NOVEMBER 2022

The Current Threat Situation in Sweden

Sector of the month: Public Sector

Current Threat Level – Threatcon

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

1	2	3	4	5
min				max

Radar. | TRUESEC

Subscribe to the monthly report: Truesec.com/monthlyreport

NOVEMBER 2022

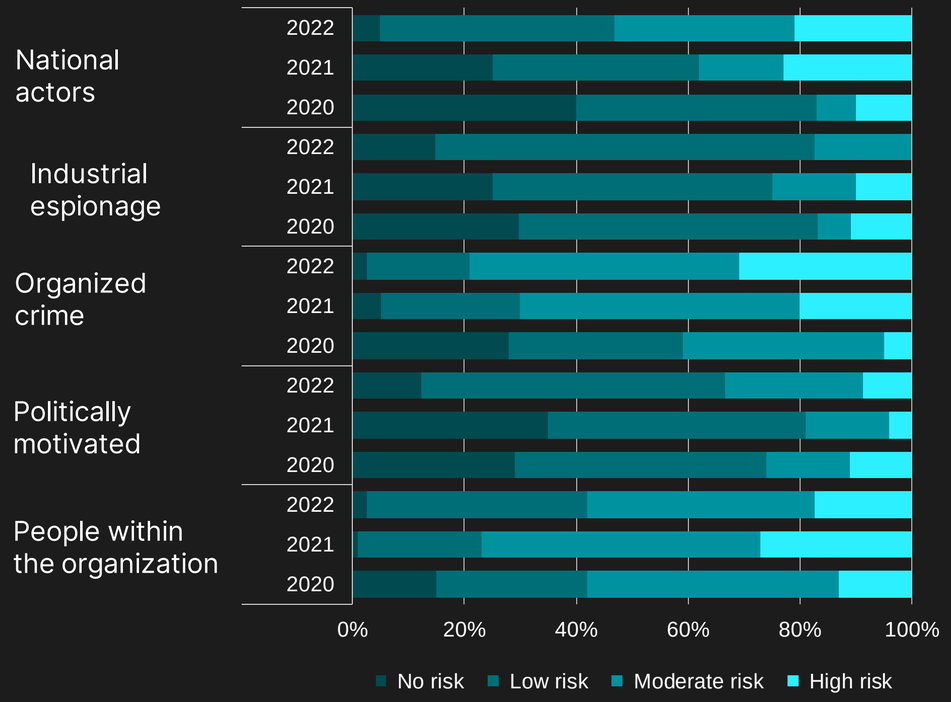
To the person reading this

We are approaching the winter season, a period when it isn't uncommon to see a rise in cyberattacks. Employees, whose responsibilities normally center around ongoing IT security and preventative measures, take off for the holidays – but just because they take off doesn't mean cybercriminals do too. Vulnerabilities are discovered and published all year round. The winter season is an opportune time for cybercriminals to strike since it gives them more time to carry out IT attacks before those attacks can be discovered.

Throughout the year, Truesec has observed how different threat groups have split apart, merged, reorganized and restructured. At the start of the year, attacks were largely motivated by cybercriminals' stance regarding the invasion of Ukraine; however, more recently, attacks have been influenced by leaks and defections on the part of threat actors. Moving forward, conditions appear to favor cybercriminals, which means cybercrime will continue to be a threat for the foreseeable future. Make sure your organization's security measures are adapted to your specific threat situation.

Stopping attacks early significantly reduces both the cost and consequences associated with the attack. It is also important to learn from the attacks that do happen and to continually improve your organization's IT security to ensure it only gets more effective at preventing attacks. Use correct and relevant information – there is good information available. By doing that, we can make the cost of carrying out IT attacks increase in relation to the cost of protection.

Perceived threats year over year, Sweden. Result based on Swedish organizations' response to the question "Assess the current threat level of each of the following actors".



Source/data: Radar.

Perceived Threat Situation

Overall, Swedish organizations perceive there to be an increased threat risk in nearly all categories, except in the categories of industrial espionage and employees within the organization, both of which decreased somewhat when it came to the high and moderate risk levels. It is difficult to identify one single factor that explains the fluctuating trend and reasons behind the variations in organizations' threat assessments. However, the reporting of incidents, vulnerabilities and geopolitical uncertainty in the media naturally plays a significant role in what is perceived as a threat. Our responders' answers are in line with the report on cybersecurity in Sweden.

