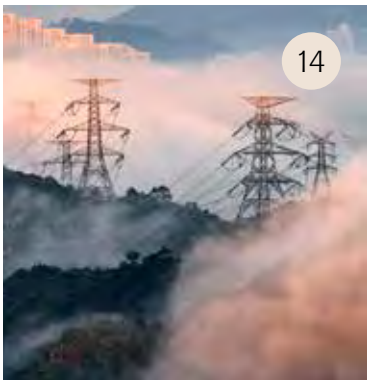
IF'S RISK MANAGEMENT MAGAZINE 02/2021

Risk Consulting

Insights into risk management and loss prevention

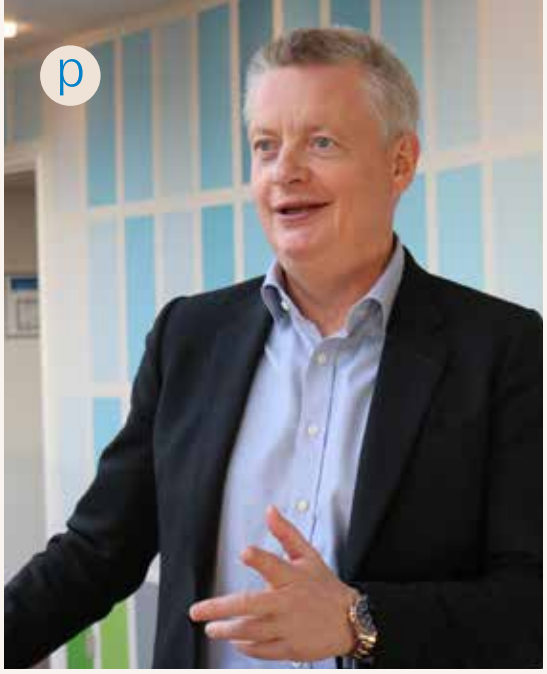
Content



Publisher If, Keilasatama 2, 02150 ESPOO, Finland, +358 10 19 15 15, www.if-insurance.com
Editor-in-Chief Kristian Orispää
Project Editor Carita Hämäläinen-Tallgren
Communications Specialist Caroline Bødkerholm
Art Director Ero Tsirika

Production If Creative Agency
Printing Newprint
Change of address industrial.client-service@if.fi
ISSN 1459-3920
Cover Photo Unsplash

Editorial



Climate change & energy security

As experts in risk management and loss prevention, insurance companies take a long-term view at what potentially lies ahead.

According to the Emerging Risks Initiative (2020), published by the CRO Forum, which consists of Chief Risk Officers from large multi-national insurance companies, the changes in the global climate will continue "to trigger more frequent severe events, especially floods and heatwaves. The increasing cost of claims is compounded by higher value insured properties concentrated in vulnerable locations (e.g. on the coasts)."

Climate change will affect the generation, transmission and distribution of electricity and we need to be prepared for potential future disturbances. Reliable energy sources and the reliable delivery of power to homes and businesses is vital to modern life. Electricity enables commerce and society at large, and it must be secured - especially when the world around us is changing.

So, what are the future challenges that will impact solar and wind energy production? What about the production of other sources of energy, how will they remain stable when temperatures reach new highs and lows? How will increased extreme weather events, for example, impact nuclear power plants, or the local electrical grid? These are important questions for both societies and commerce around the world.

In this issue of Risk Consulting magazine, we look at an ambitious research project from Sweden. As a sponsor and active participant in this 'Climate-change impact on the energy system' study, If P&C Insurance has been supporting the work which will help lay out a roadmap towards a more secure energy future for the Nordics.

We also look at exciting new technologies pioneered by Ping An, an If partner in China, which utilises artificial intelligence to assess transparency in climate risk disclosure.

