Ind.Cyber.Sec Letters

Volume 02, Issue 03. 2025, November 10

Understanding Insider Threats

Prof. Dr. Luiz Fernando Freitas-Gutierres

linkedin.com/in/lffreitas-gutierres

github.com/substationworm

luiz.gutierres@ufsm.br

Introduction

An insider threat originates from current or former employees who, through privileged access, can directly interact with an organization's assets, networks, and/or data[1]. Consultants, partners, and third-party service providers may also represent potential insider threat vectors. Such threats may be intentional or unintentional[2], and not all insider activities are malicious. In some cases, incidents stem from untrained personnel or inadvertent errors that compromise the confidentiality, integrity, or availability (CIA) of an organization's information (IT) and operational technology (OT) systems.

In this context, the third issue of the 2025 volume of Ind.Cyber.Sec Letters examines insider threats through the findings of recent industry reports published by Arctic Wolf, Cybersecurity Insiders, and the Ponemon Institute. This issue also features two case studies: the first analyzes recent incidents in Brazil's financial sector, while the second focuses on OT systems, exploring the well-known Maroochy incident, widely recognized within the industrial cybersecurity community. Finally, the issue presents investigations conducted across the Deep and Dark Web using the StealthMole's platform, uncovering underground markets where cybercriminals actively seek to recruit insiders within organizations.

General Notes

The 2024 Insider Threat Report by Cybersecurity Insiders surveyed 413 IT and cybersecurity professionals and, alarmingly, revealed that only 17% of organizations reported no insider attacks in 2024. Among most organizations (32%), between one and five insider incidents were recorded. Likewise, The State of Cybersecurity: 2024 Trends Report, published by Arctic Wolf and based on a survey of 1,000 director-level professionals, found that 61% of organizations identified at least one insider threat in 2024. Of these, 29% resulted in a confirmed cybersecurity incident, while in 32% of cases, the threat was contained before escalating into a reportable event.

For 32% of respondents to the industry report by Cybersecurity Insiders, the estimated average cost of remediation following an insider attack ranged from USD 100,000 to 499,000. As highlighted in the report, ten incidents costing USD 1 million each (a cost range reported by 21% of respondents) could easily exceed USD 10 million in aggregate losses. Consequently, the financial impact can be severe and, unfortunately, reflects a broader trend across the industry.

The 2025 Cost of Insider Risks Global Report by the Ponemon Institute, sponsored by DTEX Systems, surveyed 8,306 IT and IT security practitioners and, notably, segmented its analysis by type of insider threat. Negligent or mistaken insiders accounted for the largest number of incidents—4,321 in total—with a per-incident cost of USD 676,517. Outsmarted insiders, those exploited through credential theft, phishing, or social engineering by an adversary, represented 1,552 incidents and exhibited the highest per-incident cost, reaching USD 779,797. Finally, malicious insiders were responsible for 1,995 incidents, with a per-incident cost of USD 715,366. In the case of the latter, their primary motivations typically include espionage, intellectual property (IP) theft, unauthorized disclosure, sabotage, fraud, or workplace violence. Additionally, 32% of respondents reported incidents involving collaboration between an insider and a

[1] Cybersecurity and Infrastructure Security Agency. (n.d.). *Defining Insider Threats*. Link

[2] The CERT® Insider Threat Team. (2013, August). *Unintentional Insider Threats: A Foundational Study*. Carnegie Mellon University. Link

Figure 1. First artwork for Issue 03, Volume 02 of the Ind.Cyber.Sec Letters.

malicious external actor.

The 2024 Insider Threat Report by Cybersecurity Insiders reveals that, from the respondents' perspective, 55% of insider incidents are considered as difficult to detect and prevent as external cyberattacks, while 37% regard them as even more challenging. The report further identifies the five primary factors cited by respondents as contributing to insider attacks:

a. Increasingly complex IT infrastructures, with a growing number of employees accessing organizational services and assets.

b. Adoption of emerging technologies such as the Internet of things (IoT) and artificial intelligence (AI).

c. Inadequate cybersecurity strategies and the absence of consistent governance policies.

d. Insufficient training and security awareness programs.

e. Weak enforcement mechanisms, including a lack of accountability for employees.

According to the 2024 Insider Threat Report by Cybersecurity Insiders, 11%, 25%, and 35% of respondents stated that their organizations are extremely, very, and moderately vulnerable, respectively. However, in sharp contrast to these perceptions, only 5% of respondents reported that their insider threat management programs were ineffective. The report suggests that the increasing sophistication of insider threats, combined with the growing complexity of hybrid work environments, may help explain this discrepancy.

