Almond

October 2023

INSIDER THREAT

SUMMARY

PROJECT TEAM

Chloé GRÉDOIRE

GRC Consultant /
CTI Analyst

Albane GIROLLET

GRC Consultant /
Business and Legal
Intelligence Analyst

Mathias GARCIAU

Manager
SOC / CERT / CTI
CWATCH

Mélodie CELIN

Communication &
Marketing Senior
Consultant

EXECUTIVE SUMMARY

Whether it's breaking into a bank, obtaining strategic information about an opposing military camp, getting a head start in politics, making a fortune off other people or simply snooping on your spouse... spies and snitches have been around since the dawn of time. Sometimes they work for a good cause, sometimes not - it's simply a question of point of view. In all cases, the modus operandi remains the same ; they exploit man's weak points: greed, love, spirituality, politics, family, friends... Once they've won the trust of one or more people, it's already too late.

The employee has already opened the back door of the bank, and in exchange for a few pennies, the criminals come in and take all the money. You can call the police, but they'll soon be gone, the money and confidential documents with them. That's the same for your data ?

Anyone can and has always been able to fall on the side of the bad guys. Espionage and information strategy are not the preserve of James Bond or well-organised government entities. Each level of crime has its own means. This threat can no longer be considered solely by defence teams in general, whether they are cyber specialists, infantry, bodyguards, surveillance officers, etc. Spies and informers are targeting more and more people and is raging in an eco-system that is barely half a century old and constantly changing.

In fact, in the cyber sector the insider threat cause a great deal of damage to companies, governments, associations, etc. and make the task of the IT department, operational SOCs and CERTs much more complex. We believe that technological developments in terms of weak signal studies, behavioural analysis, AI, etc. make detection possible and credible. Just like the legal system, which has already had to deal with numerous case.

The CTI CWATCH Almond team invites you to delve into the key characteristics of this protean threat and identify possible defensive measures.

Almond's CTI

Almond has its own service to deliver threat intelligence. Our ability to contextualize information helps decision-makers to make arbitrages according to the current threat landscape. The polyvalent CTI team creates high-quality strategic, tactic and operational content to help you protect your organization with actionable information treated from a French and European perspective. We are also able to respond to your spontaneous or special requests.

Our publications are regularly updated and available on a threat intelligence platform (knowledge base of threat actors' profile; sector-focused reports; geopolitical synthesis with cyber-related insights; information notes on malicious softwares, tools and vulnerabilities).

The team relies on a wide range of data collection options (telemetry of Almond CWATCH, Board of Cyber products and technological partners; incidentology feedback from our two CERTs; offensive R&D; multidisciplinary knowledge (RSSI As A Service, Risk Manager...)).

To subscribe to our services, **visit** or **contact**.

PART 01.

INTRODUCTION

In the last decades, cybercrime has evolved, changed form and gain sophistication. But one thing has not change, most of the attacks occurs with the help (conscious or not) of the victim's employee. Less common, but deadly and difficult for companies to track is the malicious insider threat. Insider threat is mostly materialised by negligent or accidental behaviour.

This threat is overlooked because of the complexity of assessing and dealing with it, and the cost it represents, with a return on investment that is difficult to estimate.

As ransomware or APT (Advanced Persistent Threat) threats are evaluated, this threat needs to be recognized, the most likely pattern identified, and a risk treatment plan defined. The porosity between the internal threat and cybercriminal groups must also be considered which is becoming increasingly prevalent and increasing the attack surface.

The concept of defence in depth, at the heart of cybersecurity, no longer applies in this context since insiders already have access authorisations. Existing solutions are often difficult to put in place and constrain the execution of operations, which can have the opposite effect.

Almond has analysed various incident response cases and aims to provide an analysis to this well-known but little studied threat. Employees' responsibilities from a legal point of view are also questioned and the way companies can prevent and protect themselves from this threat.

PART 02.

HIDING IN THE MASS

In the vast world of cybercrime and cyberespionage, there are a multitude of actors with different capabilities, objectives, resources. Between the opportunistic ransomware groups, and the sophisticated APTs, there is an even more discreet threat: Insider.

Even though some consequences are similar in all cyber threats, like financial loss, loss of sensitive data, damage to reputation, etc, that threat is characterized by its impact on an organization. **It's not a stranger who enter your house but one of you.** The challenge is to identify what constitute an insider threat, how they operate and how to detect the first signs.

This study will enable us to clarify the contours of the various insider profiles identified and to specify the nature of the activities undertaken by these individuals.

2.1 The threat is already there

According to IBM's latest report, it takes in average "204 days to detect a breach[1]", it is most likely that the insider threat is already active in your organization.

The difficulty is the same, if not even more than the other threat actors. How can you tell for which groups or insiders you constitute a target?

To that degree of uncertainty, you must add the specificities of a structure. There is always movement, and you need to consider every current, former, or future employees (they can be part of the "insider-as-a-service" system) and service provider employees that work, have work or will. Whether consciously or unconsciously, they all could in theory constitute a threat to your organization.

The larger your organization is, with multiple departments, branches, subsidiaries, or most of your services are delivered by third parties the greater the likelihood there is an insider in hiding.

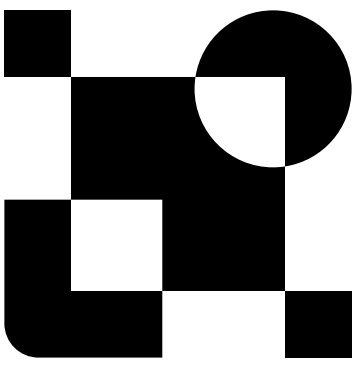
That probability can also be higher depending on the nature of your activities, your business strategy and financial situation or internal changes such as a new board, a new acquisition, a wave of layoffs or external socio-economic factors like inflation, geopolitical tensions.

It can also be completely outside the company's purview and in the personal life of the insider. The list of variables is not exhaustive and that show the complexity for an organization.

Moreover, we must acknowledge that this threat is by its very nature fluid. Unlike the external threats like ransomware groups and APTs whose aim is to disrupt their victim's information system for various purposes but with no links to the target, internal threat appears and disappears without much warning.

Insider threat is triggered by circumstances and a particular context at a given time. Most of the time, this change is difficult to predict, and weak signals do not necessarily mean that the threat will be acted upon.

One of the characteristics of an internal threat is the fact that the people involved can bypass the physical and logical security controls put in place, either for their function and daily tasks or due to their technical knowledge of the information system. In case of malicious insiders, they also can monetize those accesses to other parties. Depending on the security policies in place (BYOD (Bring Your Own Device) policy for example), those actions can prove rather easy and increase the difficulty of tracking hem.



1 IBM, 2023, "Cost of a Data Breach Report".

2.2 Who are they?

In this report, we can highlight three types of insiders:

- The malicious insider;
- The negligent insider;
- The external insider or third-party threat.

In the top tier of internal threat actors, alongside third parties, malicious and negligent insiders can be employees with traditional rights and employees with privileges and administrative rights.

Moreover, we can emphasise the difference in status that exists between the several types of insiders. Not all individuals likely to be malicious or negligent insiders have the same responsibilities or the same access to a company's information and secrets. This difference therefore has a significant impact on the scope of the threat and the sanctions associated (see section 4).

2.2.1 Malicious insider

As we already stated, there are a large set of malicious insider profiles. Existing within an organization, they have all access and knowledge on interesting projects and data to conduct effective attacks. If it is taking a long time to acknowledge an attacker in your system, detecting malicious insider is a greater challenge as he is a member of the family. Therefore, considered as adversary, organizations need to understand the different profiles.

WHO?

The malicious insider threat is made up of individuals using their knowledge of an organization's ecosystem and / or their legitimate access to carry out malicious activities themselves, on behalf of a third party or as a facilitator. Depending on the types of objectives, the profiles can range from IT employees, engineers, sales personnel, low and middle management, help-desk, secretary, etc. We can also observe groups of insiders working together.

CHARACTERISTICS?

Malicious insiders are characterized by their motivation. They act intentionally, sometimes with premeditation. According to recent data, malicious individuals are behind 20% of insider threat attacks.

Persistent malicious insiders who are generally looking for additional income and use their knowledge of their organization to carry out malicious actions leading mainly to the extraction of information.

Loners and opportunistic insiders who know very well the entity and use their privileged access in the company to cause harm, mostly its reputation.

Disgruntled employees act mainly out of revenge or resentment. They therefore look for ways to recover information and/or interrupt or even destroy the operating system. Their actions can be spotted, as this behavior generally emerges after changes in a company or in their professional and/or personal life (ex. termination, harassment, change in culture, resignation, etc.).

Insiders recruited by cybercriminals. While insiders may act on their own initiative, they can also be solicited by cybercriminals, who are playing an increasingly important role in developing the insider threat.

In 2022 the LAPSUS group published an advert to recruit insiders who could give them access to telecommunications companies (Claro, Telefonica, ATT or other), computer or video game company (Microsoft, Apple, IBM or other), call centres (Atento, Teleperformance or other) and a hosting services (OVH, Locaweb). At the time of publication of this offer, the LAPSUS Telegram channel had more than 50,000 subscribers.

WHY?

From the different types of insiders, the following motives can be identified :

- Resentment towards the employer;
- Revenge following a disagreement with the employer;
- A desire to curry favor with another organization;
- Feeling of having power over the employer;
- Greed;
- Entertainment.

HOW?

- Sabotage of the reputation and/or the information system;
- Fraud, either the alteration of company data for personal gain or information theft for an identity crime;
- Espionage;
- Theft of intellectual property, credentials, etc.;
- Disclosure of different types of access.

RESOURCES?

Malicious insiders are not equals and their capacities are reflected by their motivations.

Messaging solutions like Telegram are now used by the threat actors, in particular ransomware groups to contact and recruit insiders.

Figure 1: Malicious Insider threat ID

PROFILE	SABOTAGE	IP THEFT	FRAUD	ESPIONAGE
WHO?	Employees in IT department	Scientists, engineers, programmers, sales personnel	Lower-level employees	Any employees
	Employees with privileged access		Low and mid-level management	
WHEN?	Set up while employed	Within the last two days before departure of after leaving the company	On the long run	On the long run
	Execute after termination			
MOTIVATION?	Revenge	Starting their own business	Financial need and/or greed	Financial need and/or greed
		Found a new job position		Dissatisfaction with status, organization political view and strategy
		Approached by a foreign government and/or the organization competitor's		Ideology
HOW?	Access, ability and motivation	Data exfiltration via email, USB or physical files	Corruption of organization procedures	Depends on the profile
			Inadequate auditing of critical and irregular processes	
WHAT?	Usualy systems that they worked on	Information they worked on or had access to	Personally identifiable information	Theft of information
				Destruction of information

Figure 2: Malicious Insiders profiles inspired by the work of the CCDCOE

As stated in the previous table, to each goal can be affected an insider profile. It is interesting to note that the **when** is the most important question: because of their nature and access, to be able to bypass securities and processes in place and achieve their objectives, insiders must adapt the timing of their attacks.

While the sabotage and the IP (Intellectual Property) theft have a rather brief period of action, fraud and espionage takes on average a long time to prepare and execute depending on the information nature and the motivation.

The employees using their knowledge and privileged access usually will start by:

- Implementing unauthorized tools such as remote network administration solution, password retriever;
- Look for ways to move laterally within the network;
- Obtain elevated rights by using social engineering via their role or functions in the company for example..;
- Secure their own access even after their departure from the company;
- Install backdoors accounts, malicious software programs;
- Uninstall backup present on the network or fail to install them (as part of its function);
- etc.

Profiles have their own set of abilities depending on what they want to achieve.

Most of the time, Insiders don't even have to look for a long time. Company sometimes forget to delete or block former employees access leaving the door open for any type of action malicious or not. According to a recent study by Beyond Identity[2], approximately **25% of employees can still access their past workplaces accounts and emails.** What's even more worrying from the report is that over 41% of these employees admitted to sharing their former workplace logins."

