OCTOBER 2022

The Current Threat Situation in Sweden

Sector of the month: Energy

Radar. | TRUESEC

Current Threat Level – Threatcon

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

1	**2**	3	4	5
min				max

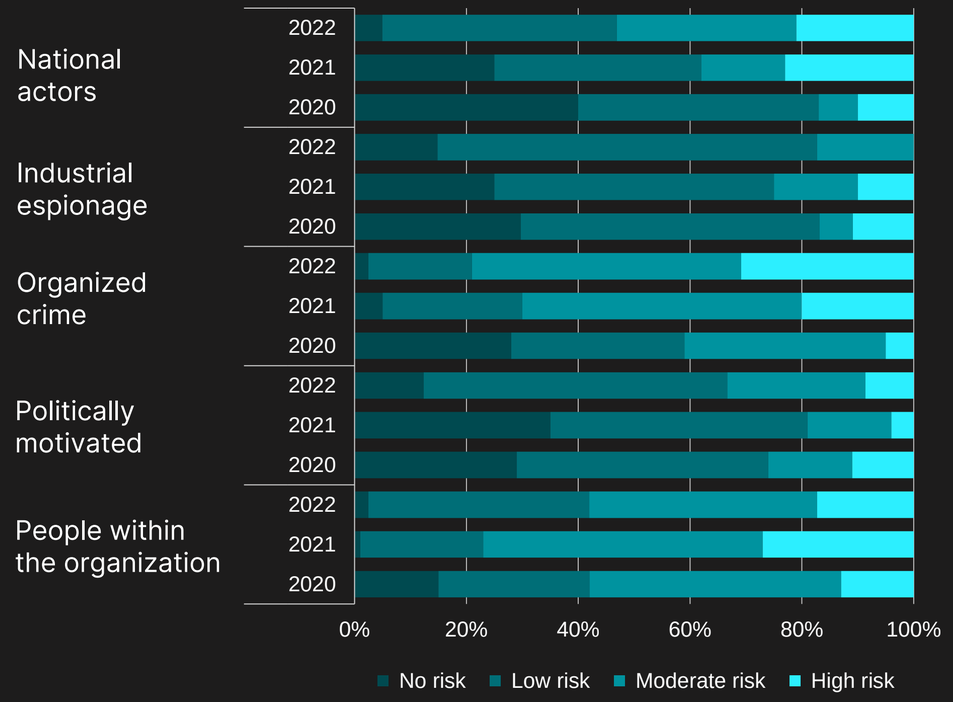
To the person reading this

The current energy situation in Europe has not gone unnoticed by cybercriminals. In addition to the usual threats facing the energy sector, the sector is now exposed to increased pressure from cybercriminals, a reality that will put the sector's IT security to the test in the coming months. However, cybercriminals' current focus on using these attacks to quickly extort money from organizations may be a lifeline for the sector.

Looking at the bigger picture, there are serious risks and vulnerabilities for companies and society if energy companies' OT environment becomes the target of these extortion attacks.

Check out this month's example. There is a lot we can learn from Ukrainian cyber defense, who has been fighting resource-rich and well-equipped adversaries for 8 years, with one such conflict coming to a head this past year. Ukraine has a deep understanding of its adversary, and the country's extensive experience and knowledge inform all of their processes and actions in responding to the threat.

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

Swedish businesses generally experience an increased threat picture in almost all categories, apart from threats from industrial espionage and their own personnel, who all back down somewhat regarding high and medium risk. It is difficult to pinpoint a single factor that allows one to explain the fluctuating trend and reasons for variations in threat assessments, but the media reporting of incidents, vulnerabilities and geopolitical uncertainties obviously have significant factors on what is perceived as a threat. Our respondents' answers are in line with the report on cyber security in Sweden.

For the entire energy sector, which is this month's industry in focus, roughly the same perceived threat picture applies, although threats from other national actors are deemed to pose a higher risk than for many other Swedish industries. We can connect the concern for well-financed threat actors with clear goals to the perceived risk, or even the societal risk, that has arisen in connection with today's global situation.

