SEPTEMBER 2022

# The Current Cyber Threat Situation in Sweden

## Example of the month: Swedish industry

Radar. | TRUESEC

**Current Threat Level – Threatcon**

Level 2: Moderate threat level.
Scattered attacks with passing effects.

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| min | | | | max |

# To the Person Reading This

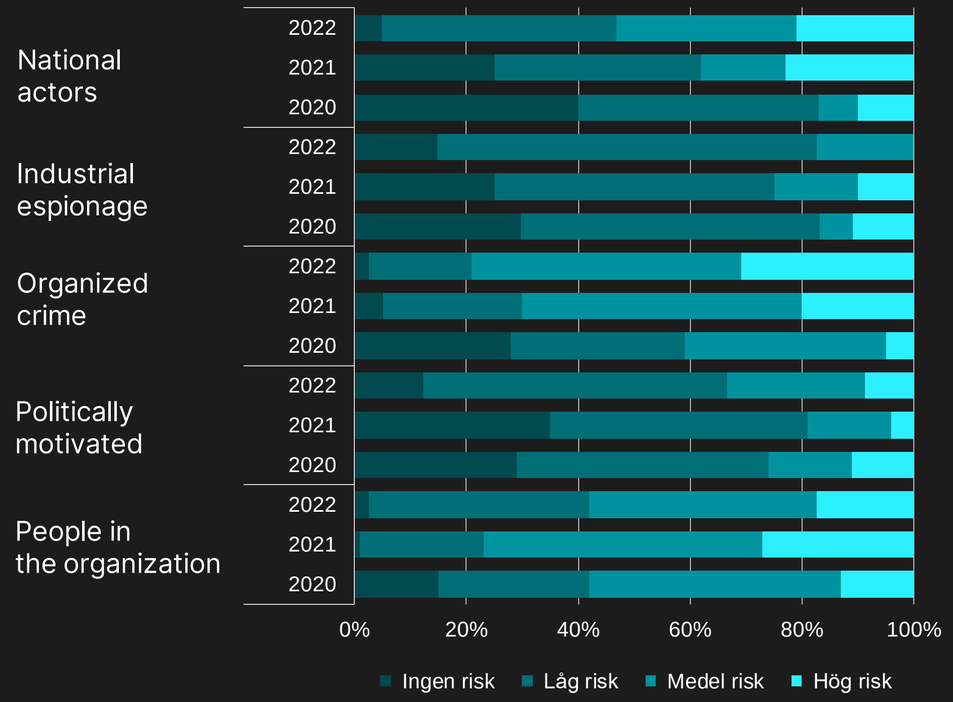
Cyber threats against Sweden and Swedish organizations are constantly changing. In a unique collaboration between Radar and Truesec, we want to give people who operate in Sweden the best possible conditions to be data-driven in their work regarding risks related to cyber threats so that they can prevent hacking.

Radar has large amounts of data and insights related to priorities and IT budgets. Truesec is a cybersecurity company that has a deep and broad insight into the current threat landscape through its operations with a leading incident management team and Security Operations Center. Together, we choose to present data and insights in recurrent reports, every time with a deep dive into a specific industry. This time, we're diving into the Swedish industry.

Radar and Truesec are launching the tool ThreatCon together to measure the level of cyber threats over time. ThreatCon indicates the current threat level for IT attacks aimed at Sweden based on actual attacks in relation to the ability to protect the target. New assessments are done regularly and presented on a scale between 1 (calm), 2 (normal), and all the way up to 5 (max).

We hope the report is helpful to you as a reader and look forward to developing the content together to give Sweden access to a data-driven snapshot of the current cyber threat situation that is also easy to understand.

Perceived threats year over year, Sweden. The result is based on Swedish organizations' responses to the question "Assess the current threat situation from the following actors".




Source/data: Radar.

# Perceived Threat Situation

Swedish organizations are generally experiencing an increased threat situation in almost all categories, except for threats from industrial espionage and their own employees, which both take a step back regarding high and medium-high risk. It's hard to point out a specific factor that can explain the changing trend and the variations in threat assessments. However, the reporting of incidents, vulnerabilities, and geopolitical insecurities in media have, of course, had a considerable impact on what's considered a threat. Our responders' answers align with the report about cybersecurity in Sweden.