2.2.2 Negligent insider

Most insiders have no intention of hurting their organization. However, that population represents a major risk for an organization. There are several reasons for this situation. Within the company, the following failures increase the risk of employees falling into traps:

- A low level of maturity in IT (Information Technology) and cybersecurity;
- The absence of mandatory awareness programs for employees;
- The absence of security processes;
- The lack of control over information flows;
- An overly permissive BYOD policy or uncontrolled devices on the IT infrastructure.

On the other hand, employees can also increase the risk regardless of the organization level of security. We can categorize employees in two categories:

- People for whom awareness programmes do not work, due to lack of interest or **non-responders**. Commonly called "Serial Clickers" these employees represent a substantial risk, particularly because of the predictability of their behaviour easily picked on by threat actors. Particularly, if they are in strategic positions (e.g., VIP) or with privileged access either to sensitive information (e.g., secretary) or to the IT system;
- People who are said to be **negligent** because they understand the security basics implemented in their organization and the associated policies, but for reasons of practicality will sometimes bypass them.

As they do not identify their behaviour has dangerous for the company, they become themselves easy targets for campaigns such as phishing, swindles, or compromise of their devices. For example, use of personal devices to store company information or the

2 Taylor, Stephen. 2022. LinkedIn. 1 in 4 Ex-Employees Still Has Access to Company Data.

consultation of private webmail on company devices is notorious but do not appear as dangerous as deactivating the anti-virus. The challenge for the company is to **close the gap between security and practicality** because employees will always choose practicality in their day-to-day work.

The careless insider can also be tricked by social engineering manoeuvres devised by attackers.

Nevertheless, we can distinguish accidental threat and negligence.

NEGLIGENCE

- "Exposes an organization to a threat through carelessness";
- Example: constantly ignoring security alerts to update a system or sharing credentials with a colleague.

ACCIDENTAL

- Mistakenly causes an unintended risk to an organization;
- Example: mistyping an email adress and sending sensitive information to a competitor or opening a phishing email.

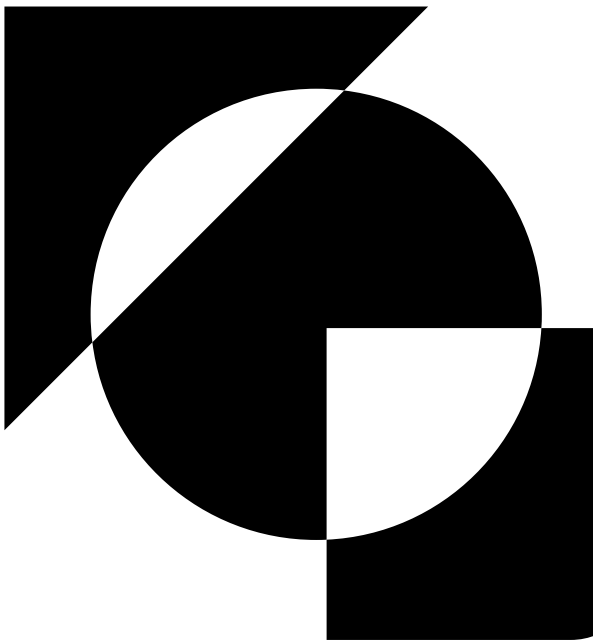
Figure 3: Negligence and accidental

The consequences of those insiders will primarily be on data defined here[3]:

- "A data breach is when sensitive data is accessed and compromised in a successful attack";
- "A data leak is the exposure of sensitive data that could be used to make a future data breach happen faster";
- Accidental data exposure[4] is a type of data breach that happen because of inadequate security measures and/or human error. It can also be due to the negligence of an employee.

For the most part, inadvertent data leaks and exposure mean that users unintentionally violate the protection policies in place, without any malicious motivation. For example, an employee who wants to finish an urgent work and transfer a confidential document containing personal or sensitive information on its personal cloud service, or on its private email.

Similarly, accounts and equipments are compromised without the user's knowledge. Negligence, on the other hand, refers to data leaks where the user has no malicious intent but is deliberately circumventing the policies in place within the company.



3 Tunggal, Abi Tyas. 2023. Upguard. "What is a Data Leak? Stop Giving Cybercriminals Free Access".
4 Gasparian, Levon. 2022. "How To Prevent Accidental Data Exposure Within Your Company".

WHO?

Accidental or negligent insider threats are individuals who, because of their knowledge of their organization and their access to confidential information, services and resources, are likely to facilitate the compromise of their organization in a non-voluntary manner. Even if the initial action is not malicious, the consequences will be the same. These individuals act either on their own or on behalf of third parties, either consciously or unconsciously.

CHARACTERISTICS?

According to recent data, negligence represents 56% of security incidents on a pool study of more than 6,800 incidents reported.

There are two categories :

- People unresponsive to awareness programs are a major risk to companies. Mostly because they are perfect targets for phishing campaigns or to act carelessly with sensitive information, without the intention of harming but rather because of a lack of interest in safety protocols and IT security standards.
- People who are said to be negligent, because they understand the security basics implemented in their organization and the associated policies, but for reasons of practicality will sometimes bypass them.

WHY?

- The overuse of emails in organization;
- Lack of IT skills;
- Poor awareness training.

HOW?

- Use of personal devices compromised for work;
- Victims of Phishing / Spearphishing;
- Vishing;
- Introducing malicious USB devices on the network;
- CEO Fraud;
- Errors in the manipulation of information;
- Loss of mobile equipment;
- Accidental data leak;
- Use of malicious code to carry out an attack (social engineering);
- Accidental or inefficient disposal of physical media.

In August 2022, Microsoft employees exposed sensitive login credentials on GitHub. Those access were possibly related to Azure servers access and internal Microsoft systems. The company immediately took action but it could've have constituted a GDPR breach if personal data had been accessed.

That type of leak are an open door for attackers seeking entry to businesses in their phase of initial access.

RESOURCES?

The impacts of unintentional insiders goes beyond data loss

- Loss of Intellectual property;
- Economic loss;
- Facilitated cyberattacks as point of entry;
- Production Shutdown;
- Data leak or Accidental data exposure;
- Legal and regulatory impact;
- Etc.

Figure 4: Negligent Insider threat ID

2.2.3 External insiders

From your IT provider to the reception office, a company's ecosystem is intricate and it's not rare that a provider is allowed to enter an office without prior knowledge or to move inside a customer office without any supervision. That's the problem, external insiders have a dual status. While there are not technically outsiders because of the mandate they have within an organization and trust, they are neither insiders. External insiders are not subject to internal controls for the most part, and service provider contract faill to have sufficient security requirements.

A stranger or a recurrent partner, the external insider can easily play with his special status. He can take advantage of the level of trust and/or anonymity that enables him to move around the company in his own way. Some external insiders have daily access to the targeted company while others can penetrate the infrastructure exceptionally. The daily access can give him a deep knowledge of the company's structure while an occasional visit makes him discreet figure.

To employees, external insiders are not seen as a threat because at some point their presence is or was legitimate, they can be in sensitive places within the office, without being questioned. Their knowledge on their clients, the granted access to sensitive information, services and resources makes them a major risk to businesses.

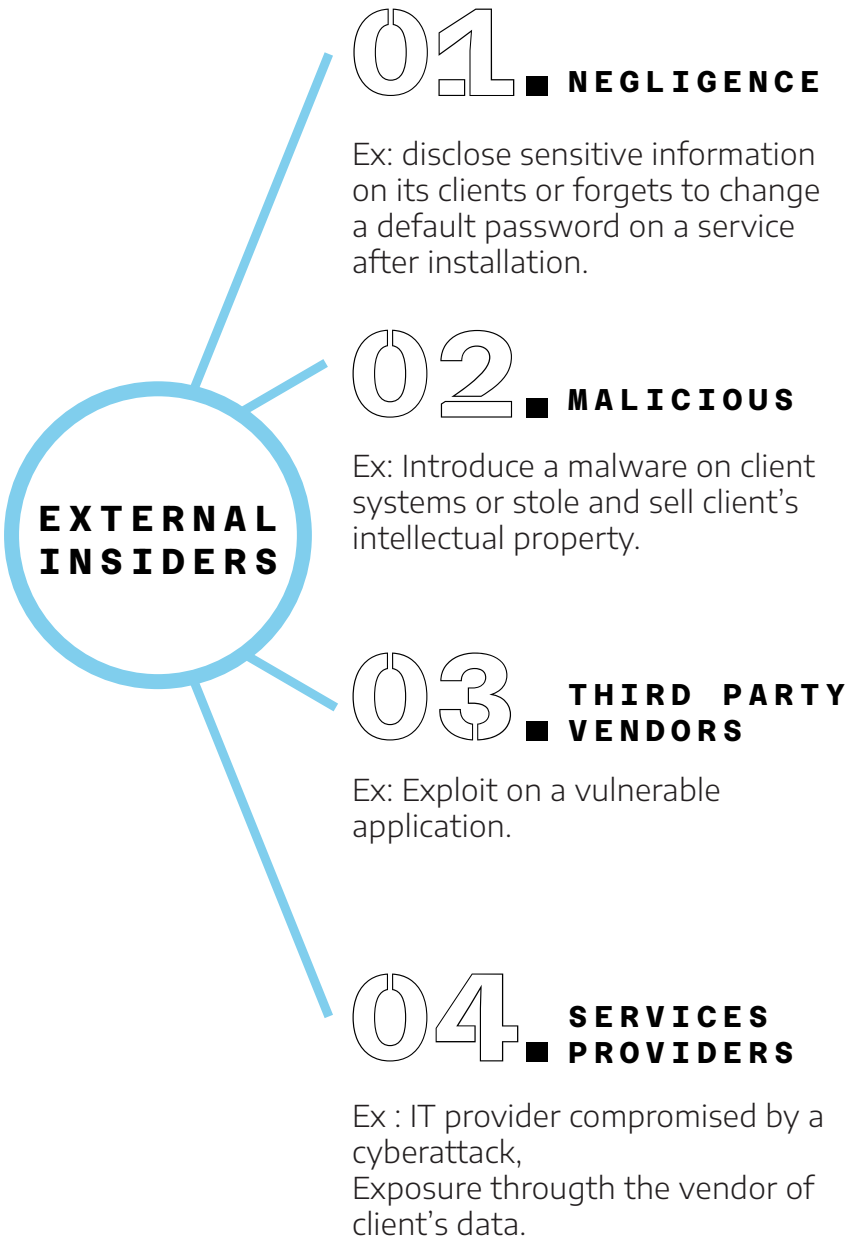


Figure 5: External Insiders

2.3 Beyond the term impact: what to expect?

Impacts varies from a victim to another depending on the organization's nature and the insider's motivation. The common consequences are:

- Sensitive data loss;
- Operation disruption or malfunction;
- Damage to the brand and its image;
- Break up innovation process and market shares loss;
- Competitive or strategic edge loss,
- Market drop;

And the list goes on. It affects both a tangible dimension, production and an intangible dimension: the information assets.

One of the challenges for companies is to be able to predict the cost of a cyberattack. Even though calculation methods have emerged in the last decades like the FAIR analysis[5], it remains difficult to known for sure what to put behind financial loss.

However, we can distinguish two types:

- Direct cost includes resources used for all actions of detection, investigation, mitigation, and remediation, operation shutdown, etc.
- Indirect cost relates to all the resources and people mobilized on the incident.

2.3.1 Information assets, your prise possession

Business value is based on all the information assets that it produces and safeguard. Those can be sensitive data, people, facilities, intellectual property, etc[6]. Because information assets can give an advantage in a competitive market, they are considered as intelligence and are protected under the law. For example, some sensitive data fall under business secrecy in French Commercial Code such as:

- Manufacturing processes;
- Pharmaceutical test data;
- Drawings and graphic representations of computer programmes;
- Distribution methods;
- List of suppliers;
- Advertising strategies;
- Formulas;
- Recipes;
- Source codes;
- etc.