The Current Situation – Attacks

The rising trend of IT attacks targeting Swedish companies is only continuing. In September, Truesec observed an 11% increase in the number of IT attacks.

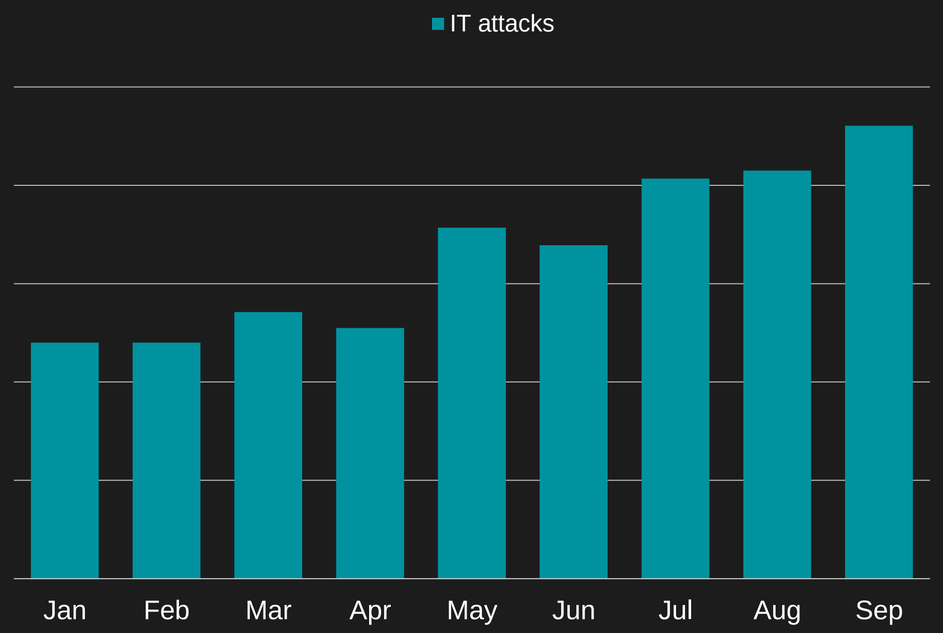
In particular, Truesec noticed a significant increase in demand for incident management throughout September from customers that currently lack active detection capabilities. It can take anywhere from a few hours to a few months for a cybercriminal to carry out an IT attack. This rising trend in attacks, which Truesec has been observing since May, is now being reflected through a significant uptick in incident management cases, where full-scale IT attacks need to be handled.

The rise in IT attacks is continuing, and it is increasing in step with the demand for management services to address full-scale incidents. Furthermore, data indicates a recurrence of last year's wave of extortion attacks.