The manufacturing industry, our focus industry this month, experiences a similar threat situation, with the major exception being that industrial espionage is perceived as a much greater risk. Additionally, threats from other national actors are also seen as a greater risk in this industry than in other Swedish industries.

We can connect the concern of both types of threat actors with the perceived risk, or even the business risk, of losing confidential business information and IP (intellectual property) along with the perceived probability that one's organization has become a target.

# The Current Situation – Attacks

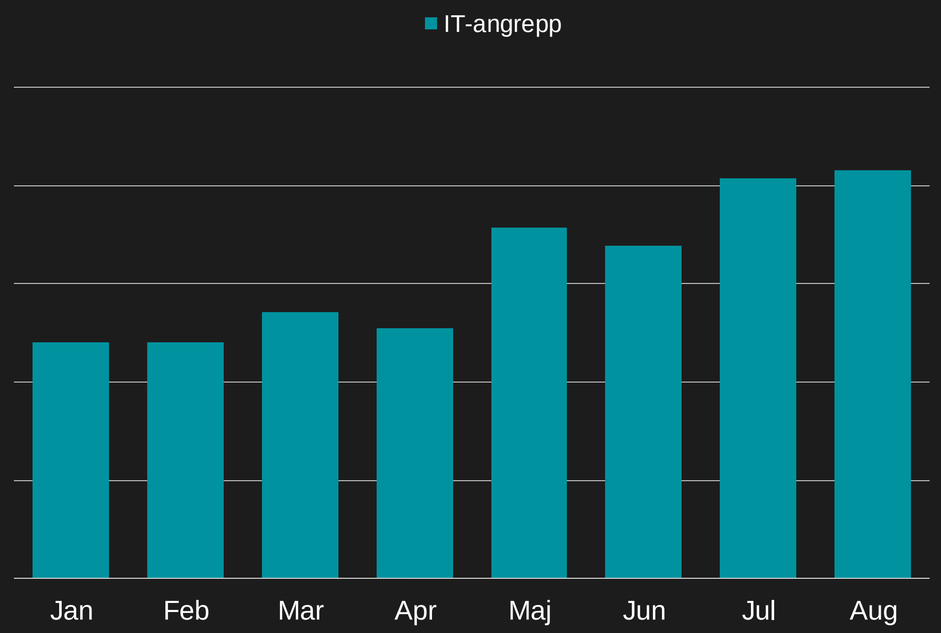
Truesec observed a 2 percent increase in IT attacks against Swedish companies in August compared to July. It might be a moderate increase, but when put into context, it means a continuation of the trend of IT attacks increasing that began in May.

After a winter and early spring with fewer IT attacks than usual, it all took a drastic turn in May, with IT attacks increasing by 40%. Since then, Truesec has seen a significant increase in IT attacks against Swedish companies. Since April, the attacks have increased by 63% and affect a wide range of industries.