In the wake of a data breach or leak, too few companies implement protection solutions (see section 5.2). It is important to bear in mind that even if the leaked data is not lost in the sense that the organization has implemented a backup program, the invisible impact is real. The data no longer has an owner since it is accessible and can be exploited by third parties to carry out other malicious actions that could once again damage the victim company.

2.3.2 Financial impacts

To understand the financial impact, we must go deeper into what business value means.

There are many ways to evaluate a business value. It can be done throughout market capitalization which "is the price an asset fetches in the market". Market capitalization is dynamic, and it depends on an assortment of factors". Intrinsic value on the over hand represents the actual cash flow that a company will generate, it is the true company worth considering its assets and liabilities values or other calculation methods.

Finally, when we want to know the financial impact of an insider attack, we must look at the ways its actions can hurt the value of the company.

5 The FAIR standard is a risk analysis methodology based on quantification. It considers the probable frequency and scale of losses.
6 Girollet, Albane. Gredoire, Chloé. 2022. Almond. "Protection du patrimoine informationnel : regard sur le cyber-espionnage".

Because stock markets are highly influenced by external factors, a company who has experienced an insider incident can see the price of shares fall but also recover as the market is always in movement. However, that recovery can take a long time, if it happens. The loss can be considerable, as we saw in multiples cases this past year, such as Medibank or Thales and affects all the ecosystem. One victim and all the supply chain can be in danger.

For the **intrinsic value**, it is another story. Because the evaluation is based on a fundamental analysis, which means that the calculation only considers the company itself and discards external factors. Losing intellectual property, which is an asset like R&D research or discovery, or customer data leaves the victim with nothing to differentiate itself from other companies on the market and lose its value.

Costs are hiding in all places as the victim besides revenue loss due to shut down will have to pay for potential lawsuit, fines, legal and audit fees. It can also hide under the degradation of credit score. It becomes difficult for such company to obtain funding from financial authorities, victims can see borrowing costs and financial risk exponentially increase.

2.3.3 Production shutdown

All risk analysis take consider operating loss as a direct impact of a cyber incident and the level depends on the business nature. From an insurance point of view, business interruption is defined as the loss of facilities or equipment that enables a company to carry on its activity and that leads to a total or partial shutdown.

In this study, the terms “disruption of operations” and “cessation of business” will therefore be preferred. This definition is essential if we are to understand the costs hidden behind the terminology. Operating loss is included in these terms.

A shutdown means a rippling effect that can be excessively costly. Interruption of a line in the automobile sector or the food industry, closure of plants, that’s people who can’t work but need to be paid, food wasted, delays to parts to be made and/or shipped, failure to complete orders and reimbursement of customers, repairs or replacement of equipment (etc.), are few examples of financial impacts in the end, next to safety impacts, social impacts, and much more.

2.3.4 An endless and vicious circle

Obviously, companies are focusing mostly on the direct financial impact, but we must consider the damage on the business as a whole. Even though we cannot put a definite number or a comprehensive idea on the real damage to a company reputation or on their partners, the impact cannot be dismissed.

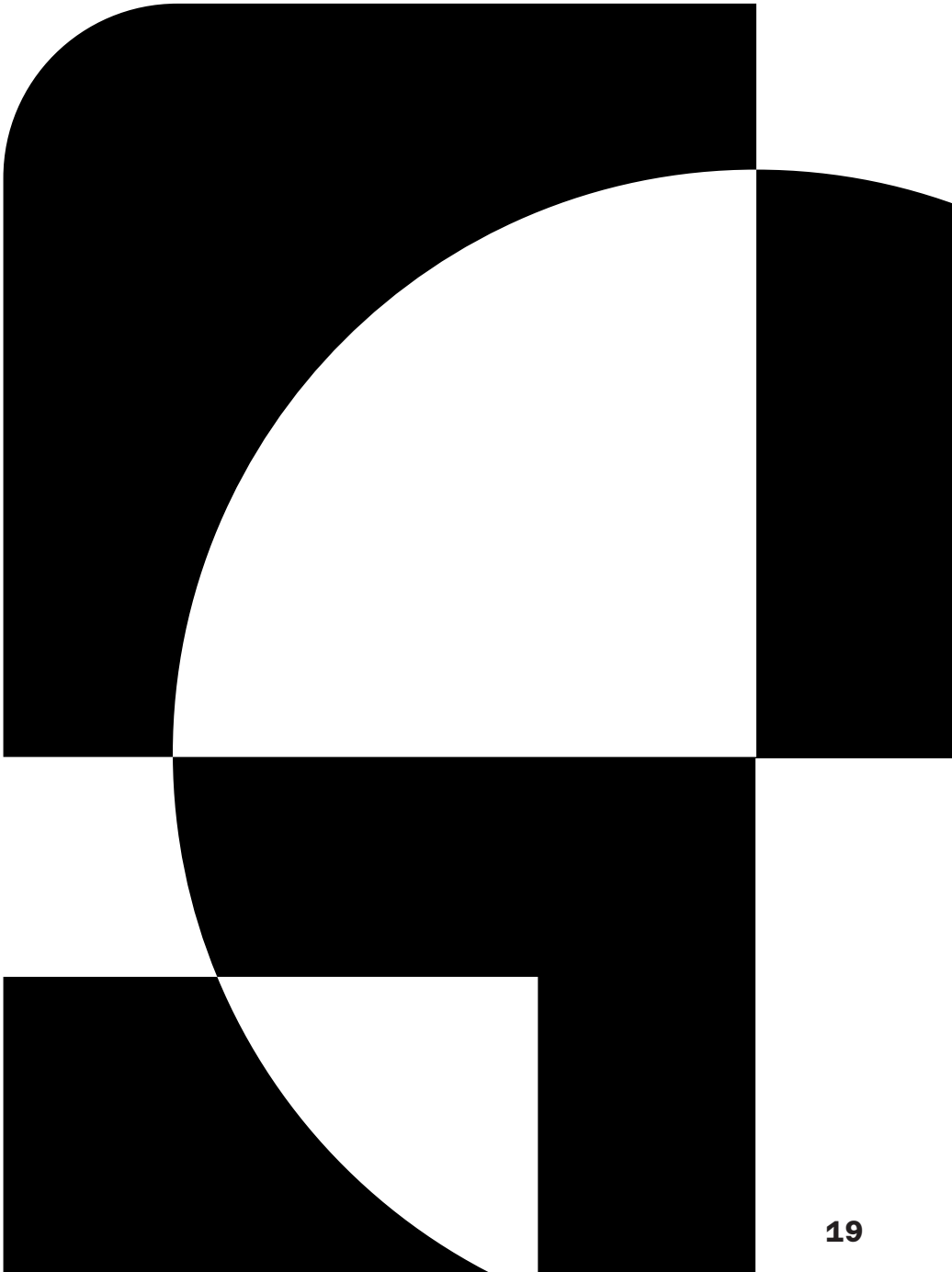
With an insider job, reputation damage can easily be more impactful, because it is represented as a failure of the company to ensure its safety and security protocols, doesn’t control its employees’ activities and cannot be trusted to safeguard customers’ data or investors’ money.

The same as a thief entering your home, even though you could have put more protection that eventuality is always on your mind. But being robbed by someone you know; people are quicker to say that you failed somewhere and that it’s your own responsibility. It doesn’t have to be true, it’s a perception and reputation is only a matter of perception.

So, a company will have to work hard to regain the customers and the market trust, rebuild its image or brand. When your company is based on its capacity to innovate and that the R&D department is compromised, that means delays on research, a loss of your time investment, and loss on business opportunities.

Social impacts are also to be accounted for. Following the metaphor of robbery, we must look also at the people remaining in the house. If it is a bit easier to blame another

party, when the intruder is one of your own, it put in disarray the company's values, the trust built in the office, against coworkers and the direction. A company's mission is to protect all data in its possession and more often the data theft concern employees of the company victim, no customers. And that means that personal and sensitive information like medical, are out in the world and can be used to hurt them in their personal life. For various industries and critical infrastructures, an attack can also have life or death consequences. Causing damage to water, energy, healthcare, telecom systems can mean putting employees but also civilians in danger.



PART

03.

HOW DOES THIS THREAT MATERIALISE?

3.1 From fiction to reality

3.1.1 Disruption in the retail sector

A single mistake and a cascade of events can lead to an economic peril. An internal feud can have external consequences such as conflict between companies and trigger the need to carry out crisis communication. We chose to demonstrate how this could happen in the fashion industry.

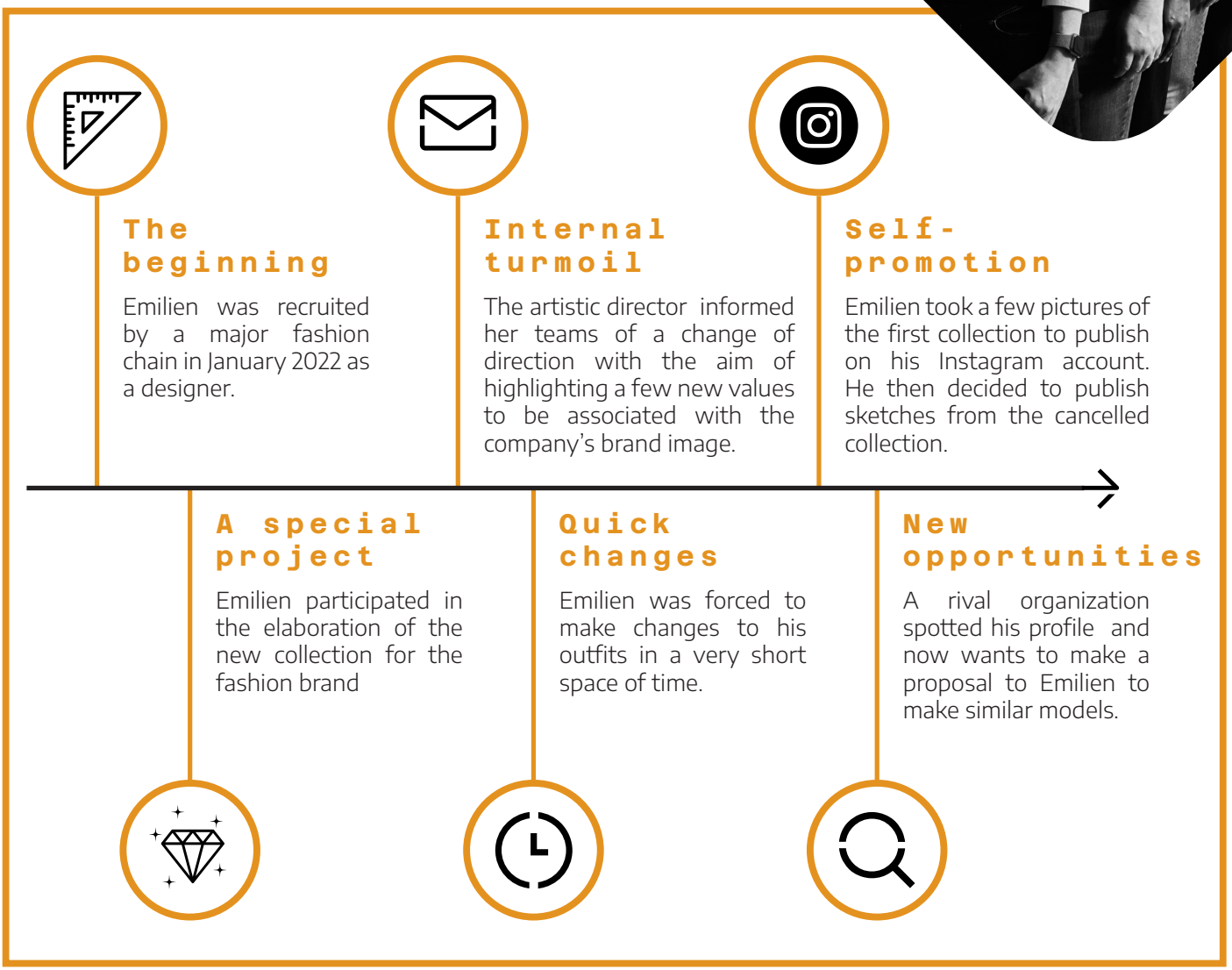


Figure 6: Scenario in the fashion industry

3.1.2 Bad practices in the healthcare sector

Medical institutions are known to have a weak security, that's why they are the prey of many ransomware gangs. These failures to comply with proper protective measures are often combined with negligence from employees.