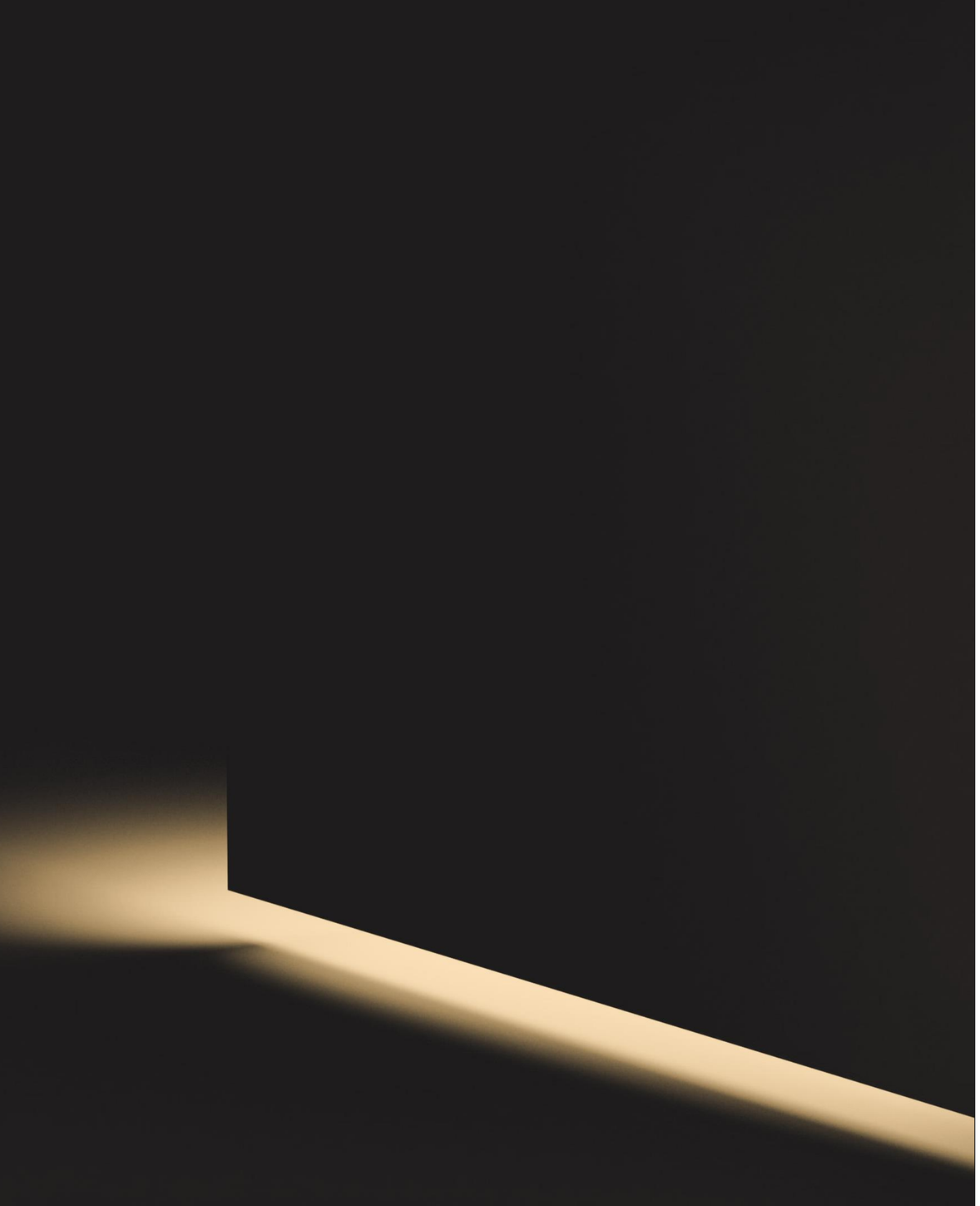
This information is based on enriched data from analysts having done an individual assessment of each case and concluded that the IT attacks, had they not been stopped, could have led to serious consequences for the targeted company. Check out this month's example to learn how these kinds of incidents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

Despite both the continued rise in IT attacks and its subsequent effects on the increased demand for incident management, Truesec assesses this month's threat level to be within normal range. Truesec, together with Radar, rates the 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: ENERGY