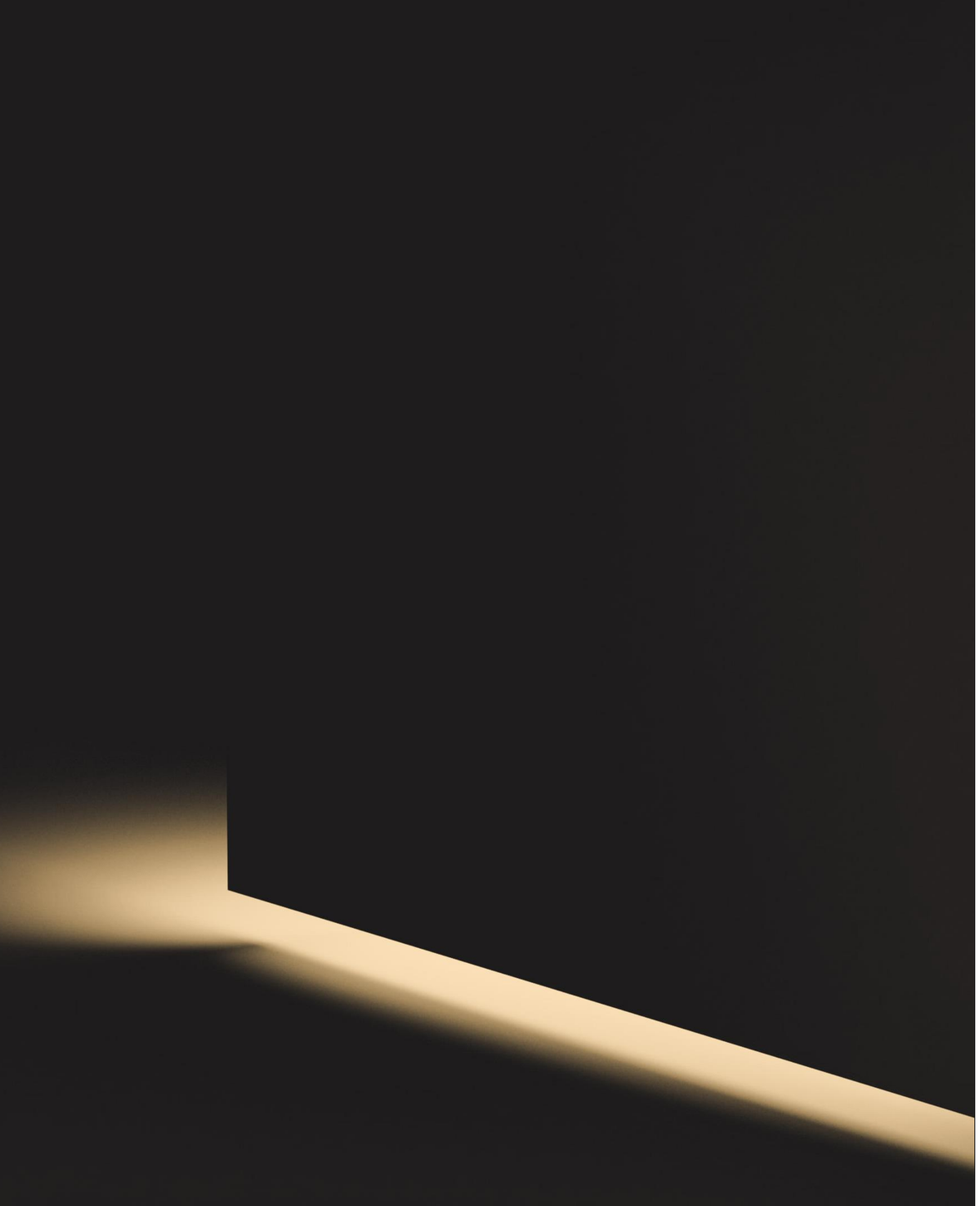
The information is based on enriched data from analysts having done an individual assessment of each case and concluded that the IT attacks, had they not been stopped, could have led to serious consequences for the affected company. Check out this month's example to learn how these types of incidents can develop if they're not detected and disarmed quickly.

Based on the presented and underlying data on the current threat situation and the world around us, Truesec chooses to, together with Radar, declare that the current threat level is a level 2 out of 5. This means that we're currently at a moderate threat level where attacks, for the most part, aren't concentrated but spread out. The effects of the attacks are also mostly passing.

IT attacks, Sweden. Development over time 2022.




Source/data: Truesec.