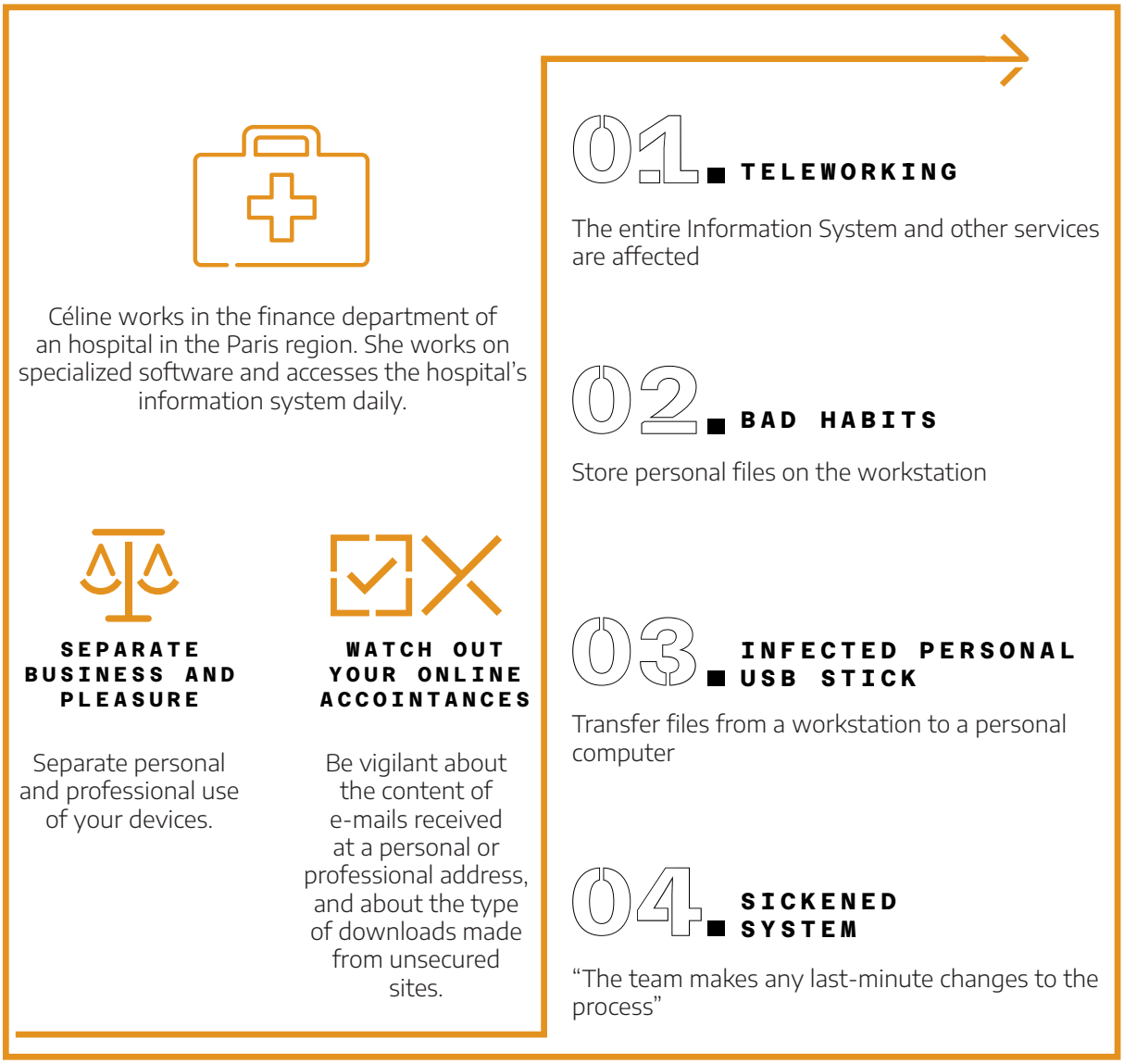


Figure 7: Scenario in a hospital

3.1.3 Data leak

A European consultancy firm has suffered a data leak following the departure of several employees in 2022 and 2023. In fact, since the departure of its employees, the company says it has seen a drop in business, justified by the termination of contracts with some of its long-standing partners and customers.

A member of management claims to have found 'worrying' emails sent to her ex-partner's email address, such as a list of clients and information on files she personally manages dating back to 2017 and 2019.

CERT CWATCH was commissioned by the company to conduct a forensic investigation of its information system to confirm or refute the hypothesis that confidential data had been leaked by staff who had left the company.

Furthermore, the employees under investigation are not the only ones who use their personal email addresses for professional exchanges. During our investigation, we were able to identify other employees using private e-mail addresses (although these were outside the scope of the study). In total, 3,432 e-mails were sent from work mailboxes to the personal e-mail addresses of the employees concerned.

CERT CWATCH Insights

The insider threat today is often people who are compromised by the clumsiness of employees. Almond's CWATCH has observed very few malicious insider threats but what we see the most are IT service providers being compromised or not complying with security standards. They don't monitor what their service providers are doing (applications not up to date, no mfa, etc.). When you're a big company, you can monitor your service providers, but not when you're an SME.

The striking new trend is that attackers are moving more and more towards supply chain attacks, attacking at random to compromise everything, and very often they start from a compromised account that already has high levels of access to the customer's domain.

3.2 The Dark web, an alternative LinkedIn

With the professionalization of cybercrime, threat actors have adopted a structure identical to a legitimate business. That means, in particular ransomware operators, have a division of labour based on skills and specialities and have support department like human resources. Inside their recruitment strategy, some cybercriminals show particular interest toward insiders because they offer several advantages:

- Either obtaining direct access to an organization targeted by attackers (the attackers have already found out about the company they are interested in);
- Or gaining access to a company that had not been identified by the attackers (the targeting of this organization had not yet been decided or the organization was unknown to the group of attackers).

As ransomware victimology rests on opportunities, it's the same for attacks convening insiders. However, with APT threat actors, different trends of behaviour can be of notice and determined by the target activity nature or sector.

3.2.1 The domination of cybercriminal groups

The cybercrime is like a spider web and insiders can be recruited by several types of cybercriminals that we must differentiate:

- Ransomware-as-a-Service (RAAS);
- Affiliates of RAAS;
- Third-party organizations such as Initial Access Brokers.

Three groups are known to have recruited insiders using a familiar language to create a strong bond with them: **LAPSUS$**, **Karakurt** and **BlackBasta**.
In November 2022, the Karakurt group published a general announcement on its Telegram channel stating:
"Do you work for a company that you hate with all your heart? Or maybe your boss fired you but forgot to turn off your network access? You can find solace in our arms."
BlackBasta was interested in buying access to companies located in Western countries, particularly among the Fives Eyes' members. This is one of the only BlackBasta posts identified on cybercrime forums.

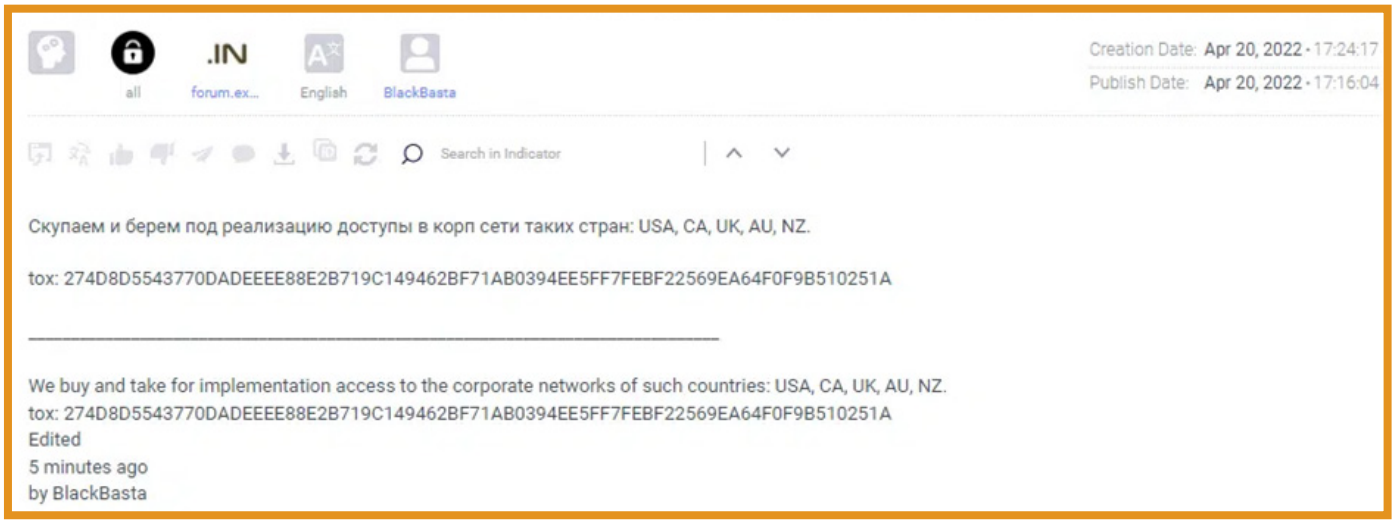


Figure 8: BlackBasta seeking access to corporate networks on the Exploit[.]in forum (source : https://cyberint.com/blog/research/blackbasta/)

3.2.2 Cybercrime forums: job providers

Like on business websites, groups have made available a category "Job Offer" on their forums. It can be well-organized groups like ransomware with strong marketing and communication skills or lone wolves with no attachment but rather acting on their own. Accessible on the Clear and on the Dark web, those pages allow forum members to publish job offers, including for insiders.

Analysts at Almond CWATCH have investigated several Dark web forums, including DARK2WEB. This is a Russian-speaking forum accessible via the TOR browser. On the DARK2WEB forum, CWATCH analysts identified two highly professional attacker profiles: "fastestinfo" and "MAESTRO_INFO".

Recruitment of employees from various structures for permanent cooperation in the field of information retrieval

- Hospital staff from the Russian Federation or European countries;
- Employees of mobile phone operators;
- Civil servants working for the Russian Federation;
- Employees of banks, including the French bank Société Générale;
- Employees of companies linked to social networks, including two American companies with Instagram and Twitter;
- Employees of messaging services, including the American company Whatsapp and the Chinese company Wechat;
- Employees of Russian postal services;
- Employees of taxi services and valet drivers, including the American company Uber;
- Employees of transport companies;
- Payment service companies, including the American company Paypal.

Figure 9: Insider job advert published by threat actor "fastestinfo"

Although this is an exceptionally lengthy list, the threat actors are not limiting their ambitions to this list and are accepting applications from insiders from other organizations not identified in this publication.

