpetrators with repeat experience in methods, infrastructure and systematic approach.

Position of Trust

A threat actor’s ability to utilize the help of an employee inside the company.

Threat actors who enjoy a low level of trust (e.g. outside parties) can be repelled with technical and procedural measures. Red flag detection and emergency plans are more important for actors with a high level of trust (e.g. internal employees).

Examples:

🤝○○○○: Social engineers who can only gain trust through electronic means.

🤝🤝🤝○○: Spies who are able to smuggle in threat actors or recruit them personally.

🤝🤝🤝🤝🤝: Insiders who already have the trust of one or more employees.

Financial Resources

The possibility of financing attacks and compensating deficits through purchases

Threat actors with high financial resources can compensate for some of their deficits by purchasing assistance, e.g. by hiring specialists. However, not every threat actor exhausts their full financial possibilities for each victim. Examples:

- 💰○○○○: Threat actors who finance themselves through private resources (in the tens of thousands of Euros).
- 💰💰💰○○: Threat actors who can raise considerable funds (with corresponding profit prospects up to high six-figures).
- 💰💰💰💰💰: Threat actors with access to large budgets or substantial funds from previous operations.

Groups of Threat Actors

The card background assigns the threat actor to a group. Groups are not necessarily selective and lines between them are blurred.

- 🟥 Organized crime, small groups of criminals and lone actors
- 🟪 Governmental or state-aided actors in „Cyberwar“
- 🟪 Traditional secret services and espionage organizations
- 🟨 Ideological perpetrators
- 🟧 Attention-seekers
- 🟧 Customers, investors and fans who intentionally act to harm the company
- 🟩 Typical insider: employees and former employees
- 🟦 Competitors, rivals, fellow industry contacts
- ⬜ Accomplices: unintentional, accidental or manipulated

Organized Crime

₿

Organized crime that uses IT and cyber attacks to prepare or facilitate traditional attacks (kidnapping, burglary, smuggling, theft, money-laundering).

🧰🧰○○○ 🛡🛡🛡🛡○

💡💡○○○ 🤝○○○○

💰💰💰○○

Cybercrime: Fraud

Single hacker or organized crime that tries to manipulate processes and people in order to misappropriate assets (e.g. Business E-mail Compromise such as Fake President, Payment / Goods Diversion).

●●○○○ ●●●●○

●●●○○ ●○○○○

●●●○○

Cybercrime: Blackmail

Single hacker or organized crime trying to blackmail companies with technical attacks to collect ransom (e.g. ransomware, darknet information leak, denial of service).

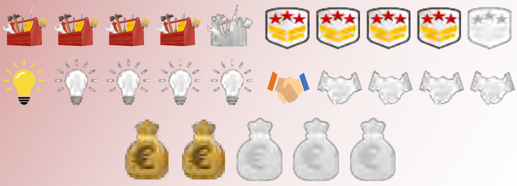
🧰🧰🧰🧰○ 🛡️🛡️🛡️🛡️○

💡💡○○○ 🤝○○○○

💰💰◐○○

Cybercrime: Malware Operations

Single hacker or organized crime trying to make money indirectly by installing malicious software (hiring themselves out as a botnet, selling passwords/address data, identity theft)



White-Hat Hacker

📢
₿

Security researchers and IT experts who are looking for vulnerabilities in systems, either to sell them to the highest bidder or to make a name for themselves at conferences or through publications.

🧰🧰🧰🧰🧰 🛡🛡🛡🛡○

💡💡○○○ 🤝🤝○○○

💰💰○○○

Script Kiddies, Leisure Hackers

📣 ✊

Future IT security experts, leisure hackers, kids, and students who carry out cyber attacks to attract attention and test their skills.

🧰 🧰 🧰 ○ ○ 🛡 ○ ○ ○ ○

💡 💡 ○ ○ ○ 🤝 ○ ○ ○ ○

💰 ○ ○ ○ ○

Journalists, Media

Journalists who are trying to make headlines with breaches, (cyber-)attacks, potential vulnerabilities or other scandals in order to generate maximum publicity.