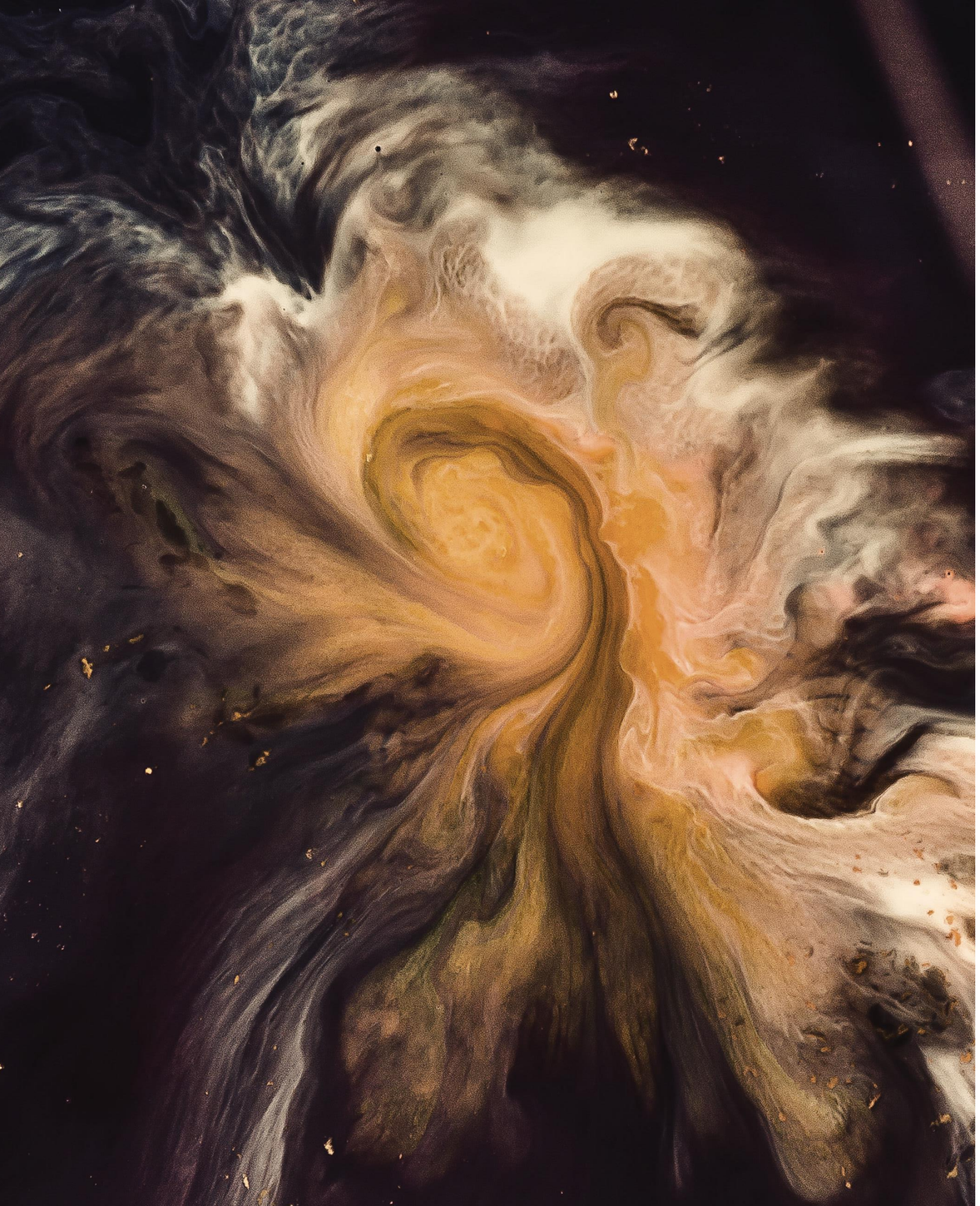


# A lack of updates led to an extortion attack

In the spring of 2022, Truesec received a mission to manage a severe ransomware attack on a Scandinavian company. It turned out that the attack had happened in two steps. In the first step of the attack, which occurred in the winter, a threat actor used a known weakness in Microsoft Exchange to gain access to the network. Despite this weakness being published and publicly available for months, the company never installed the security update.

When this threat actor got access to the network, they installed a so-called crypto miner – a harmful code that steals computer power to produce cryptocurrency. This threat actor was most likely first and foremost interested in selling access to the network to other cybercriminals. The harmful code was probably a way to make a little extra money while they were waiting for buyers.

Source/data: Truesec.



**CASE OF THE MONTH: SWEDISH INDUSTRY**

A lot seems to point to that there was a transaction on the DarkWeb after about two months, where the threat actor that first got ahold of the company's network sold the access to another threat actor. The new threat actor went into the system, closed down the crypto mine and started to take control of the entire network and encrypt all of its information. The company was now under a full-blown ransomware attack, and the threat actor tried to make the company pay them in cryptocurrency to get back its encrypted information.

This proves that broad mass attacks where the vulnerabilities in software are used to gain a foothold in many vulnerable systems can lead to severe attacks months after the imposter first gains access to the system. It also proves that all harmful code active in a network is serious, even if the code that's been activated doesn't have the capacity to do significant damage, since the threat actor can make lots of money by selling the access to other criminals who have intents with much more severe consequences.

Source/data: Truesec.

# The Primary Focus and It Budgets

The industry generally reacts quicker than the national average to changes in the national economic situation, and it has once again started shifting its focus to cost reduction. It's also worth mentioning that the industry, to a greater extent, has tended to have a more cautious optimizing strategy, apart from in 2020, when they invested in innovation to a greater extent than the national average.

Historically, focusing on innovation has often meant security has had a lower priority. However, our priorities have led to the different areas of investment changing over time, which has resulted in differences in specific investment areas between our industry and the national average.