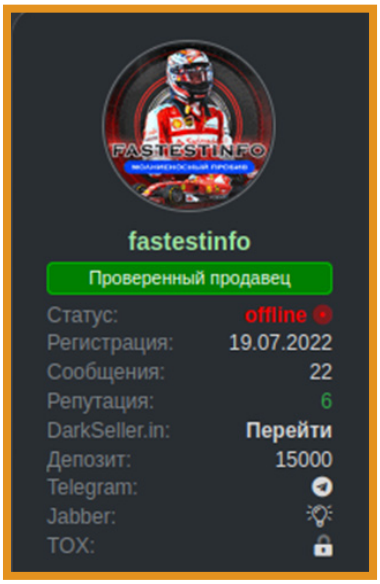


Figure 10: "fastest info"'s profile on the DARK2WEB forum

This malicious actor has a reputation score of 6 and 15,000 credits. This means that this threat actor has received several positive feedback from other forum members who have collaborated with him. "fastestinfo" also uses a few platforms to communicate with other cybercriminals, including Telegram, Jabber and Tox. Telegram is the most accessible, particularly for individuals unfamiliar with the codes of cybercriminal forums.
On its Telegram channel, "fastestinfo" resells data and documents from the same organizations from which they recruit insiders.

Figure 11: "In the 'Banking' category, the organizations Alfa Bank and VTB, which were present in the previous publication, are mentioned.

One of the threat actors identified by analysts at Almond CWATCH recruiting insiders in a substantial way is "MAESTRO_INFO".

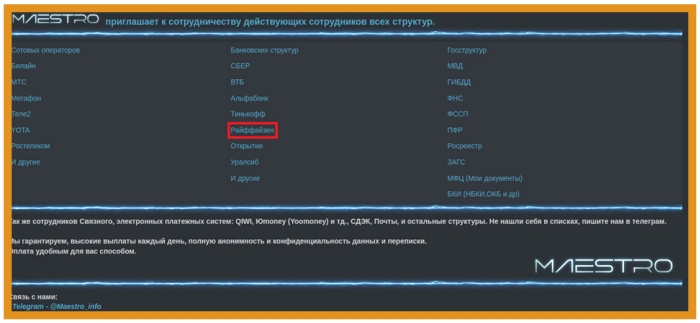


Figure 12: "MAESTRO_INFO" main targets

Like "fastestinfo", "MAESTRO_INFO" targets many organizations, mainly Russian, divided into three categories:

- Mobile phone operators;
- Banks;
- Government entities.

We have also identified one European organization, Raiffeisen, the third largest Swiss banking group. It should be noted that in 2022, this bank made more than half of its profits in Russia[7].
In addition to the categories listed, "MAESTRO_INFO" specifies its interest in individuals working with companies controlling electronic payment systems. Once again, the companies mentioned are Russian. However, the attackers mention that "if you are not on this list, contact us on Telegram". This threat actor is specialized in the collection of information throughout Russia and the Commonwealth of Independent States.

Figure 13: "MAESTRO_INFO"'s logo and moto

"MAESTRO_INFO" presents itself as an information research agency providing its employees with a high income, daily payments and a stable, regular earnings.

7 Anne, Drif. 2023. Les Echos. Ukraine : les profits embarrassants des banques européennes en Russie.

These two examples show us that these are structures akin to legitimate companies with substantial resources dedicated in part to human resources and to building a brand image that shines through the cybercrime ecosystem, at least the Russian one. For insiders, this professionalism can be seen as a guarantee of the financial resources of these groups, their ability to pay and the durability of the collaboration between the two parties. In this perspective, "MAESTRO_INFO" also ensures the complete anonymity and confidentiality of data.

However, this affirmation can be nuanced. Profiles that are less developed and seem to have fewer resources are also interested in insiders.

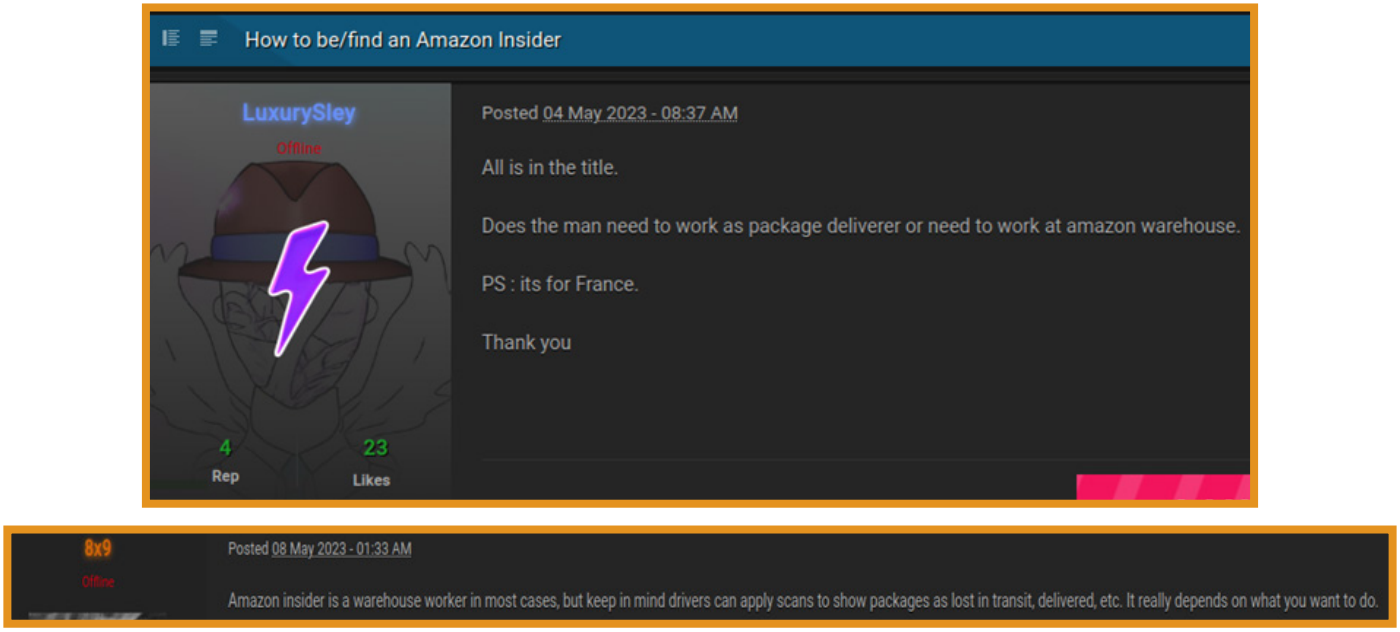


Figure 14: A very specific request to infiltrate a GAFAM company

Occasionally, cybercriminals ask their peers for advice to improve their malicious skills. Analysts at Almond CWATCH have also identified an offer published by a cybercriminal asking for advice on how to becom or find an insider at Amazon's offices in France. More specifically, in the body of his message, this individual asks about the best status an insider could adopt:

"Should the man work as a parcel delivery man or work in an Amazon warehouse?"

A forum member replies that in most cases, an insider works in Amazon's warehouses. He also highlights the place occupied by "drivers who can apply scans to indicate that parcels are lost in transit, delivered, etc.".

The example displays another hostile dimension of the malicious insider. He is not only likely to act on data, but also to disrupt the various stages of a process such as parcel delivery. For example, an employee having access to the warehouses of a company like Amazon could target specific individuals by accessing certain databases.

3.2.3 Interpretation of an insider's itinerary

How would an insider know about these forums?

We know that cybercriminal forums are also frequented by individuals with no technical knowledge, also called script kiddies. This paradigm shift has been made possible by the cybercriminals themselves, who have invested in new means of communication such as Telegram messaging or the Discord platform,

which are much more accessible than forums (see "Messageries et cybercriminels" in our **Threat Landscape 2022**). This new context is making it much easier for new cybercrime adepts to enter the insider market and start an unusual career.

Be courted or do the first step: a professional seduction exercise

Individuals driven by the conflict existing between them and their employer and a desire for revenge are particularly willing to contact cybercriminals. A malicious insider may make contact by responding directly to an offer or by directly publishing information already in the insider's possession.

People who are not involved in criminal affairs is not necessarily aware that it is possible to sell information in his possession. They can therefore simply seek to harm this organization in any way they wish by doing a simple internet search and quickly finding indications as to the nature of the sites to consult.

Nevertheless, despite the use of multiple platforms by cybercriminals, this type of offer has limited visibility due to its criminal nature and will not be listed on official job search websites.

The insider is also subject to the uncertainty of being hired by criminal organizations. There is no guarantee that the insider will receive the sum for which he has agreed to provide information.

In the end, being an insider is an uncomfortable position. You can easily be caught between your employer and the cybercriminals with whom you collaborate. They both have enough power to condemn the insider's future. When the insider relies on the expectation of getting paid for what he is about to do while putting his career at risk, the attackers have sufficient means of pressure to obtain more information about the organization and endanger their recruit.

Assumptions on physical canvassing

In the real-world job market, headhunters are always looking for the right person to hire. It the same in the criminal industry. Given the scale of the financial resources available to groups recruiting insiders in several sectors, it is plausible that they will deploy resources specifically dedicated to insider needs.
It is conceivable that their human resources departments could develop specific recruitment methods to approach individuals occupying strategic positions or with access to sensitive data.

In a comparable way to intelligence agencies seeking to contact sources, a highly organized group of attackers can sound out individuals able to provide information that will enable them to gain access to an organization's information system.

In some circumstances, these cybercriminals can pay somebody off, not to hire him specifically, but to try to clone badges and get inside with a normal access. Once inside, they can manipulate people and sit at a random unlocked workstation. No need for a VPN access. Even before starting anything, being able to walk within the company can easily appear as a sign of legitimacy and give some sense of trust to the people around so firewalls are not going to stop anything.

Lone wolves around: insiders using Dark web resources

An insider doesn't necessarily need to integrate a cybercriminal structure. There is enough malicious material available on underground forums to harm an organization. Someone with a non-technical background can buy ready-to-use platforms implementing useful functionalities. Everything is already set up by an experienced attacker and often work with user-friendly interface. If some elaborate malicious products can be available for a high price, there is also an abundant number of malware accessible for a cheap cost. Many of these services are popular and ready-to-use such as bots, phishing and exploit kits.

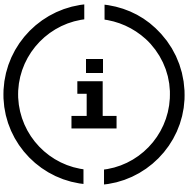
PART

04.

LEGAL TOOLS TO COUNTER INSIDER THREAT: CASE STUDY AND LEGAL SITUATION IN FRANCE

The insider threat is a major concern in enterprise risk management.

The means of mitigating this risk, taking disciplinary or even penal action, may be confronted with requirements in terms of data confidentiality and privacy.



Caution: When an employee neglects its duties, his company's liability can be engaged in order to compensate its customers/ partners.

The convicted company can also act against its employee (under certain conditions). However, the employee's personal liability is directly engaged when:

- Acts outside the scope of his duties;
- Acts without authorization;
- Acts for purposes unrelated to his or her duties.

Fighting insider threats requires a thorough understanding of the legal and regulatory implications. Programs addressing these threats delve into various intricate legal matters, like privacy rights, labour laws, and individual due process rights, among others.

In France, companies have few legal options to shield against inside threats but these actions must be fair and respect employees' rights and freedoms.

To use legal means, companies first need to qualify the offence by determining whether it was unintentional (negligence, accident) or intentional (malicious act).

Nevertheless, using these measures involves the presentation of evidence, which raises concerns about legitimacy, admissibility and balancing with privacy rights.

4.1 How does a company fend off insiders?

While under a contract, any employee must behave according to the company's rules. Otherwise, an employer has the possibility of inflicting sanctions. You can pay a high price for misconduct and eventually end being dismissed.

If employees fail to comply with the rules imposed by their employment contract or internal company regulations covered by French labour law, they may be penalized. These sanctions must be proportionate to the fact and can go as far as dismissal for serious misconduct.

That's why it's important to include specific confidentiality and non-competition clauses in employment contracts so that they have a real legal force.

In the same way, the company's internal regulations must specify particular information systems security rules, as well as the punishments for breaking them. It is also recommended to append the IT charter for employees and administrators to the company's internal regulations or to each employee's employment contract.