Shady Politician

Domestic or foreign politician or governmental offical using their position of power in a arbitrary or criminal fashion as a career booster or to gain financial advantages.

●○○○○ ●●○○○

●●●○○ ●●●○○

●○○○○

Cyber-Mercenary

Hired hacker groups paid by the private sector to extract information from companies, modify data or sabotage services.

Military Cyber-Units

Units of regular armies specializing in cyber-warfare carrying out training or real attacks to achieve operational goals set by their governments.

🧰🧰🧰🧰🧰 🛡️🛡️🛡️🛡️🛡️

💡💡○○○ 🤝🤝○○○

💰💰💰💰💰

State-Sponsored Actors

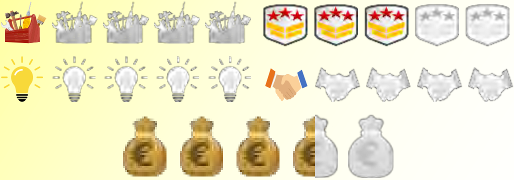
State-funded hacker groups commissioned by governments or armies to obtain information, alter data or sabotage services.

Technical Secret Services

Technically oriented departments of secret services (e.g. NSA, FAPSI, GCHQ), which use modern technical espionage (SIGINT, MASINT) to reach governmental objectives.

Religious or Political Actor

Fanatics and extremists motivated by religion, left or right-wing extremism or other ideologies.



Cyber-Terrorists

Cyber-departments of traditional terrorist organizations who act to spread fear and uncertainty.

🧰 🧰 🧰 ○ ○ 🛡 🛡 🛡 ○ ○

💡 ○ ○ ○ ○ 🤝 ○ ○ ○ ○

💰 💰 💰 💰 ○

Whistleblower

Employees who leak company secrets because they believe certain situations, processes or procedures are so wrong that the general public needs to be informed.

Non-Profit Organizations

Not-profit and non-governmental organizations carrying out high-profile attacks in cyberspace in order to draw attention to grievances or stop unpopular actions.

Hacktivists

Groups like "Anonymous" that use IT attacks to achieve political goals or demonstrate civil disobedience in cyberspace.

●●●●○ ●○○○○

●○○○○ ●○○○○

●●○○○

Employees in Trouble

₿ 🧠 ⚠

Employees (e.g. from IT, finance or research departments) in financial or other difficulties who commit crimes against the company on their own initiative or instigated by third parties.

🧰 🧰 🧰 🧰 ○ 🛡 ○ ○ ○ ○

💡 💡 💡 💡 💡 🤝 🤝 🤝 🤝 🤝

💰 ○ ○ ○ ○

Frustrated Employees

Employees (e.g. from IT, finance or research departments) who want to harm the company out of frustration by undermining strategies, publishing information or maliciously changing data / systems.

🧰🧰🧰🧰 🛡

💡💡💡💡💡 🤝🤝🤝🤝🤝

💰

Vengeful Ex-Employees

Employees (e.g. from IT, finance or research departments) who have left the company in disgrace, feel they have been treated unfairly, want to receive compensation, or intend to harm the company out of revenge.

●●●●○ ●○○○○

●●●●● ●●●○○

●○○○○

Competing Ex-Employees

Ex-employees who systematically collect information during their time in the company in order to set up a competitor business after leaving.

🧰🧰🧰○○ 🛡○○○○

💡💡💡💡💡 🤝🤝🤝○○

💰💰○○○

Resentful Family Members

Family members of managers or company owners who are dissatisfied with their own situation. Blackmailing, discrediting and illegal acquisition of compromising materials are not unusual.

●●○○○ ●●○○○

●●●●○ ●●●●○

●●●●○

Detective Agencies

Private investigators working with social engineering, open-source intelligence and, if necessary, with simple technical means.

They are either commissioned or collect and sell information proactively.

●●○○○ ●●●○○

●●●○○ ●●●○○

●●○○○

Competitors

Competitors who do not shy away from robust methods of information gathering in context with “Competitive Intelligence”.