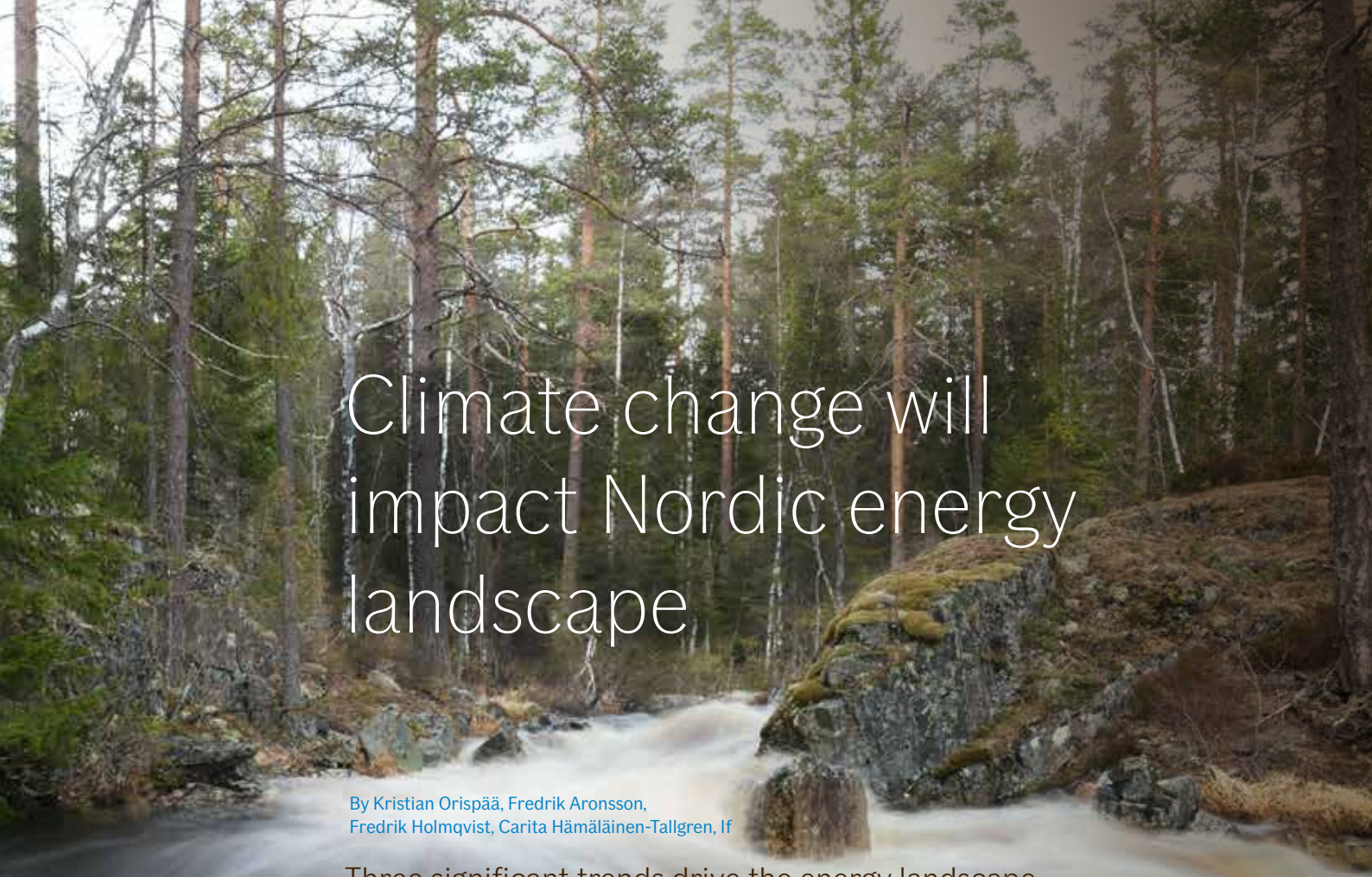
Be sure to also read the article on the race to build fully autonomous vehicles. From driver aid's which protect pedestrians, drivers and their passengers, to the latest technological innovations around smart, driverless cars and more environmentally friendly modes of transportation.

We also provide information on If's Safety Academy in Finland capturing insights into electrical fire prevention. Finally, learn how drones have become an important tool in the insurer's toolbox.

We are by your side, from enabling renewable energy projects to consulting on your risks and loss prevention to help secure your business and its continuity into the future.

Poul Steffensen
Head of BA Industrial, If

If P&C Insurance, contact information
Finland: +358 1019 15 15 Sweden: +46 771 43 00 00 Norway: +47 98 00 24 00 Denmark: +45 7012 24 24 France and Luxembourg: +33 142 86 00 64
Germany: +49 6102 710 70 The Netherlands and Belgium: +31 10 201 00 50 Great Britain: +44 20 7984 7600 Estonia: +372 6 671 100
Latvia: +371 7 094 777 Lithuania: +370 5 210 89 25



Climate change will impact Nordic energy landscape

By Kristian Orispää, Fredrik Aronsson,
Fredrik Holmqvist, Carita Hämäläinen-Tallgren, If

Three significant trends drive the energy landscape currently; the shift towards renewable energy sources, the electrification of society and finally the increased risks of weather-related losses.