In the context of OT environments and industrial control systems (ICS), insider threats are also present within industrial facilities. However, insider threats in OT-ICS extend beyond data or intellectual property theft; they can result in physical damage, process disruption, or even loss of human life. In some cases, such incidents require specialized technical knowledge of industrial

processes, which may still be safeguarded by safety instrumented systems (SIS). A system, however, can be compromised through insider knowledge or by bypassing defensive measures if the individual is aware of their placement or configuration[3]. Nevertheless, no one is better positioned to inflict physical harm on an industrial process than those who work directly with it. These individuals often possess not only the necessary expertise but also physical access to critical assets such as remote terminal units (RTU), supervisory control and data acquisition (SCADA) systems, or auxiliary devices. Additionally, OT-ICS systems face the vendor over-privilege risk, a category of supply chain attack that exploits trusted relationships. Such attacks may occur through unauthorized or shadow IT devices, compromised hardware or software, or routine updates containing hidden malicious payloads.

Whether in a corporate banking network or an industrial network within a steel plant, one should never assume that staff members are so loyal that they would never be influenced by ideology, shifting allegiances, or personal incentives that could turn them into insider threats[4]. Likewise, no employee behavior monitoring program can prevent an insider from acting under coercion or duress—for example, in situations where kidnapping or blackmail is used to compel an employee to perform specific actions. In this regard, insider threat mitigation strategies are essential but should not be regarded as entirely effective or foolproof.

Another important factor is overall employee satisfaction, as dissatisfied personnel are significantly more likely to become insider threats. Moreover, such individuals often exhibit a diminished willingness to collaborate proactively on security-related matters within the organization. Supporting this observation, an analysis of 30 insider IT sabotage cases across United States critical infrastructure sectors[5] revealed that 57% of insiders were disgruntled due to unmet expectations, including insufficient salary or bonuses, lack of promotion, and poor relationships with coworkers, among other reasons. Notably, 92% of the incidents occurred following a negative work-related event. In addition, 97% of these cases had previously drawn the attention of supervisors or colleagues for concerning behaviors—such as aggressive conduct, substance abuse, workplace conflicts, or poor job performance—prior to the attack. Technical precursors were also identified in 87% of insider IT sabotage cases, including the use of hacker tools, unauthorized access to customer or coworker systems, and failure to maintain backups. These findings reveal observable patterns that justify the mitigation strategies discussed in the next section.

Mitigation Strategies for Insider Threats

As reported in The State of Cybersecurity: 2024 Trends Report by Arctic Wolf, one of the most effective approaches to preventing insider attacks is the adoption of a security awareness program (SAP) that provides continuous training for employees and contractors. A security-oriented culture must be fostered—one in which every employee approaches security seriously and regards it as an essential part of their daily responsibilities. An effective security program encourages all personnel to understand that security is a shared responsibility, not solely the duty of dedicated security teams.

[3] Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A.-M. (2018). *Insider Threat Detection Study*. NATO Cooperative Cyber Defence Centre of Excellence. Link

[4] Bunn, M., & Sagan, S. D. (2014). *A Worst Practices Guide to Insider Threat: Lessons from Past Mistakes*. American Academy of Arts and Sciences. Link

[5] Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008, May). *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastrutuctures*. Carnegie Mellon University. Link

The 2025 Cost of Insider Risks Global Report by the Ponemon Institute indicates that 81% of organizations either have implemented or plan to implement an insider risk management program (IRMP). The majority of companies surveyed by the Ponemon Institute stated that this proactive strategy shortened incident response times, preserved brand reputation, and reduced financial losses associated with data breaches. While a SAP aims to reduce risk through training and educational campaigns—seeking to lower the likelihood that an employee becomes an insider threat—an IRMP focuses on detecting, monitoring, and responding to internal risk behaviors. The latter integrates technological capabilities, governance and compliance frameworks, and behavioral analytics to identify and mitigate insider threats. Thus, an SAP often serves as a foundational component within an IRMP.

Other security measures recommended by major players in the industrial cybersecurity sector, such as Dragos and Nozomi Networks, to mitigate insider threats include:

- Enhancing visibility and accountability by tracking, monitoring, logging, and recording user interactions with the organization's critical assets. Greater visibility enables the identification of anomalies, such as accounts logging in outside normal working hours, employees badging into restricted areas, or attempts to install unauthorized software.
- Implement access control solutions that enforce role-based, the principle of least privilege and ensure prompt revocation of access for former employees and contractors following termination.