●●○○○ ●●●○○

●●●○○ ●●○○○

●●●○○

Industrial Spy

Hired industry experts who get paid to extract specific information from companies.

●●●○○ ●●●●○

●●●○○ ●●●○○

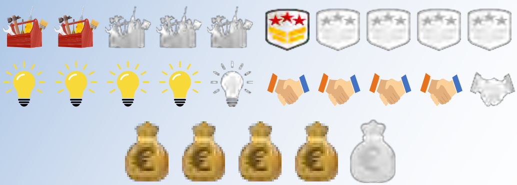
●●●○○

Overambitiuous Service Provider

Employees of service providers who use secret proprietary information of the company to impress competitors.

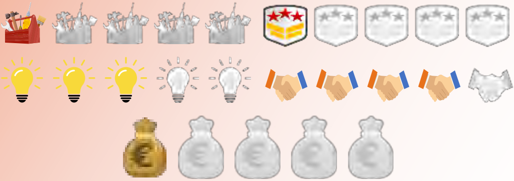
Fraudulent Partner

Partners in sales, technologies or other projects, foreign branch offices or joint-ventures who steal intellectual property and exploit it to their own benefit.



Dishonest Customers

Customers who want to obtain additional options, features, services or more usage time for less money.



Product Pirates

Small companies who use stolen information or ideas to pirate products or spare parts to benefit from the company's intellectual property.

🧰🧰○○○ 🛡○○○○

💡💡💡💡○ 🤝🤝🤝○○

💰💰💰○○

Modding Community

Hobbyists, DIY'ers, tuners or "modders" who change the properties of products or services in a way unintended by the manufacturer. They offer their expertise on the internet, for free or for sale.

🧰🧰🧰🧰○ 🛡🛡🛡○○

💡💡💡💡○ 🤝🤝🤝○○

💰💰○○○

Corporate Raiders & Insider Traders

Broker and trader seeking insider information about future plans or trying to generate negative company news to manipulate the stock market or to influence M&A activities.

🧰 🧰 ○ ○ ○ 🛡 🛡 🛡 🛡 ○

💡 💡 💡 ○ ○ 🤝 🤝 🤝 ○ ○

💰 💰 💰 💰 ○

Infiltrated Employees

Non-professionals (students, interns, PhD candidates) or "perfect" applicants, who aim to be hired to extract as much proprietary information as possible.

Manipulated Associations

Business associations, consulates, embassies, NGOs, chambers of commerce infiltrated by secret services or interest groups, which investigate organizations and processes and extract information from companies.

Infiltrated Service Provider

Contractors (e.g. factory security, cleaning services, data centers, SOC providers) that have been infiltrated by foreign governments or companies in order to gain access to secrets or circumvent security measures.

Foreign Propaganda

Troll factories, secret service departments, competitors or private organizations who spread disinformation, false reports and propaganda.

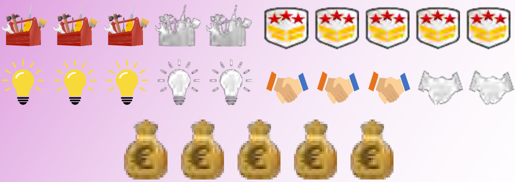
🧰 ○ ○ ○ ○ 🛡 🛡 🛡 🛡 🛡

💡 ○ ○ ○ ○ 🤝 ○ ○ ○ ○

💰 💰 💰 💰 ○

Traditional Intelligence Services

Intelligence services that use social engineering (HUMINT, SOCINT), open sources (OSINT) and, if necessary, the help of technical service providers, to achieve goals set by their governments.



Careless Employees

Employees who unintentionally harm the company because they publish information or facilitate attacks accidentally, due to stress or lack of training.

Careless Service Provider

Employees of service providers who store secret proprietary information on their own company servers, from where it is passed on or stolen.

Law Enforcement

Law enforcement authorities such as the police, public prosecutor's office, tax investigators, regulatory authorities, which are manipulated to take unjustified action against the company.

Remote Locations

Remote sites that are connected to the company network but are poorly maintained or do not have the same security level.