Recently, the Energiforsk project "Climate change impact on the energy system", which includes partners Profu, SMHI, IVL Swedish Environmental Institute and Chalmers University of Technology, released the results of the study on the consequences of climate change on the energy system.

If P&C Insurance has been an active sponsor of the project, participating in the study groups with partners and industry.

It is common knowledge today, that greenhouse gas emissions will continue to grow globally. One prediction, for example, is that global temperatures will rise by some 1,5 to 3 degrees Celsius. This change is also expected to occur in the Nordic region.

Expert analysis was conducted on the potential risks around climate change, looking across the coming decades with respect to different energy systems. From wind to nuclear power, the research provided some important learnings on what life will look like in the Nordics and what needs to be done to secure its energy system.

CHANGES IN THE WEATHER SYSTEM

Some issues of particular importance to the energy sector, that were uncovered by the study, noted changes in wind and large-scale atmospheric circulation. Researchers also foresee an increased risk of stationary weather conditions, specifically high-pressure situations with little wind, or situations where multiple low-pressure fronts are sustained for longer periods of time. This may have consequences for electricity generation by wind farms primarily constructed in the northern part of Sweden.

Other changes that are expected include further variations in wind speeds (including mean winds and storms) and alterations in the amount of precipitation. Hydrological changes, both in frequency and intensity, are expected locally and regionally. This will include the growing distribution of rain and snow, as well as the increased amount of rainfall. Similarly, an expected increase in the frequency and intensity of thunder, hail, as well as extreme weather events will continue. Researchers also noted that weather events with a very long return period (> several hundred years) will become more common as will Compound Events, where several weather events will occur at the same time and interact.

WARMEST YEAR ON RECORD

In Europe, 2019 was the warmest year ever recorded. As global greenhouse gas emissions will continue to grow, temperatures are expected to reach 3 °C above today's averages by end of the century.

ENERGY SECTOR BRACES FOR CHANGE

Sweden also belongs to the Arctic Region, together with Iceland, Norway and Finland. In this area, the climate is expected to change at a faster pace than elsewhere in the world.

According to Erik Kjellström, SMHI, there will be major changes in the Nordic climate. These will include higher temperatures for all seasons, with a longer summer season and shorter winters. Also, increased precipitation is expected, while there will be less sea ice during the winter.

Erik Kjellström notes, "we have already seen a major change in the climate. The continued gradual change to increasingly warmer temperatures will shift the seasonal weather patterns. We can expect a more intensive hydrological cycle. There will also be great variability between the years, with alternating hot or cold years, as well as years with increased rain or dryness. There is also uncertainty about changes in the wind climate, however more frequent and increasingly varied extreme weather events are expected."

GROWING FOCUS ON RENEWABLE ENERGY

Today, climate change is influencing the development of energy systems around the world. One key element in the fight against climate change has been the rise of renewable energy production. As Thomas Unger, Profu states, "Climate change will work in a different energy system than what we know today – we and our neighbouring countries are mitigating the impacts of climate change!"

Our future energy system will be more weather dependent (regardless of climate signal); wind power, solar and biofuels will grow in importance. However, we will also become more dependent on electricity, therefore the significance of the electricity grid, will remain vital. The overall impact of climate change is dependent upon the importance of each respective energy type, and their role in the energy system of the future.

In the "Climate change impact on the energy system" project, all types of energy have been analysed separately, however the electricity grid is the cohesive link and is sensitive to sudden events. A certain aspect of climate change can be hidden, featuring natural variations over several years that will need to be strengthened.

Some of the main take-aways include forest fires, which are estimated to increase in frequency and threaten transmission lines. In addition, fires in biomass storage locations are expected to increase as well. As the sea gets warmer, the cooling effect is reduced for nuclear plants, leading to reduced output.

For hydropower, which is the main electricity generation source in Norway and Sweden, increased events of severe precipitation will add pressure on

dams and emergency spillways. This will impact the ability to tap excess water to avoid dam breaks.

Many wind farms are installed, and many wind projects are planned in Northern Scandinavia. However, in this region also icing of blades are believed to be an increased problem when the average temperatures increase. Also, transmission lines will be exposed for increased icing.