On the other hand, it is worth noting that, according to the 2024 Insider Threat Report by Cybersecurity Insiders, the two primary obstacles identified by IT and cybersecurity professionals in implementing insider threat management programs are technical challenges and high costs. Regarding the latter, it is essential that organizations view these expenditures as strategic investments aimed at strengthening their security posture and advancing their cyber maturity. This perspective aligns with findings from IBM's 2023 Cost of a Data Breach Report, which emphasize that preventive measures are typically more effective and cost-efficient than reactive responses.

Finally, executives and security teams should not assume that established rules and procedures are being universally or strictly followed. At times, competing organizational priorities may lead supervisors to instruct their teams to bend security policies to meet operational goals. Similarly, employees may fail to fully comply with security guidelines for various reasons, among them the belief that doing so could enhance productivity or reduce inconvenience.

Case Studies

Recent Incidents in the Brazilian Financial Sector

On June 30, 2025, C&M Software—a technology company providing connectivity and integration solutions that enable financial institutions to interface with the Central Bank of Brazil's systems—was the target of a cyber incident[6]. The attack resulted in unauthorized access to reserve accounts (unrelated to end-customer accounts) belonging to at least six financial institutions and led to the diversion of more than BRL 800 million. The incident is regarded as the largest cyberattack ever recorded against Brazil's financial sector.

[6] g1. (2025, July 06). *Depoimento de suspeito preso por ataque hacker detalha esquema que desviou mais de R$ 540 milhões* [Video]. YouTube. Link

Figure 2. Second artwork for Issue 03, Volume 02 of the Ind.Cyber.Sec Letters.

The breach was primarily facilitated by an insider, an employee who initially sold his access credentials and was later bribed to execute malicious code within the organization's systems in exchange for BRL 15,000. The insider was a junior programmer who had been employed at C&M Software for three years.

In cooperation with law enforcement authorities, the company reviewed internal surveillance footage to analyze employee behavior, leading to the arrest of the insider. As of the latest reports, twelve individuals have been arrested in Brazil and seven others abroad, with assistance from Interpol[7].

Another recent case involved the seizure of a cell phone and laptop belonging to a Banco do Brasil employee who allegedly demanded BRL 1 million to facilitate a cyber intrusion into the bank's systems by selling his access credentials to cybercriminals[8]. According to the limited information disclosed, Banco do Brasil detected and thwarted the attempt through internal monitoring systems and promptly alerted law enforcement authorities.

The Maroochy Incident

This incident occurred in the former Maroochy Shire, Australia, between February and April 2000 and involved a malicious insider (C0020). The individual disrupted the operation of the community's sewage control systems, resulting in the discharge of more than 800,000 liters of raw sewage into parks, rivers, and residential areas. Reports cited environmental consequences, particularly affecting the region's marine life. Witnesses described a darkened creek and an

[7] g1 Paraíba. (2025, October 31). *Suspeito de participar do maior ataque hacker do país que desviou R$ 800 milhões é preso em Campina Grande*. Globo Notícias. Link

[8] Rodrigues, M. *Funcionário do Banco do Brasil cobra R$ 1 milhão para permitir invasão a sistema*. g1 Distrito Federal, Globo Notícias. Link

strong stench that became unbearable for nearby residents[9].

The individual, then approximately 40 years old, had previously worked for a company responsible for installing SCADA systems within the wastewater infrastructure managed by the shire council. After leaving the company—and reportedly following a strained professional relationship—he applied for a position with the council. His application, however, was rejected, which apparently served as the trigger for the subsequent acts of sabotage against the local sewage systems.

The sewage collection SCADA network managed by the shire encompassed 142 pumping stations, supervised by two operator workstations and operating across three distinct radio frequencies[10]. Each station was equipped with a RTU that could be remotely controlled from the central facility (for example, to start or stop pump motors) and was also responsible for transmitting data, messages, and alarms. Communication between the pumping stations, as well as between the stations and the control center, was carried out through a private, dedicated bidirectional radio network supported by repeater stations.

The individual had previously worked with SCADA systems and IT services for the shire, serving as an employee of the company responsible for their implementation. He can be characterized as an insider, as he possessed specialized and prior knowledge of the shire's systems and of the equipment required to carry out the sabotage. It is also likely that he personally contributed to the installation and configuration of devices within the shire's wastewater network.

The shire's sewage system began to experience a series of malfunctions: pump assemblies failed to operate as expected, alarms were not being reported to the control center, and unauthorized modifications were identified in the configuration of equipment and in the control logic of the pumping stations. Even after a complete software reinstallation and system verification, configurations continued to change unexpectedly. Multiple anomalous events were recorded before the incidents were finally recognized as intentional acts. At that point, engineers and specialists concluded that the root cause of the problems was linked to an individual with remote access to the systems.