4.2 Penal sanctions targeting insiders: multifaceted qualifications

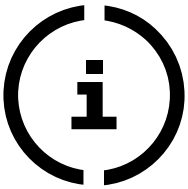
Several texts in French criminal law can be retained in the context of internal threat. The relevant category of our context analysis is the category of the misdemeanours.

What does French criminal law say? "There is no crime or misdemeanour without the intention to commit it".

Certain acts performed by insiders can be translated legally by employers:

- **Damage to automated data processing systems**, in particular fraudulent accesses, and this may include unauthorized access to the data; or obstruction, as hindering or distorting the functioning of the system; or even providing the means (tools, passwords, etc.) to commit an offence;
- **Theft**, defined as taking someone else's property with intent, applies to tangible items under French law. So, it's the physical aspect that matters. However, making unauthorized copies of company data (like photocopying or using a USB drive) could still be seen as a form of theft;
- **Breach of trust**, which can be constituted when an employee makes improper use material or immaterial property entrusted to them for a specific purpose (misappropriation, damage, and intent);
- **Fraud, complicity in fraud or attempted fraud**, constituted by an act of deception to enable someone to get money, assets, services, or agreement for something.

Furthermore, some French codes contain penal provisions, as the French labour code[8] and covers the case of divulgation of trade secret manufacturing or such as the French Intellectual Property Code with counterfeit of intellectual property rights.



Legal proceedings are not a piece of cake and providing evidence can quickly become complex.

Evidence must be gathered fairly, with due respect for the dignity of justice and the rights of others. This is the principle of "legality of evidence" in French law. This means, for example, respecting the right to privacy of employees.

8 Ruling of September 30, 2020, by the Social Division of the French Court of Cassation.

4.3 Conciliation between professional obligations and privacy

An employee was dismissed for serious misconduct by the French company Petit Bateau following the publication of a photograph on a social network.

PETIT BATEAU BEING IN DEEP WATER

An employee published on Facebook a photograph depicting part of the next collection

A confidentiality clause in the employee's contract prohibited the publication of such a photograph

It was a private account reserved for "my friends", which did not include the employer

The employee contested her dismissal before the Paris Court of Appeal, which nonetheless ruled that she had committed serious misconduct.

The evidence was sent to the company by another employee, authorized to access the private account and therefore there was no reason to disregard it.

The evidence infringed on the employee's privacy, but the employer's right to evidence justified a judgement of proportionality.

Figure 16: Petit Bateau being in deep water

4.4 The CNIL, the watchdog of your data position

To prevent the risks associated with the insider threat, a certain number of measures recommended by the CNIL[9] should be taken upstream by companies, as a preventive measure. For example, the CNIL recognises the relevance of carrying out certain types of checks regarding the internet use within an organization:

- Installation of site filtering systems;
- Virus detection;
- These checks can also be carried out on the company's email system;
- Tools to measure the frequency of sending and/or the size of messages;
- Anti-spam filters.

The CNIL points out that a company's powers of control and surveillance are limited by its obligation to respect the privacy of its employees. The separation of private and professional affairs is very prevalent in France (see **section 4.3** Conciliation: the right of evidence and the employee's right to privacy).

The employer cannot access communications or files deemed as private by the employee. Their private nature is defined by the employee. However, "mail will not be considered personal simply because it is filed in the "my documents" directory or in a folder identified by the employee's initials[10]."

But private doesn't mean that these files completely sealed and unattainable. Two circumstances to remember. First, the employee must be present if his or her superiors wish to consult these files. Second, if criminal proceedings are brought against a malicious insider suspected of stealing data, the courts will be able to inspect the suspect's correspondence.

4.5 Concrete examples from France and Europe

There are many known examples of insider threat abroad, particularly affecting large companies. In the case of France, we have identified few examples that have been brought to court.

4.5.1 An employee installs a malware in his company[11]

In the 2000's, an employee unintentionally installed malware on their company's computer system. Following this incident, the employee was dismissed on the following grounds: "gross misconduct also results from his failure to warn his line manager or the IT technical department when he saw the first viruses arrive". The Versailles industrial tribunal reclassified the misconduct as simple misconduct.

4.5.2 Data leak at Cdiscount[12]

In 2021, an employee holding a position of responsibility within the company (warehouse manager) took the initiative of downloading data containing information about 33 million of the organization's customers. The individual created a profile on a Dark web forum with the aim of selling the data to one or more malicious parties.

9 The CNIL, or the French Data Protection Authority (Commission nationale de l'informatique et des libertés), is an independant administration in charge of the protection of personal data. It has the power to inform and advise organizations as well as inflict sanctions for non-compliance with the RGPD and the Data Protection Act or even invasion of privacy.
10 **CNIL. 2015. Le contrôle de l'utilisation d'Internet et de la messagerie électronique.**
11 **Tabaka, Benoît (blog). 2010. "La contamination par un virus du réseau de l'employeur n'est pas une faute lourde mais une faute simple."**
12 **CAPITAL.2021. "Cdiscount : un haut responsable soupçonné d'un immense vol de données de clients."**

The individual has been charged with a few misdemeanours:

- Fraudulent extraction of data from an automated processing system;
- Breach of trust;
- Swindling.

4.5.3 Internal data theft[13]

In 2014, an employee of an insurance brokerage company stole more than 300 files belonging to his employer. The documents were sent from his work e-mail account to his personal e-mail account.

Following the trial, this individual was:

- Found guilty of breach of trust;
- Fined €10,000;
- Ordered to pay symbolic damages of €1.

4.5.4 Belgian bank Degroof Petercam takes legal action against its former employees[14]

In Belgium, in 2023, the Degroof Petercam bank acted against several of its former employees following a data leak involving hundreds of customers. The files stolen were sensitive customer files relating to stock option plans. They had been downloaded to an IP address outside the bank's networks. The data exposed includes postal address, email address, user ID, bank account numbers, passport and ID card numbers, and financial data. The company says it has reported the incident to the Belgian data protection authority.

13 Madjid, Dalila. 2014. Legavox. "Abus de confiance : détournement de données confidentielles au préjudice de l'employeur."
14 LE VIF. 2023. Degroof Petercam: la banque poursuit des ex-employés pour vol de données personnelles".

PART

05.

THE MAIN STAGES OF THE FIGHT AGAINST THE INSIDER THREAT

To protect organizations, programs are put in place to reduce the risks associated with this threat. These programs are structured by internal company policies. They help to raise employee awareness and anticipate threats. Alongside these programs, multiple solutions are available on the market, whose key role is to detect suspicious behaviour.

5.1 Awareness and training, the first course of action

Implementing the right measures from the beginning should prevent the proliferation of insider-related events. Raising awareness and anticipating the insider threat are the priority steps to set a good strategy.

5.1.1 Peers' vigilance: letting social control do the job

In an IBM report[15], experts identified that in all types of data breach, from insiders or cybergroups, employees training is a key factor to reduce the occurrence and the cost of incidents. In addition to standard precautions, programs must be updated to reflect the insider threat complexity. Like whistleblowers, employees are the first guard and must be able to identify suspicious activities without creating an untrusted work environment. The awareness program should address diverse groups to inform of responsibilities and educate on recognizable early signs.

Obviously, there are little actions that you can do on profiles like malicious or unresponsive insiders. You may want to invest on detection solutions but at what price and what you must do before.

Employees

- Understand what constitutes an insider threat and risks;
- Knowing the IT charter, its responsabilities and the sanctions in case of failling to comply;
- Knowing the internal security requirements and best practices;
- Understand the main indicators in their environment;
- Recognize the way they can become unintentional insiders;
- Identify targeting behaviour or approach attempts from external threat actors;
- Knowing the internal alert process in case of suspicion.

Management

- Understand what constitutes an insider threat and risks;
- Identify the different profiles of insiders;
- Understand the main indicators in their environment;
- Identify reportable behaviour from employees and potential insiders;
- Describe the way to respond to identified insider behaviour;
- Knowing the alert internal process in case of suspicion.

Insiders

- Understand what constitutes an insider threat and risks;
- Knowing the IT charter and its responsabilities and the sanctions in case of failling to comply;
- Understand the consequences of becoming a malicious insider;
- Knowing the internal security requirements and best practices.

Figure 17: Awareness programs targeted for specific populations

15 IBM. 2023. "Cost of a Data Breach Report".

5.1.2 Or replace humans by machines?

Of course, the most serious incidents concern information or technologies granting value to a company. But **the solutions also have an educational role to play**, helping to train a company's population in every branches.

A UEBA (User & Entity Behaviour Analytics) solution must be able to raise awareness. UEBAs are user behaviour analysis software. They operate like a set of alerts within a SOC (Security Operations Center). These alerts can be triggered very easily and will increment a sort of score. As soon as they exceed a certain threshold, behavioural detection is triggered (see How UEBAs (User & Entity Behaviour Analytics) work in **section 5.3**).

As with all detection mechanisms, they can be used to identify usage that does not comply with the company's policy. A well-designed UEBA technology must be able to distinguish between these two types of insiders. This distinction will be made at the level of the user's modus operandi. For example, a careless user will occasionally perform actions that do not comply with the rules. And even if some use is not malicious, it must be reported. This makes it possible to raise awareness among negligent users and to guide a company's population, improve employees' reflexes and put a stop to bad practices, even if they are not harmful.

In UEBA, malicious actions will take the form of a concatenation of actions that lead to compromise or damage to reputation. A UEBA technology must be adapted to a company's detection needs. For an organization, the conditions for moving the detection cursor from very verbose to less verbose must be determined, while trying to limit exposure to a loss of relevance.

Insiders' diversity is a driving force to develop the solutions market. We can find even more specialised solutions, such as phishing solutions. They offer to supervise employees' behaviour by sending alerts via Windows that open automatically and directly inform the user of their bad behaviour. As well as raising awareness on an ad hoc basis, there is ongoing monitoring of the employee with the aim of avoiding any risky behaviour. The employer's main concern is therefore to reduce the risks to the company's integrity and health. But these choices raise other questions regarding the level of surveillance and constraints imposed on employees.

5.1.3 Resources available to the employer

Although employees are protected by a few measures such as the obligation for an organization to inform and consult their works council, companies also have the capacity to mobilize several means. Prevention and the training of employees in the threats posed by insiders are the main tools that employers can mobilize.

Not everyone is equal in a company and some departments are particularly at risk, especially recruiters. Cybercriminal syndicates hire and train individuals with the aim of infiltrating companies and amass sensitive data. This is an unorthodox business model known as **Insider-as-a-Service**, which is part of a larger model known as **Cybercrime-as-a-Service**.

It is important to train human resources teams who recruit new employees to assess them. This threat also affects people who already hold office or about to be promoted. People who are promoted are potentially able to obtain new, more restricted access rights within the organization, and to obtain information at a higher level of confidentiality. So, depending on their status and internal development, employees can be assessed according to their risk profile. Several factors need to be considered when carrying out this assessment, such as the individual's history within or outside the company and their relationships with other employees.

An insider's mission can be a one-time assignment.

However, a successful collaboration between an insider and a cyber gang can lead to a long-lasting partnership and cause more damage to a company.

5.2 Protecting your information system

About the network, you need to consider the appropriate segmentation strategy. The IT department must put in place a strict access rights policy and avoid mistakenly giving someone an unauthorized access or access they do not need during their duties. The alternative can be an open door for threat actors that look for people with access during their reconnaissance phase. They can either compromise them through social engineering and phishing or hiring them as insiders. Threat actors look particularly for employees in the IT department, who have privileged access to anyone's workstation. Gaining access to an administrator's machine without him knowing it or with its complicity, is a sesame for any attacker to reach all parts of a network. A solution like a Zero-Trust architecture appears to be a possible approach to protect an information system for insider's intrusion attempts.