It is notable that, within the public sector, the threat of organized crime is not at all perceived in the same way, namely that it poses an overall lower risk. The reverse applies to the perceived threat situation linked to politically motivated actors and employees within the organization. The former may seem obvious given the fact that we are much closer to "the Swedish state" within the public sector, but it is still worth highlighting this type of motivation and driver.

However, what is very noticeable is the perceived threat and risk stemming from inside the organization and our own employees.

The Current Situation – Attacks

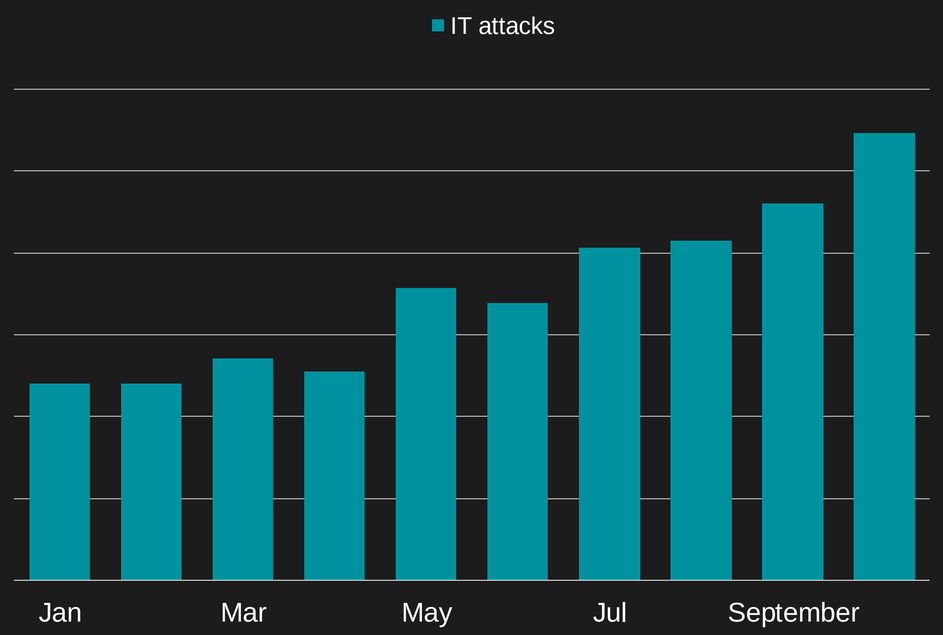
Throughout October, the number of IT attacks that Truesec prevents continued to rise in line with the trend from previous months. Month-on-month, IT attacks increased by 19%.

If we look at previous years, late fall and winter are both periods when attacks intensify. However, 2022 is different from previous years in that, this year, we have seen a nearly uninterrupted rise in the number of cyberattacks since the early summer, which is different from the fluctuating peaks and valleys that we have seen over the fall months in years past.

For Security Operations Centers (SOC) with capabilities to disarm IT attacks early on, demand for these services naturally increases in reaction to this rise in cyberattacks. However, organizations that lack continuous detection and disarmament capabilities are primarily the ones hit hardest by these attacks, as they require incident management.

Truesec, together with Radar, rates this month's threat level a 2 out of a maximum of 5, which represents a moderate threat level where attacks are predominantly spread out and not concentrated. The effects of the attack are also, for the most part, transient.

IT attacks, Sweden. Development over time, 2022.



Source/data: Truesec.

CASE OF THE MONTH

Hacked Email Accounts

An organization was the victim of a cyberattack where the attacker managed to gain control of an email server.

One of the services that most companies and organizations have to expose is their email server. Once vulnerabilities in these servers arise, organizations need to respond fast and establish additional protection protocol until an update is made available that will fill the security gap.

In this case, the hacker initiated the attack at an early stage before additional protection protocol had been established. Hackers with a specific target can wait several months or even years for a vulnerability to become available within a certain software. Either immediately or shortly after a vulnerability has been published, hackers are able to procure an attack code linked to the vulnerability, enabling them to either continue or commence a cyberattack against their targets.

Source/data: Truesec.