In one of the sabotage attempts, alarms were disabled at four sewage pumping stations. At that time, the individual was already under suspicion and surveillance. Law enforcement officers located his vehicle, which contained specialized equipment and an antenna—both stolen from his former employer—as well as a laptop equipped with software capable of communicating with the shire's sewage control systems. The antenna was configured to operate on the same frequency used by two of the three repeater stations in the region. The insider used the laptop to emulate a false pumping station (a "bogus station"), from which he transmitted deceptive data and commands to the control system[11].

The malicious actor was sentenced to two years in prison and fined AUD 13,110.77 for the damages caused[12]. The analysis of this incident underscores how challenging it can be to defend against insider attacks, as well as the need to implement robust security and authentication

[9] Abrams, M., & Weiss, J. (2008, July 23). *Malicious Control System Cyber Security Attack Case Study: Maroochy Water Services, Australia*. Link

[10] Sayfayn, N., & Madnick, S. (2017, May). *Cybersafety Analysis of the Maroochy Shire Sewage Spill*. Cybersecurity Interdisciplinary Systems Laboratory, Massachusetts Institute of Technology. Link

[11] Supreme Court of Queensland. (2002). *R v Boden [2002] QCA 164*. Link

[12] Mustard, S. (2005, December). Security of Distributed Control Systems: The Concern Increases. *Computing and Control Engineering*, 16(6). Link

mechanisms in SCADA systems and to maintain detailed logging records of access and historical commands. Finally, the case highlights the importance of well-defined service contracts that clearly establish the responsibilities of third-party providers, along with the training of personnel and the implementation of personnel security controls.

Investigations Using the StealthMole's Platform

Assessments were conducted across the Deep and Dark Web to identify instances of insider threat recruitment activity and potential individuals offering non-public intelligence about organizations. Using the Dark Web tracker (DT) and Telegram tracker (TT) tools from the StealthMole's platform, multiple cases were identified in which suspected malicious actors sought to recruit insiders within companies across various sectors, most notably in telecommunications and e-commerce. Table 1 summarizes findings obtained through the TT. The following are selected observations about the identified cases:

- Evidence was found of insider recruitment for the exfiltration of account data and manipulation of official records.
- Instances of insider trading were also identified, involving the use of confidential and non-public information to gain financial advantage in market operations. These included the sale of proprietary corporate data, such as financial results prior to disclosure, merger and acquisition plans, investment tips, and other leaked information related to private companies.
- Additional findings included offers to recruit insiders within mobile network operators, frequently to enable subscriber identity module (SIM)-swap attacks, in which a victim's phone number is transferred to a SIM card controlled by the attacker. This allows the threat actor to receive the victim's text messages, phone calls, and two-factor authentication (2FA) codes.
- In most cases, the identified activity involved online personas seeking insiders. However, there were also instances of alleged privileged employees offering to carry out malicious actions against their own organizations.
- The items above represent the majority of the observed cases. It is also noteworthy that some instances involved attempts to recruit insiders within critical infrastructure organizations and entities typically operating OT-ICS systems.
- In many insider recruitment messages, large financial rewards were promised, and alternative communication channels, such as qTox, Session, and Signal, were often suggested to continue negotiations more securely.

Figure 1 compiles screenshots of several such occurrences observed during the investigations conducted on the Deep and Dark Web. However, it should be noted that the veracity of these messages and offers has not been assessed, and each case was not extensively investigated. The purpose of these findings and screenshots is to demonstrate the existence of active insider recruitment efforts on underground forums and Telegram channels.

Conclusions

The third issue of the 2025 volume of Ind.Cyber.Sec Letters examined insider threats, presenting general notes and observations derived from recent industry reports published by Arctic Wolf, Cybersecurity Insiders, and the Ponemon Institute. The issue also explored case studies at both corporate and OT-ICS levels, highlighting their nuances and emphasizing the inherent complexity

Channel ID	User ID	Date	Message Excerpt
1199******	400******	2025-11-04	SEARCHING FOR MICROSOFT INSIDER! Need Xbox/Microsoft account lookup by its Gamer Tag, Email, or XUID. (...) lookups can be done by low level support agents or software engineer
1980******	7784******	2025-03-24	*I Need Amazon insider service , Need lower referral fee please PM me (...) I can also reward you $ 200for this connection (...)*
1778******	6133******	2025-01-10	*I need an insider at the SAAQ . DM me please*
1898******	5042******	2025-01-08	*i need a insider at Orange moblie or SFR (...) or any french moblie carrier insider. Pm. paying 5 figs*
1402******	7305******	2024-11-20	*I Need Amazon insider, payment in upfront obv, text me*
1774******	7166******	2024-07-08	*I need IRS insider. I've over 400 names I need their paystubs so I can hit their retirement funds, average is 20k, 50/50 split with the insider (...)*
1880******	5126******	2024-05-06	*I need Rogers insider for SIM activation. No sim swap. Many work. Paying really well (...)*

Table 1. Examples of insider recruitment messages identified on Telegram.

of identifying such threats and implementing effective mitigation strategies.