The Zero-Trust model is based on the principle of least privilege and is designed to respond to the fact that the perimeter defence model has been overtaken by the rise of the cloud and the use of personal machines to carry out professional tasks (Bring Your Own Device). It is based on the principle that no individual can gain unauthorized access to an organization's resources. Not a single employee requesting access, regardless of its status, can be given a sufficient level of trust. At each new connection attempt and each new access request, individuals must authenticate themselves and the devices they use to demonstrate a form of legitimacy. This control over individuals is constant, progressive and is applied to each new access request and to each network component separately to partition each area in the event of an intrusion.

This model is in line with the concept of "defence in depth", i.e. "a global and dynamic defence, coordinating several lines of defence covering the entire depth of the system. The term depth must be understood in the broadest sense, i.e. in the organization of the IS [information system], in its implementation and finally in the technologies used. The aim is to enable actions to be taken to neutralise security breaches, at the lowest possible cost, thanks to risk management, an intelligence system, reaction planning and the constant enhancement of feedback[16]".

This model also has certain limitations:

- A Zero-Trust Architecture is complex to implement;
- Authentication processes take a lot of time;
- Maintenance costs can weight on an organization's resources;
- A Zero-Trust architect doesn't eliminate risks.

As part of an overall strategy, we must consider other prevention solutions including Data Loss Prevention (DLP). It enables an organization to identify, discover, monitor and classify sensitive data according to their level of confidentiality. Similarly, to Zero-Trust, a DLP solution is another layer added to administer the attribution of different types of accesses. It should be implemented to avoid the misdirection, abuse or mishandle of data leading to their exfiltration.

The more effort you put to elaborate your strategy, the more compliant you will be with security norms such as PCI DSS and the GDPR. The same way you must manage who has access to your company and to what extent, you should bring to light the way information circulates within the company. Is this transfer of information between two people legitimate? Who is the person transmitting data and who receives it? Once you'll be aware of it, you'll be in a position to enforce sharing policies and better protect your assets as well as intellectual property.

16 Secrétariat général de la défense nationale. 2004. La défense en profondeur appliquée aux systèmes d'information.

A DLP solution is also a mean to improve your overall organization by giving visibility to all the types of information you own. The status attributed to the classified information will rule over your ability to move data outside of the network and eventually blocking it.

5.3 Detecting the threatening behaviours

Detection is the last line of defence against insider threat meaning that it comes at the last moment. In short, all the barriers preceding the actual detection of the insider have failed and the company's overall protection strategy needs to be reviewed.

Detecting a case of insider threat means having excellent overall security hygiene. You need to have mechanisms in place upstream, a zero-trust network and air gap networks when you are trying to protect highly confidential information or technologies.

The use of solutions alone cannot help detecting an internal threat and they are not a means of prevention either.

UEBAs are positioned at the end of the chain, with detection mechanisms coming into play when all other security mechanisms have failed. But in other situations, when it is linked to a SOAR, incident prevention can be envisaged, because with each new detection, it is possible to mitigate an incident according to a decision tree.

Solution Focus: misconducts to expect

In most solutions, there are common categories of insider behaviour taken into consideration. Some of the selected behaviours can sometimes seem far from a deviant one. They concern internet use, the type of connection, email communication and use of available tools and devices.

Internet use	Type of connection	Transfers & communication	Use of available tools & devices
Private browsing/ Changing security settings	Impossible journey	Email containing sensitive data or offensive content	Using the screenshot tool/ Pasting texts of files
Job search websites	New location	File sharing	Large print job
Clear browser history	Unusual time of the day	Uploading documents on the cloud	Using easily hijackable software

Figure 18: Common behaviours analyzed by UEBAs

The over-representation of a category of behaviour may depend on the type of population analysed. However, there are certain behaviours that we find more often such as manipulating files, plugging in USB sticks and using a service in an unusual way. They are notably more common than password compromise which constitutes a strong signal.

5.4 User behaviour analysis software: a necessary step in detecting insider threats?

5.4.1 How UEBAs (User & Entity Behaviour Analytics) work?

Despite their elaborated denomination, these solutions do not contain any innovative technology. They are an aggregation of specific detection techniques. We will see that this software is developed in a certain context and that these solutions present several limitations. We can also highlight that not all UEBA mechanisms are suitable for all contexts and do not work on all types of businesses. Some solutions are linked to information systems implementing Windows and Kerberos authentication. Some services are also customized by a robot. They must apply to the sector of activity concerned and to their populations.

The main challenge facing all these players is to avoid false positives, even more so within a SOC. An incident can also be tagged using assets, which makes it possible to assess whether one incident is more critical than another during the qualification phase.

Overall, these solutions are only one link in a more comprehensive threat detection strategy.

First thing first, you need to consider with your editor solution a cursor on the volumetry of behaviours you want to monitor.

One of the issues to deal with is the verbosity of alerts. Within a given organization, it is likely that a certain number of individuals will exfiltrate data. However, not all this data is confidential. That may impact the solution's reports relevance.

UEBA technology must be adapted to a company's detection needs.

For example, a company seeing its data related to a due diligence exfiltrated is a serious event that could lead to a contract loss or the disruption of stock market prices. To Private Equity companies, a single file that is released is an occasional occurrence from a UEBA point of view, but to the business it's a serious event. The same example can be applied to the retail sector.

5.4.2 A pertinent solution? The case of a use within a SOC

These tools are only of interest when they are used in addition to other threat detection solutions. A UEBA is one of the detection sources of a SOC. That detection can be automated and linked to SOARs, if available.

However, the UEBA rule sets are not suited to the same uses as a SOC. The solutions can detect malicious and weak signals. Around 5 to 6 weak signals are enough to classify a behaviour as malicious. Unlike the alerts that can be processed by a SOC, many weak signals change little or not at all. However, strong signals must evolve depending on the modus operandi spotted. If these strong signals are not properly identified, then we can consider that the detection has failed.

Solutions are malleable objects. They adapt and consider threat intelligence feeds, IP address reputation data and Windows updates to better determine and qualify a threat. The use of threat intelligence feeds as well as the MITRE ATT&CK framework enables these solutions to adapt instantly to the threat landscape. They must also consider Living Off The Land Binaries (lolbin) and Living Off The Land Binaries And Scripts (lolbas). Other technical aspects such as DevOps and machine learning need to be kept up to date and may require monitoring.

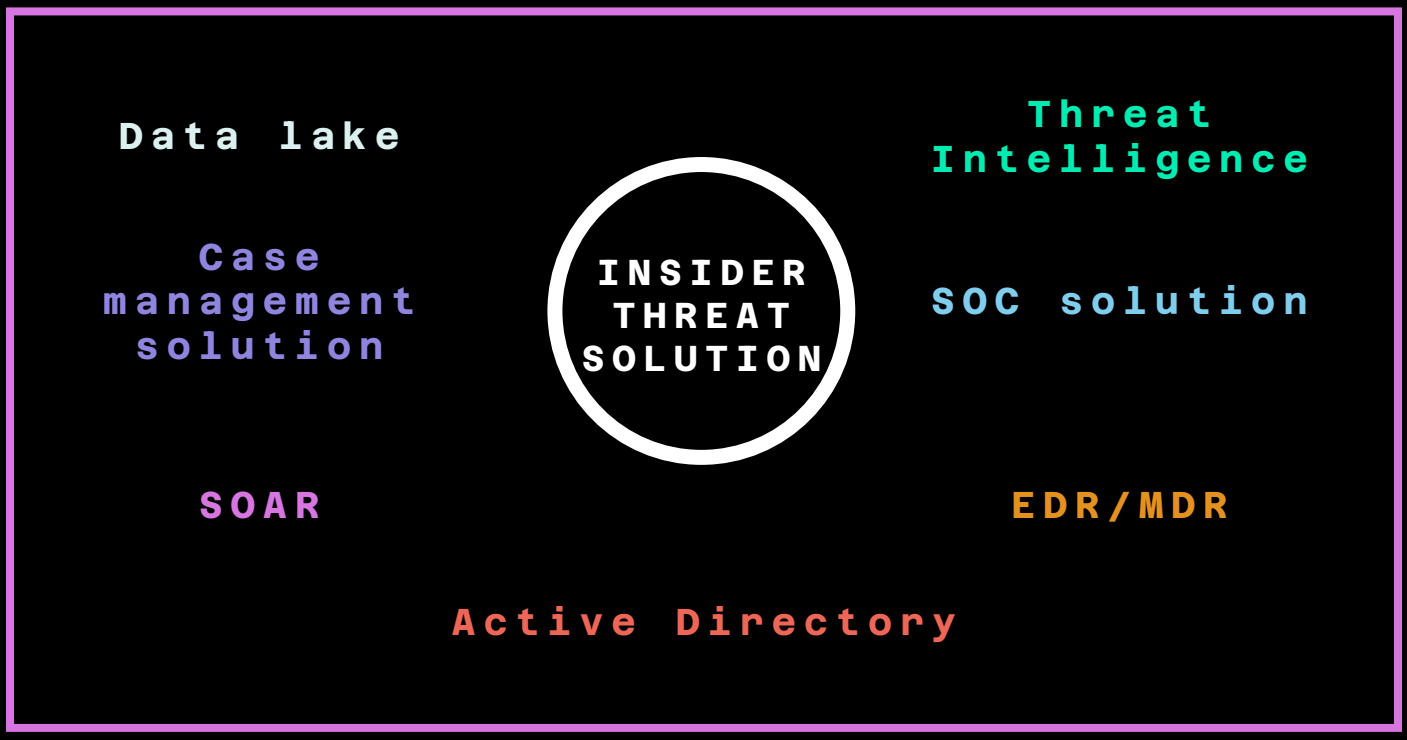


Figure 19: Types of platforms used to feed an Insider Threat solution

People who want to implement solutions must take the rights decisions to create a structured and efficient product able to detect insiders' behaviours.

Firstly, you must use a combination of methods and to select the relevant logs.

You must keep in mind that blind spots can appear when you don't have the logs available to cover all scope of your employees' activities.

Another key element is the solution configuration and proper usage. A company can implement all kind of solutions, but it is possible that nobody is looking at them. At the end, there is a good chance that the solution will miss something. You must bear in mind that to reduce the number of false positives, you must keep an eye on things that seems of no interest to you. When put into a certain context, those false positives can have a real impact.

You can also have editors who implement the solution in a partial way and make the solution lose its interest. But ultimately, the customer chooses where to place his priorities. The perfect blend is not unique because multiple variables specific to a company must be acknowledged and considered by the editors. A solution should be as efficient as possible and easy to use while ensuring that customers do not need cutting-edge resources.

5.4.3 Machine learning and behaviour detection: beyond the buzzword

Artificial intelligence is flooding the solutions market. Machine learning enables an insider threat solution to learn the behaviour of users and the machines they use.

The way it works, this learning process takes around 3 weeks. When a user's behaviour changes, the score used to evaluate them and indicate the number of incidents increases. The history of an individual's score, on the other hand, shows a clear change in behaviour and provides an overview of all the anomalies detected over a given period (rule results). This score is therefore likely to change. Depending on the individual, this score may exceed a certain threshold and therefore must be managed by analysts. These changes in behaviour can be detected even without a specific rule. For some solutions, there are

more than 1,000 rules based on machine learning and combined with risk analysis.

Some solutions may be based on unsupervised machine learning, which enables the entities to be monitored to be profiled. This will make it possible to challenge what has been learned and what is currently being done. As well as learning new behaviours, machine learning will also eventually understand behaviours becoming normalised.

The challenge for all the players offering this type of solution is to avoid false positives even more than a SOC or an EDR (Endpoint Detection & Response), because there are large notes, and you need to be able to close them immediately. When an EDR is put in place, there is a whole learning phase, which will build up a set of contextual data about the company.