The industry increased its security investments dramatically in 2021, and digitalization has returned to the same levels as in 2020. It's also interesting to note that IoT is an area that keeps growing as information classification takes a step back. This hints that a lot of people already know what information is going to go through the nodes – or that this is an area that will face considerable challenges later on. Both groups are increasing their outsourcing, which can also come with future challenges if you don't know how the information will be exposed to risks in long and complex chains.

Specific investment areas. The number indicates the number of organizations that plan to invest in each specific area, stated in percent.

| | Industri | | | | Sverige | | |
|---|---|---|---|---|---|---|---|
| | 2020 | 2021 | 2022 | | 2020 | 2021 | 2022 |
| Införande av AI och kognitiva lösningar | 8 | 0 | 9 | | 21 | 14 | 11 |
| Införande av blockchainbaserade lösningar | 4 | 0 | 0 | | 1 | 0 | 2 |
| Digitalisering av verksamhetens processer | 69 | 78 | 68 | | 60 | 42 | 61 |
| Införande av igenkänningsteknik | 8 | 0 | 0 | | 4 | 2 | 4 |
| Säkerhet (cyber- och informationssäkerhet) | 46 | 67 | 64 | | 48 | 38 | 74 |
| Internet of things (IoT) och sensorteknik | 15 | 22 | 27 | | 12 | 13 | 21 |
| IT-upphandling och avtalsrevisioner | 27 | 0 | 14 | | 23 | 16 | 25 |
| Leverantörsutvärderingar och prisjämförelser | 15 | 0 | 18 | | 12 | 7 | 11 |
| Kompetensförsörjningsstrategi | 8 | 11 | 14 | | 13 | 10 | 21 |
| Omvärldsanalys och bevakning | 19 | 0 | 9 | | 16 | 7 | 14 |
| Informationsklassificering | 23 | 22 | 9 | | 27 | 21 | 32 |
| Insourcing eller "hemtagande" av IT-leverans | 8 | 0 | 14 | | 6 | 5 | 11 |
| Utflyttande av IT-leverans till extern leverantör | 12 | 33 | 32 | | 13 | 8 | 26 |

Source/data: Radar.

Swedish organizations' priorities. The number states the priority (where 1 is the highest priority) for each specific area in Swedish organizations.

| | Industri (Sverige) | | | |
|---|---|---|---|---|
| | 2019 | 2020 | 2021 | 2022 |
| Säkerhet (strategi & efterlevnad) | 5 (4) | 7 (5) | 1 (2) | 1 (1) |
| Automatisering (nyckelprocesser) | 1 (2) | - (-) | 1 (1) | 2 (2) |
| Säkerhet (utbildning & medvetenhet) | - (-) | 11 (10) | 6 (7) | 3 (3) |
| Applikationer (förvaltning av befintliga) | 8 (8) | 2 (4) | 13 (6) | 4 (4) |
| Applikationer (införande av nya) | - (-) | 5 (3) | 2 (5) | 5 (6) |
| Infrastruktur (förvaltning av befintlig) | 6 (7) | 6 (13) | 7 (9) | 6 (8) |
| Säkerhet (teknik) | 10 (14) | 10 (12) | 12 (11) | 7 (7) |
| Ökad digitaliseringsgrad | 3 (3) | 1 (1) | 3 (4) | 8 (10) |
| Digitalisering (förändra verksamhets- & affärsmodeller) | 7 (5) | - (-) | 8 (3) | 9 (5) |
| Styrning (IT-organisation) | 11 (9) | 3 (6) | 13 (10) | 10 (9) |

Source/data: Radar.

# Priorities and Challenges

Priorities and challenges change every year, but we have always emphasized change. During the first year of the pandemic (2020), cost reduction climbed to the top ten list of most prioritized focus areas, accompanied by new applications, digitalization, and automation. Security, which has always been seen as a rather prioritized area and a challenge in Swedish organizations, got a lower priority in 2020. In 2021, the priorities returned to a similar situation as before the pandemic, with the focus moving to digitalization and automation, as well as security.

As one of the most digitalized countries in the EU, Sweden has historically prioritized innovation and transformation over security. In 2022, security became the highest priority for most Swedish organizations for the first time ever, even higher prioritized than digitalization and automation. Thankfully, the compromize between security and innovation is a lot less prominent today since the question is gaining more and more attention from company boards – probably primarily due to more attacks being reported by the media, but also thanks to urgings and requirements from authorities.