CASE OF THE MONTH

Once the perpetrator had gained access to the email server, a number of email accounts were soon hacked. The attacker was then able to use the identities of several of the employees to carry out the next stage of the attack, this time targeting a third party – the hacker's true target most likely.

Once the hacker had moved on to the next stage of the attack, the email server was abandoned; however, it wasn't until the third party reached out to ask about an email that had been sent that the organization began incident mitigation and the course of events was discovered.

This case shows how confident a hacker can be carrying out their attack, as well as how complex an attack can be. It also shows how even smaller business operators can be caught up in an IT attack, even when they themselves are not the ultimate target.

Source/data: Truesec.

Primary Focus and IT Budget

Sweden's public sector has primarily focused on innovation and transformation to a much greater extent than Sweden as a whole. However, as of 2022, its primary focus on innovation and transformation has now started to shift towards optimization, or in other words, towards the further development of existing investments. The strategic IT budget claims that this is not just lip service even though the share for operations is quite low compared to the share for change. Even so, there has been an increase in the optimization portion of the IT budget compared to previous years.

Parallel with the Swedish public sector's continued investment in digitalization, the sector has also been increasing its investments in cyber and information security as well as in information classification throughout 2022. Furthermore, there is also increased focus on external IT (IT procurement as well as outsourcing of IT services), which makes it important to monitor, interpret and manage the risk associated with the already large, and rising, outsourcing trend in order to understand how it will impact the sector's security and the risk (third party) that outsourcing entails. However, this may be problematic given the fact that the category of supplier evaluations has continued to drop as an investment area for the second year in a row. Thus, the areas of outsourcing and evaluations should be combined to ensure some form of due diligence with recurring security audits of selected and trusted suppliers.

Specific investment areas. The number indicates the percentage of organizations that intend to invest in each specific area.

	Public Sector			Sweden		
	2020	2021	2022	2020	2021	2022
Implementation of AI and cognitive solutions	45	18	6	21	14	11
Implementation of blockchain-based solutions	0	0	3	1	0	2
Digitalization of the organization's processes	86	82	82	60	42	61
Implementation of recognition technology	3	3	3	4	2	4
Security (cyber and information security)	62	68	70	48	38	74
Internet of things (IoT) and sensor technology	28	18	21	12	13	21
IT procurement and contract audits	21	24	39	23	16	25
Supplier evaluations and price comparisons	14	3	0	12	7	11
Skills development strategy	17	18	21	13	10	21
Intelligence analysis and surveillance	21	13	18	16	7	14
Information classification	55	40	52	27	21	32
Insourcing of IT services	3	8	3	6	5	11
Outsourcing of IT services to external supplier	28	16	21	13	8	26

Source/data: Radar.

Priorities for Swedish organizations. The number indicates how the priority ranks (with 1 being the top priority) for each specific area in Swedish organizations.

	Public Sector (Sweden)			
	2019	2020	2021	2022
Security (strategy & compliance)	3 (4)	5 (5)	3 (2)	1 (1)
Digitalization (changing company & business models)	4 (5)	- (-)	2 (3)	2 (5)
Automation (key processes)	5 (2)	- (-)	4 (1)	3 (2)
Security (technology)	14 (14)	17 (12)	11 (11)	4 (7)
Increased degree of automation	1 (1)	2 (2)	6 (8)	5 (12)
Applications (management of existing)	9 (8)	7 (4)	8 (6)	6 (4)
Infrastructure (implementation of new)	- (-)	12 (9)	9 (12)	7 (11)
Management (IT Governance)	6 (9)	6 (6)	10 (10)	8 (9)
Increased degree of digitalization	2 (3)	4 (1)	1 (4)	9 (10)
Meets laws and requirements (Compliance)	12 (13)	14 (8)	13 (17)	10 (20)

Source/data: Radar.

Priorities and Challenges

For a long time, the public sector has focused on the digitalization of its operations within IT (read: streamline and rationalize). This is evident through the fact that the public sector has prioritized digitalization and automation to a much greater extent and over a longer period, not to mention the fact that the two have ranked in the sector's top 3 priorities for a long time. Security (strategic) has also ranked among the sector's top 5 priorities, as has security (training and awareness). However, security (training and awareness) has fallen out of the sector's top 10 priorities as of 2022, whereas security (technology) has seen a spike compared to previous years, now ranking within the sector's top 5 in 2022.