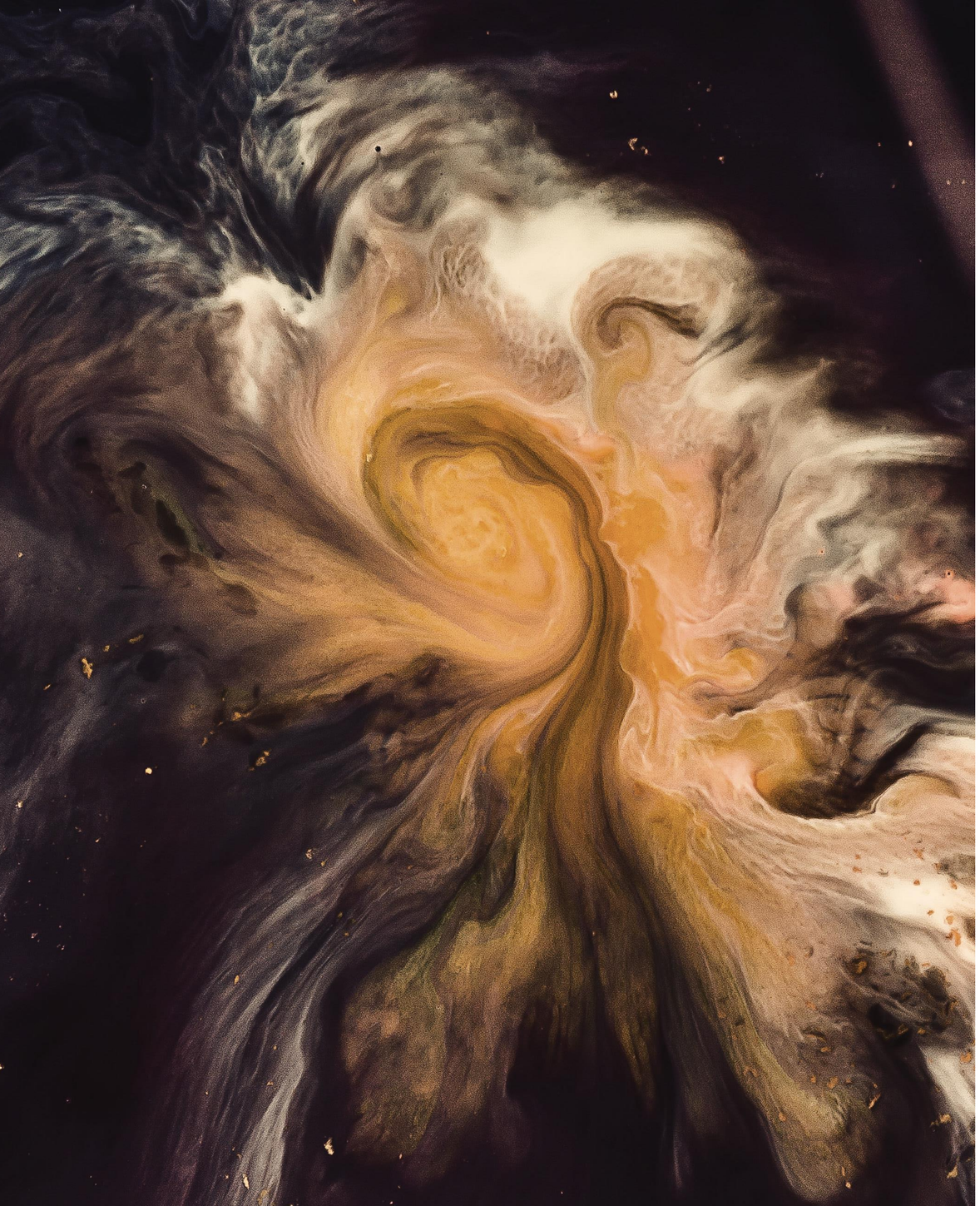
An Extortion Attack Could Have Ended Much Worse

A European company was the target of a serious cyber-attack. The attacker had gained access to the company's network through a poorly patched Microsoft Exchange mail server.

Once inside, the hacker was then able to quietly search through the network, gaining access to more systems and information, until they finally managed to hijack an administrator account. This process took some time, but because the company lacked a robust monitoring system inside of the network, the attacker wasn't in any hurry.

After two weeks, the attacker had taken complete control of the office network. At this point the attacker could have pivoted to the OT environment as well. However, this attacker was primarily interested in extorting money from the victim, choosing instead to download large amounts of sensitive data, including important customer data covered under GDPR legislation.

Source/data: Truesec.