It is the same thing for UEBA editors, who have an active data set (which relates to around the last 20 days) and a passive data set (which relates to general events). There is also a question of tagging assets to better qualify the criticality of an incident.

A UEBA solution aggregates all the data made available but must maintain a balance between the volume generated and the relevance of the alerts presented. It is technically possible to focus on the surveillance of a particular individual, but this operation is likely to alter the level of relevance of the threshold set and would increase the risk of missing a malicious action.

A solution can also distinguish between nominative accounts and service accounts because the same detections are not applied to them. To avoid false positives, a solution can also combine the analysis of an individual's history with that of the behaviour of groups of users to highlight behaviour that deviates from a norm. A solution can include a behavioural index based on models that profile users in relation to themselves and in relation to a group.

For example, someone working in the human resources department uses a super admin account and then uses another machine. This change in behaviour will be considered by machine learning, which integrates the fact that this user has never used a privileged account and therefore considers it to be an anomaly. In the same way, the behaviour of an individual logging in from another country will be considered if they are not a roaming user.

Although monitoring users' behaviour remains a key point, when an organization is faced with the theft of identifiers, these solutions will not be able to take this into account.

Overall, these solutions are developed in a certain context and have several limitations. The use of artificial intelligence and machine learning is increasingly mentioned by the publishers behind UEBA solutions. However, analysts at Almond's CWATCH believe that AI (Artificial Intelligence) should be used in a more targeted way and is not relevant in all cases. It should be used to aid interpreting results as well as decision support.

5.4.4 Further considerations

Beyond their technical aspects, there are multiples other stakes surrounding insider threat solutions.

First from an organizational point of view, when implementing those types of surveillance solutions, we must be aware of your employees' perception. You may choose not to communicate on the new detection solution, but after some time, it may become popular knowledge and even a social problem within your organization. To be effective, when an insider behaviour is detected, an action must be taken like contacting the manager. That action means putting a light on the solution which can be an issue in organization with a trade union. Employees becoming aware of the solution can also act as a deterrent. However, if you choose to make it public in the early

decision process you may be constrained to abandon the project due to a union resistance. Within organization, it's always a struggle navigating between a perceived surveillance and security.

Almond CWATCH advises transparency and put in place a change management process to help employees see the importance and the true purpose of those type of solutions. It's important that without necessarily know their score, they understand why there is a system monitoring and what they can expect in terms of alerts, reports and sanctions. It must be put in the IT charter, a document certifying the maturity of a company and the degree of control is has over their tools.

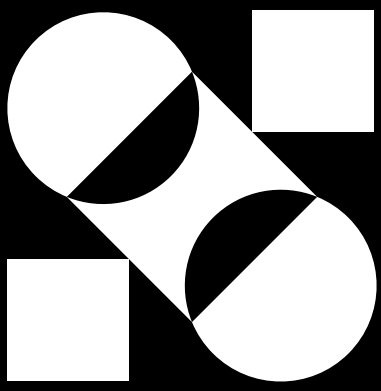
Almond also recommends having a strong process in place to deal with the human repercussions of an insider's actions, mostly for the negligent insiders. The type of sanctions to be applied must be precisely defined in internal policies.

Customers of a SOC or a detection solution will be notified when a negligent insider has been identified. The use of these solutions very often leads an organization to identify individuals who do not comply with internal policy and to become aware of the necessary adjustments. These are negligent insiders who, through ignorance, carry out harmful actions. It happens that the occurrence of several successive reports leads employees to become aware of the surveillance carried out during their professional activities.

It is also important to qualify the nature of the behaviours that may come under the heading of insider threat. A behaviour identified as an anomaly is not necessarily a threat. One type of behaviour may be problematic for one company but not for another, even though these threats are often underestimated.

Secondly, from a regulation point of view, authorities have introduced the principle of personal liability into the new security texts like the European Directive Network and Information Security 2 (NIS2). Indeed, the NIS2 directive, makes directors liable for failure to comply with cybersecurity obligations which could have helped to detect this type of threat.

Lastly, the location of a company can affects the way a solution is implemented. What's more, implementing these solutions in Europe often involves considering elements that are specific to this regulatory environment. Although there are similar expectations between the European and foreign markets regarding the content and capabilities of these solutions, the protection of personal data has become an essential step for European organizations. Logging, or log management, must therefore comply with the standards imposed by the General Data Protection Regulation (GDPR), as well as the provisions set out in employees' contracts of employment. Some solutions offer features used mainly by the European market, such as the implementation of technologies to encrypt overly sensitive personal data for certain types of users. The same goes for artificial intelligence. Europe through the IA Act tries to regulate the usages of those type of technologies in an organization. It sets new standards with identified risks considered as unacceptable. Social scoring is one of them and it could lead to the classification of people based on their behaviour.



CONCLUSION

The insider threat occurs on multiple levels within an organization and requires to be constantly on guard. From the legal framework to technology, there are tools to help you deal with it. But that's not enough. You must invest in humans and in an elaborated access control policy to regulate employees' admissions according to their current rights.

As a multi-dimensional threat, the insider is able to tackle and pass over all traditional security barriers put in place. Because of its nature, protective measures must target global processes, the company's environment and external connections as well as individuals.

When all measures put in place to counter the insider threat failed, and the crisis eventually breaks out, it is time for remediation. Remediation designates activities relating to the restoration of all the internal processes within an organization to their initial operating state.

A few figures, according to the data published by the Ponemon Institute in 2022, it takes between 77 and 85 days to detect an insider threat. In total, the remediation of an incident costs $6.6 million on average and "the total average cost of activities to resolve insider threats over a 12-month period European companies had the next highest cost at $15.44 million". Incidents relating to credential theft are the most expensive incidents for companies with an average cost of $804,997 per incident[17].

There are several other important considerations for an efficient remediation:

- Identify information adding value to the company and evaluate the legitimacy of the staff who has access to it;
- Wipe the state clean and renew the way you award and control IT and physical access;
- Reconsider your data storing policy to keep them as safe as possible;
- Establish a follow-up to monitor the evolution of an organization's practices.

Insider threats will continue to grow in complexity as working methods evolve. With the standardization of remote working and the use of artificial intelligence, sensitive data is more likely to be leaked, increasing the types of possible malicious configurations.

The growing importance of data-related issues in Europe is forcing companies to take the insider threat seriously, by trying to prevent the irruption of an insider.

Now you are prepared to do the job: put tons of measures in place to push them aside and keep your workplace safe. When they say, "keep your friends close but your enemy closer", remember that an insider is your most intimate adversary and that the risk number one is human.

17 Ponemon Institute. 2022. Proofpoint. "2022 Cost of Insider Threats Global Report". "Inside Threat Actors: Dark Web Forums vs. Illicit Telegram Communities".

BIBLIOGRAPHY

Bleeping Computer. 2023. “Inside Threat Actors: Dark Web Forums vs. Illicit Telegram Communities”.

Cappelli, Dawn. Andrew, Moore. Randall, Trzeciak. 2012. “The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)”.

CEI. 2023. “The Consequences of Cyber Attacks and Their Impact on Cybersecurity”.

Charney, David L. 2010. National Insider Threat Special Group. “IV. Insights on the Profession”.

Chen, James. 2021. Investopedia. “What Is Market Value, and Why Does It Matter to Investors?”.

CNIL. 2015. “Le contrôle de l’utilisation d’Internet et de la messagerie électronique”.

Court of Cassation, Civil, Social Division, September 30, 2020, 19-12.058, Published in the bulletin.

Cuvakin, Anton. 2026. Gartner. “Our “Understanding Insider Threats” Paper Publishes”.

Ekran System.”Insider Threat Statistics for 2023: Facts, Reports & Costs”.

European Parliament. 2023. “EU AI Act: first regulation on artificial intelligence”.

Flynn, Lori. Clark, Jason. Moore, Andrew P. Collins, Matthew. Tsamitis, Eleni. Mundie, David. Mcintire, David. “Four Insider IT Sabotage Mitigation Patterns and an Initial Effectiveness Analysis”.

Gihon, Shmuel. 2022. Cyberint. “New Black Basta Ransomware Group”.

Groww. 2022.” Difference Between Market Value and Intrinsic Value Of Stocks”.

Hanley, Michael. Montelibano, Joji. 2011. “Insider Threat Control: Using Centralized Logging to Detect Data Exfiltration Near Insider Termination”: Fort Belvoir, VA: Defense Technical Information Center.

Huang, Keman. Xiaoqing, Wang. William Wei. Stuart, Madnick. 2023. Harvard Business Review.”The Devastating Business Impacts of a Cyber Breach”.

IBM. 2023. “Cost of a Data Breach Report 2023”.

BIBLIOGRAPHY

Miller, Sarah. 2016. Carnegie Mellon University. “The Frequency and Impact of Insider Collusion”.
Miller, Sarah. 2016. Carnegie Mellon University. “Insider Threat Deep Dive on IT Sabotage: Updated Statistics (Part 1 of 2)”.

Moore, Dark Reading Andrew P. Cappelli, Dawn M. Trzeciak, Randall F. 2008. “The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures”.

Moore, Andrew P. David, McIntire, Dave. Mundie. Zubrow, David. 2013. “Justification of a Pattern for Detecting Intellectual Property Theft by Departing Insiders”.

Ponemon Institute. Proofpoint. “2022 Cost of Insider Threats Global Report”.

Secrétariat général de la défense nationale. 2004. “La défense en profondeur appliquée aux systèmes d’information”.

Simpson, Jim. 2023. Dark Reading. “Hunting Insider Threats on the Dark Web”.

Tessian. 2022. “Insider Threats Examples: Types and Real-World Scenarios”.

Tessian. 2023. “Real Examples of Negligent Insider Risks”.

Thompson, Shawn. 2017. CSO online. “Reading between the Lines: The Real Impact of Insider Threat”.

Toulas, Bill. 2022. Bleeping Computer. “Ransomware gangs increase efforts to enlist insiders for attacks”.

Tunggal, Abi Tyas. 2023. UpGuard. “What Is an Insider Threat? Definition, Examples, and Mitigations”.

World Intellectual Property Organization. “Secrets d’affaires”.

Gasparian, Levon. 2022. “How To Prevent Accidental Data Exposure Within Your Company”.

Tunggal, Abi Tyas. 2023. Upguard. “What is a Data Leak? Stop Giving Cybercriminals Free Access”.

Girollet, Albane. Gredoire, Chloé. 2022. Almond. “Protection du patrimoine informationnel : regard sur le cyber-espionnage”.

FOR ALMOND

+400 collaborators

+59M€ turnover

+25% growth

+400 clients

WE HELP YOU STRENGTHEN ALL THE PILLARS OF YOUR CYBER SECURITY.

Understanding evolving threats, assessing risks and treatment options, convincing and obtaining funding, investing in human resources, processes and the right technologies to strengthen an organization's security, testing and auditing results, ensuring compliance to regulations while considering differences, raising awareness, preparing everyone for incidents which, despite all efforts, are bound to occur, responding to it in times of crisis, rebuild, analyze, start again...

The lives of the men and women who work in cyber security are certainly not easy, but it's a passion that the 400 Almond experts share to assist you with services, innovations and products that will contribute to your cyber security.

Whether you need to anticipate, protect, detect, react or rebuild, Almond can help!

I NEED ANTICIPATION

Identify risks, define rules, prepare your defense.

I NEED PROTECTION

Arm yourself for optimum security.

I NEED DETECTION

Detect incidents as early as possible.

I NEED REACTION

Don't stay alone, act quickly with our experts.

I NEED TO RECOVER

Opt for efficient reconstruction and optimal recovery of your operations.

MOVE
FORWARD
WE'LL
WATCH
YOUR
BACK

almond

PARIS_
STRASBOURG_
NANTES_
RENNES_
LYON_
GENEVA_

THANK YOU

contact@almond.eu
+33 1 46 48 26 00