Finally, investigations were conducted across the Deep and Dark Web using the StealthMole's platform, which revealed digital recruitment efforts targeting insiders within organizations—and, in some cases, alleged privileged employees offering to take malicious actions against their own companies. In this context, it is important to underscore the potential application of open-source intelligence (OSINT) and cyber threat intelligence (CTI) techniques to proactively monitor emerging threats within Deep and Dark Web environments.

Acknowledgments

The author thanks the entire StealthMole team for their support and for granting access to the platform's trackers.

by [redacted] • 4 months ago

Insider and affiliate opportunity, make more money than your boss! (Full list of criterias below)

Hey there everyone!

Real business opportunity here for anyone who fits the criterias or has contacts who do. Anyone providing contacts for us also gets rewarded also.

Why here/ why us:
- Our motive is to gather more customers so that we can can get to higher levels in our business area
- Experience and solid software are behind our work opportunity
- High payouts in this industry, these are to be discussed in private

We are looking for you if youre any of these:
/ Corporate insiders (IT/Admin/Helpdesk) willing to monetize their access
/ Access brokers with valid RDP/VPN/Domain access to mid-large orgs
/ Social engineers skilled at initial intrusion, phishing, or physical infiltration
/ Employees with USB access or local privileges (AD-connected machines are a priority)
/ POA (Proof of access) needed, with OPSEC considerations for your safety

by [redacted] • 3 weeks ago*

[JOB - XMR] Be an insider or find them, industry leading payment guranateed. Professional team looking for partners. *Full proof of previous operations and demo ready!* JOB

Hey!

Im here on this platform once again with a new opportunity. I will spare the technical details but for anyone interested im happy to provide it.
Before commenting or downvoting please take a look at my profile where i clear some things up. Thank you!

Who are we looking for?
-As stated in the title of the post, im looking for anyone whos an employee and has been for a long time at a legit company/firm with privilages in their network.
So local or domain admin access is obviously a big bonus, that shows greatly in the payment at the end, but im ready to hear any offer and opportunity thats presented.
Windows/Linux/Esxi systems and servers included.

by [redacted] • 4 months ago

[JOB] Insider Access – Need Skilled Operator for Ransom Job 💻💰

I'm an internal employee at a large-sized company in the Caribbean, approx. 1,500 staff. I have unrestricted access to internal HR systems, payroll files, and employee records. No real security team on-site and barely any monitoring.

I want to partner with someone experienced in ransomware deployment. I will provide access. You handle the technical side. We split the ransom 50/50.

Not looking to destroy anything, just lock it down until they pay. Maybe lock entire payroll systems or something they can't operate without idk but you get the idea.

Serious operators only. No newbies or drama. DM with proof of work.

XMR only so we arent traced. Timing - ASAP

Commented on: [redacted] • 3 months ago in [redacted]

...i have an ***insider*** who will infect and my ransomware will do the job and the company has ton of files of clients i gotta steal the files and store them...

by [redacted] • 2 weeks ago

NEED AT&T INSIDER FOR SIMSWAP [BTC, XMR, ETH] JOB

by [redacted] • 5 months ago

[Job - XMR] Insider info on Oil and Gas companies

Databases, internal emails, address books, strategic plans. BP, Exxon, Shell, Aramco etc.

Figure 3. Examples of online posts promoting insider recruitment on underground forums.

Ind.Cyber.Sec Letters

Volume 02, Issue 03. 2025, November 10

Understanding Insider Threats

Luiz F. Freitas-Gutierres (a.k.a. substationworm) is a professor in the Department of Electromechanics and Power Systems at the Federal University of Santa Maria. His primary research interests include: industrial cybersecurity, cyber threat intelligence, and the automation of electric power systems.

Ind.Cyber.Sec Letters is a collection of studies and analyses of incidents in the field of industrial cybersecurity.

Prof. Dr. Luiz Fernando Freitas-Gutierres

linkedin.com/in/lffreitas-gutierres

github.com/substationworm

luiz.gutierres@ufsm.br