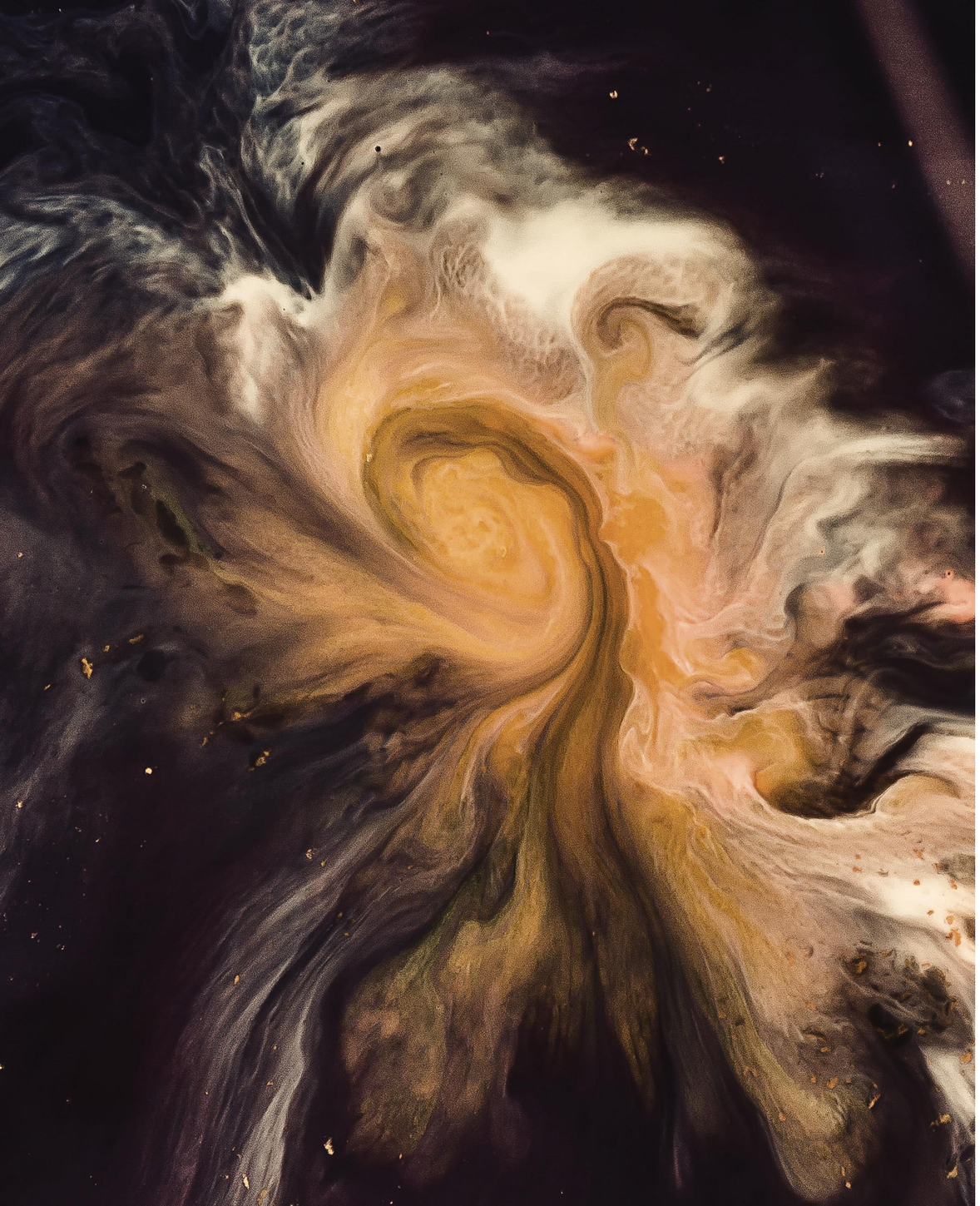


CASE OF THE MONTH: ENERGY

Since 2021 it has become much more common for criminals to extort money from victims by stealing sensitive data and threatening to publish it unless the victim pays a ransom. This is done either by simply stealing data or using ransomware. The reason so many victims likely end up paying such large sums of money is just as much to recover information that has been destroyed or encrypted as it is to avoid admitting that they have been hacked. Additionally, it isn't uncommon for these criminals to threaten victims with GDPR fines that companies are liable to pay if customer information is leaked.