Just like the national average, the industry's priorities have been very similar regarding automation and digitalization, but the difference is that security became the highest priority in 2021, even beating automation. Similarly to the national average, the area moved down during the first year of the pandemic (2020), which might have resulted in a loss that now needs to be made up for.

Swedish organizations' challenges. The number states the level of challenge (1 being the biggest challenge) for each specific area in Swedish organizations.

| | Industri (Sverige) | | | |
|---|---|---|---|---|
| | 2019 | 2020 | 2021 | 2022 |
| Säkerhet (strategi & efterlevnad) | 4 (4) | 4 (3) | 3 (1) | 1 (1) |
| Säkerhet (teknik) | 9 (12) | 13 (14) | 5 (5) | 2 (5) |
| Säkerhet (utbildning & efterlevnad) | - (-) | 5 (6) | 1 (3) | 3 (3) |
| Kompetensförsörjning | 6 (2) | 3 (2) | 15 (4) | 4 (4) |
| Digitalisering (förändra verksamhets- & affärsmodeller) | 8 (5) | - (-) | 6 (2) | 5 (2) |
| Digitalisering (förstå & hantera digital affärsrisk) | - (-) | - (-) | - (-) | 6 (7) |
| Öka digitaliseringsgrad | 1 (1) | 1 (1) | 7 (9) | 7 (9) |
| Applikationer (införande av nya) | - (-) | 8 (4) | 12 (6) | 8 (6) |
| Automatisering (nyckelprocesser) | 2 (3) | - (-) | 4 (11) | 9 (11) |
| Stärka verksamhetens konkurrenskraft | 7 (8) | 2 (8) | 14 (17) | 10 (14) |

Source/data: Radar.

# Priorities and Challenges

When looking at challenges, we can see that security has been a top 5 priority even before the pandemic, accompanied by digitalization and competence provision. Technical security has also made the top-5 list of challenges these past two years. This implies that the development surrounding digitalization and its possibilities is now starting to create serious predicaments regarding how to protect oneself.

The industry's challenges are similar to the national average, the difference being that all security categories (strategy, technology, education, and awareness) are in the top 3, while digitalization and competence provision follow shortly after. Considering that the industry has started to outsource to a much larger extent than previously while also investing in IoT (or IIoT as it's called in the industry), it has become rather clear that technical security will become a much more significant challenge in the future.

While on the subject of priorities and challenges, it's interesting to note that competence provision, which is seen as a big challenge, still isn't a priority. Insufficient and/or having the wrong priorities is still an issue many companies struggle with. The constantly growing extent of cybersecurity activities, such as vulnerability management, surveillance, awareness training, etc., lead to a lot of organizations falling behind on their goals before they've even begun. One explanation for the insufficient efforts is the skills shortage since two-thirds of Swedish decisions makers state that there's a lack of security competence. And the lack of security competence has been seen as a bigger problem in the IT industry field compared to Sweden as a whole, as they've seen a more significant skills shortage than the national average since 2020.

# TRUESEC

Truesec is a leading cybersecurity company with a clear purpose: to prevent data breaches and protect data. The team consists of more than 250 employees with a wide variety of cybersecurity expertise. Ever since they started in 2005, they have delivered security solutions to clients in the private and public sectors, both in Sweden and internationally.

The ability to surveil, detect, and respond to attacks are all important cornerstones in modern cyber defence. Read more about Managed Detection and Response.

– ”The most important thing to start with is investing in your ability to detect data breaches, and then quickly being able to take action so that it doesn’t lead to any severe damage,” says Marcus Murray.

Marcus Murray
marcus.murray@truesec.se
+46 (0)70 918 30 01

For more information: truesec.com

# Radar.

Radar is a small but strong team of analysts and advisors that, thanks to their extensive expertise and excellence, is the natural choice for local, independent, data-driven insights for all of actors in the IT ecosystem.

At Radar, we want to help Swedish companies become winners of the world development. Strong companies lead to a stronger society and a stronger Sweden. Cybersecurity consitutes a great challenge and a real business risk and is about so much more than just technology.

– ”Security work is important and Swedish information that’s easy to understand and interpret has been missing. This is the next step in helping IT Sweden understand how the threat situation is developing, openly and with no secrets – that way, everyone wins.

Hans Werner
hans.werner@radargrp.com
+46 (0)73 539 15 51

For more information: radargrp.com