DIVE INTO THE GRID

For any society to function, the electricity grid is of vital importance. Without power, society will quickly come to a halt altogether. The electricity grid is also sensitive to sudden events, so preparing for the scenarios carefully will be important to ensure reliable energy distribution in the future.

According to the study, several climate change related factors were identified, which may affect the electricity grid. Some examples of issues that can have a direct impact on the electricity network include:

- *Increased risk of icing and changes in icing in different regions*
- *More intense and heavier thunder events, which in turn can affect the electricity networks, transformers, control system, for example.*
- *Risks relating to the increasing number of extreme events, e.g., ice storms and hurricane winds?*

For each potential threat, an evaluation was created which considered multiple factors to raise awareness of the scenario and its potential risks.

Today, there is a large knowledge base in place, which includes extensive reports, data and information that will allow decision-makers in industry and the relevant authorities to implement the changes needed.

However, we need to act now, in order to benefit from these study results. Acting later will be more difficult and unnecessarily expensive.

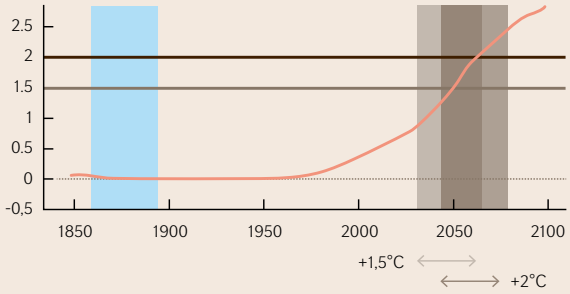
A PROJECT WITH A PURPOSE

According to Fredrik Aronsson, Risk Engineer at If P&C Insurance and Chairman of If's Energy Competence Centre, "If joined the project in January 2020 as a sponsor and our role has been to contribute our expertise in risk management and claims knowledge. Naturally, the findings of this research are not limited to energy companies, but the changing climate will also impact many other industries as well."

According to Lisa Göransson, Chalmers University of Technology, the changes in the energy resource base will impact the composition of the electricity distribution system. Significant system impact is expected, including the increased inflow to water reservoirs, increased growth of biomass, while the

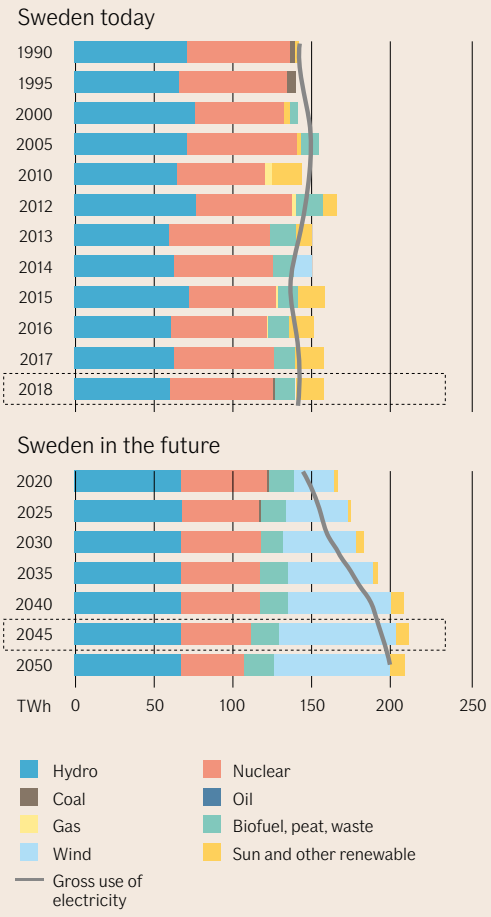
Global temperature

Continuous 30-year global average temperature



Changing climate

The impact of climate change on the energy system



Source: 'Climate change impact on the energy system' study 2021

demand for heat will decline. Other examples include, unforeseen costs stemming from power blackouts or heavy rainfall may be significantly higher than believed. There is now a large Nordic knowledge base and what is needed next, is action. By acting now, energy producers and distributors will minimise the risk of facing unnecessarily expensive changes to existing production methods and systems.

ROADMAP FOR THE FUTURE

Many researchers and analysts found the “Climate change impact on the energy system” study to be a milestone project, bringing together climate scientists and technology experts to study climate change and plan for what lies ahead. Utilising reliable data and accurate modelling has helped to establish a clear view of what lies ahead as well as lay the foundation for concrete planning on how to mitigate these impacts.