In this incident, it is unclear if the criminals understood how much damage they could have caused if they had taken over and encrypted parts the OT environment, but it could have just as likely been a calculated plan to offer the victim a chance to pay the ransom to keep the attack a secret.

Source/data: Truesec.



CASE OF THE MONTH: ENERGY

Once the attacker finally contacted the victim and explained that they had stolen sensitive company information, there was a period of threats and escalation from the criminals. To increase the pressure on the company, the attacker threatened to hack the company again and outright destroy the data.

This scenario is a clear example of how extortionists can spend large amounts of time trying to force victims to pay ransoms, even after a successful cyberattack. That is why it is so important for any organization targeted by a cyberattack to find the right professional support as early as possible to expel the attacker from the network, minimize any damage and manage the extortion situation.

Source/data: Truesec.

Primary Focus and IT Budget

The energy sector, which normally does not react in the same way as, for example, industry or the national average when it comes to events like market changes, has nonetheless started shifting its focus towards cost reduction. The years of forward-looking IT budgets have come and gone, replaced by a much more prevalent price consciousness. However, given the context, it is worth noting that the energy sector, to a larger extent, has had several years characterized by very aggressive IT budgets in terms of change, even in the first year of the pandemic in 2020, when they invested much more heavily in innovation and transformation when compared to the national average.

Additionally, the energy sector's large investments in security are now leading to increased investments in information classification. If you combine this with the increasing investments in outsourcing to external suppliers and supplier evaluations, you begin to see a coming change regarding the entire sector's IT resource supply. Taken as a whole, a clear image emerges of a sector that invested in IoT, automation and securing its own IT early on and is now preparing for a larger number of external suppliers. This is leading to a rise in investments related to information classification, given that the sector now wants to know exactly which information is passing through which nodes, as well as the need to clearly present the risks associated with exposing data to long and complex chains where attack surfaces are increasing.

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

	Energy			Sweden		
	2020	2021	2022	2020	2021	2022
Implementation of AI and cognitive solutions	23	18	9	21	14	11
Implementation of blockchain-based solutions	0	0	1	1	0	2
Digitalization of the organization's processes	78	57	65	60	42	61
Implementation of recognition technology	0	0	0	4	2	4
Security (cyber and information security)	68	48	81	48	38	74
Internet of things (IoT) and sensor technology	21	22	24	12	13	21
IT procurement and contract audits	24	25	48	23	16	25
Supplier evaluations and price comparisons	10	17	16	12	7	11
Skills development strategy	22	14	24	13	10	21
Intelligence analysis and surveillance	14	6	25	16	7	14
Information classification	39	29	53	27	21	32
Insourcing of IT services	22	21	22	6	5	11
Outsourcing of IT services to external supplier	11	7	35	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.

	Energy (Sweden)			
	2019	2020	2021	2022
Security (strategy & compliance)	1 (4)	2 (5)	1 (2)	1 (1)
Automation (key processes)	4 (2)	- (-)	3 (1)	2 (2)
Increased degree of digitalization	9 (3)	7 (1)	6 (4)	3 (10)
Applications (management of existing)	2 (8)	6 (4)	4 (6)	4 (4)
Cost reduction	14 (13)	- (8)	7 (17)	5 (20)
Applications (implementation of new)	- (-)	3 (3)	8 (5)	6 (6)
Remove human interaction from core processes	- (-)	- (-)	- (16)	7 (15)
Digitalization (changing company & business models)	11 (5)	- (-)	2 (3)	8 (5)
Infrastructure (implementation of new)	- (-)	10 (9)	9 (12)	9 (11)
Security (training & compliance)	- ()	4 (10)	10 (7)	10 (3)

Source/data: Radar.