The Swedish public sector's prioritizations show us that the sector is taking the issue of security seriously, just like Sweden as a whole. It is somewhat surprising to note, however, the relatively sharp jump in prioritization of technological security. A possible explanation for this sudden change could lie in the fact that, for a long time, the sector focused heavily on "soft initiatives" (e.g. strategy, training, awareness), while also introducing added complexity through the digitalization of its processes. Now, after the fact, the sector may finally be recognizing the importance of bolstering its technology after several years on the back burner.

IT governance has always been a high priority for the Swedish public sector, ranking slightly higher on average compared to Sweden as a whole. The question that needs to be asked is if IT governance has been/is being built up together with cybersecurity in a way that would be comparable to the due diligence needed to investigate and manage third-party risk (see previous slide). Only time will provide an answer to that question.

Challenges for Swedish organizations. The number indicates how the challenge ranks (with 1 being the biggest challenge) for each specific area in Swedish organizations.

	Energy (Sweden)			
	2019	2020	2021	2022
Digitalization (changing company & business models)	1 (5)	- (-)	1 (2)	1 (2)
Security (strategy & compliance)	3 (4)	8 (3)	2 (1)	2 (1)
Skills development	4 (2)	3 (2)	5 (4)	3 (4)
Meets laws and requirements (Compliance)	8 (14)	11 (10)	6 (7)	4 (8)
Security (technology)	12 (12)	13 (14)	8 (5)	5 (5)
Automation (key processes)	5 (3)	- (-)	15 (11)	6 (11)
Security (training & compliance)	- (-)	10 (6)	4 (3)	7 (3)
Increased degree of digitalization	2 (1)	2 (1)	3 (9)	8 (9)
Applications (management of existing)	10 (6)	12 (7)	10 (8)	9 (10)
Digitalization (understanding and managing digital business risk)	- (-)	- (-)	- (-)	10 (15)

Source/data: Radar.

Priorities and Challenges

The public sector's challenges fall mostly in line with the sector's priorities. The largest challenge is tied to digitalization, which has been the case for many years. The same applies to the second largest challenge in 2022: strategic security. Unlike Sweden as a whole, strategic security has not been considered the largest challenge, be it this year or in previous years. Furthermore, the area of training and awareness as a challenge has declined, which can be linked to the decline in prioritization of the same area (even falling out of the sector's top 10). This is rather notable since training and awareness are still seen as a relatively large challenge, despite the area's sharper decline in prioritization. In terms of challenges, the area of technical security has increased, which is also reflected in the increased prioritization of the same area.

Today, the compromise between security and innovation – which we have spoken about earlier – has lessened, as the issue has now been given more attention within management teams, most likely thanks to attacks being reported about in the media, as well as recommendations and requirements from authorities. Given its societal mission and role in fulfilling functions that are critical to society, the public sector has lived with regulatory requirements for a long time. This is reflected through its priorities regarding both strategic security and the issue of compliance with laws and requirements, the latter of which is becoming increasingly important and, consequently, a larger challenge – larger than for Sweden as a whole.

TRUESEC

Truesec is a global cybersecurity company with one clear purpose: to foster security and sustainability in a digital world through the prevention of cybersecurity breaches and minimizing their impact. Over the years, Truesec has gained a strong reputation and earned the trust of organizations from around the world. Today, Truesec is made up of 250+ dedicated cyber specialists whose expertise covers the gamut of cybersecurity.

“The most important first step is to invest in your ability to detect data breaches and then to be able to quickly take action to minimize damage as much as possible”, says Marcus Murray.

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

For more information: www.truesec.com

Radar.

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

At Radar, we want to help Swedish companies stand at the forefront of global development. Strong companies lead to a stronger society and a stronger Sweden. Cybersecurity not only represents a great challenge and a real business risk, but it is about so much more than just technology.

“Security is important, and there has been a lack of information specific to Sweden that is easy to understand and learn from. This is the next step in helping IT Sweden shore up its defenses and understand how the threat situation is developing, openly and without any secrets – that way, we all win.”

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

For more information: radargrp.com

Subscribe to the monthly report: Truesec.com/monthlyreport