Priorities and Challenges

In terms of automation and digitalization, the energy sector's priorities have closely resembled the national average. However, unlike the national average, the energy sector ranked security as its number one priority in 2019, ahead of automation. Security, which has always been viewed as a prioritized area (as well as a challenge) by Swedish organizations, was given lower priority in 2020, even by the energy sector. Even so, this lower priority can be considered very minor, seeing as security was still the second most prioritized area in 2020. In 2021, priorities returned to resemble their pre-pandemic levels, and security (strategic) reclaimed its spot as the sector's number one priority.

Today, the compromise between security and innovation 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. The energy sector, which is responsible for infrastructure that is critical to society, has lived with regulatory requirements for a long time, which is also reflected through their priorities regarding strategic security and the fact that the issue has been the sector's top priority for a very long time.

Another difference compared to the national average is that the focus on cost reduction has also had an impact on the sector's priorities, given that cost reduction has ranked among the sector's top 10 priorities since 2021. One final note that is worth pointing out is the rising number of external IT services that is reflected through the sector's prioritization of new infrastructure implementation, which has ranked in the sector's top 10 priorities since 2020.

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
Security (strategy & compliance)	1 (4)	4 (3)	1 (1)	1 (1)
Digitalization (understanding and managing digital business risk)	- (-)	- (-)	- (-)	2 (7)
Skills development	2 (2)	5 (2)	3 (4)	3 (4)
Applications (implementation of new)	- (-)	2 (4)	7 (6)	4 (6)
Remove human interaction from core processes	- (-)	- (-)	- (15)	5 (15)
Infrastructure (implementation of new)	- (-)	13 (11)	8 (14)	6 (12)
Security (technology)	3 (12)	6 (14)	5 (5)	7 (5)
Security (training & compliance)	- (-)	7 (6)	4 (3)	8 (3)
Management of the IT organization	13 (9)	- (12)	2 (13)	9 (17)
Reducing IT costs	6 (7)	12 (9)	9 (10)	10 (13)

Source/data: Radar.

Priorities and Challenges

The energy sector's challenges are similar to the national average, the difference being that two of the security categories (technology and education & awareness) rank somewhat lower. In terms of challenges, we can see that security (strategic) has ranked as one of the top 5 challenges even before the pandemic, along with digitalization and skills development. However, technical security has not ranked in the top 5 challenges for the last three years. This suggests that the energy sector no longer sees development and digitalization as being difficult to balance, meaning that the maturity of those areas is relatively high.

Considering the fact that the energy sector intends to outsource to a larger extent than it has previously (see investment areas and priorities), while already having made extensive investments in digitalization, automation and IoT, the sector has been working with technical security for a long time out of necessity.

It is also interesting to note that skills development, which is considered a large challenge, is not a prioritized area (see previous slide). The ever-increasing scope of cybersecurity activities, such as vulnerability management, surveillance, training & awareness, etc., means that many organizations risk falling behind on their goals before they've even gotten started. One explanation for these insufficient efforts lies in the shortage of skills, given that two-thirds of Swedish IT decision-makers report there being a lack of security knowledge and skills. In other words, skills development as an area should be more heavily prioritized from a challenges standpoint. Additionally, given the fact that skills development is the area with the largest discrepancy between priorities and challenges, this is also where the sector should invest its resources in order to avoid an imbalance between the sector's needs and capabilities.

TRUESEC

Truesec is a leading cybersecurity company with one clear purpose: to prevent data breaches and minimize the damage in the event of a breach. The team consists of more than 250 employees with a wide range of expertise in cybersecurity. Since its founding in 2005, Truesec has delivered security solutions to customers in the private and public sector, both in Sweden and around the world.

The ability to monitor, detect and respond to attacks is the cornerstone of modern cyber defense. Find out more about Managed Detection and Response.

“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: 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