*“It is important that we **work together to increase knowledge** of how climate change affects the energy system and society at large.”*

– Stefan Montin, Energiforsk

Fredrik Aronsson reminds us that the consequences of climate change will affect not only the power industry in the Nordic region, but may also impact end users, including industries that are relying on a steady supply of electricity. “The stability of electrical supply varies between different grids across the world. It is important that we continually assess our exposures to electrical blackouts, and what mitigation measures your local facility should put in place to avoid any serious damages in case of power failure."

Power and electricity are vital to our current ways of life. Without robust and reliable energy production and distribution commerce and societies would face inexplicable consequences.

GETTY IMAGES

GETTY IMAGES

GETTY IMAGES

Ping An uses artificial intelligence to detect greenwashing

AI-driven transparency indicators complement ESG ratings and analytic tools in market

This article has been reprinted with permission from Ping An.


GETTY IMAGES

(Hong Kong, Shanghai, 8 December 2020)

Natural Language Processing (NLP) technology, used to analyze language from company disclosures, can help to detect potential “greenwashing” by high emission companies, according to the latest report from the Ping An Digital Economic Research Center (PADERC), a member of Ping An Insurance (Group) Company of China, Ltd. (HKEx:2318; SSE:601318), and the Brevan Howard Centre for Financial Analysis at Imperial College London, the world’s leading climate finance research center.


GETTY IMAGES

The report, "Climate Disclosures and Financial Performance", also found that artificial intelligence (AI)-based climate disclosure indicators perform better than some existing ESG ratings at differentiating green companies from other high emission companies – making these tools a valuable complement to ESG ratings for investment analysis.

The study found that firms with better disclosure of financial impact metrics tend to have higher valuations, lower leverage and lower cost of capital, after controlling for carbon emissions and other firm characteristics. Large cap firms that follow the TCFD recommendations tend to have higher valuations, but small and medium cap firms engaging in climate disclosures may still offer considerable opportunities for appreciation. A range of existing ESG ratings, however, appear to have a weak or inconclusive bearing on valuations.

"AI-based indicators offer a valuable addition to the asset manager's toolkit to enhance and refine their investment screening process, with more objective information on the climate risk exposure of firms," said Chenxi Yu, Deputy Director of Ping An Digital Economic Research Center. "They can also detect potential greenwashing that may be at play in particular companies."

The researchers developed a series of AI-based indicators related to climate risks and financial impacts, drawing from the guidelines of Task Force on Climate-related Financial Disclosures (TCFD) for relevant words and expressions. The NLP techniques automatically assessed the coverage of the indicators in the climate risk disclosure reports of US and Chinese firms in the S&P 500 and the CSI 300.

UNDER-REPORTING OF CLIMATE METRICS BY HIGH EMISSION FIRMS MAY BE ERRONEOUSLY REWARDED

The study found that AI-driven indicators perform better than some traditional ESG ratings to detect corporate "greenwashing" – providing misleading or incomplete information to give the impression that a company is more environmentally responsible than it actually is. The indicators were better than some ESG ratings in differentiating between so-called "brown" firms – those in high emission industries, such as mining, transportation, and infrastructure -- and lower emission firms.

The indicators found patterns in the disclosure among brown firms, including:

- *Under-reporting of the capital and financial impacts of climate risks, such as the impact of stranded assets and liabilities for oil and coal companies*
- *Limited disclosure of Scope 3 emissions (all indirect emissions, except for emissions generated by purchased energy, that occur in the value chain of the company, including upstream and downstream emissions)*

Furthermore, the study found that some ESG ratings penalize companies for climate risk disclosure, which may be encouraging selective non-disclosure instead of transparency from other companies.

PROVIDING COMPANIES, ASSET MANAGERS AND INVESTORS A MEANINGFUL TOOL

The study shows the potential of AI-driven climate risk disclosure indicators as an effective tool to analyze the impact of climate risk on business value, such as:

- *Helping asset managers structure meaningful decarbonization strategies – differentiating companies that may play a crucial role in transitioning to a low-carbon economy*
- *Helping investors inform and support portfolio tilts – allowing investors to articulate their view on the pace at which information on climate risk exposures will be dynamically incorporated in market valuations*
- *Helping investors better understand climate risk premiums beyond emissions – although a carbon risk premium has been documented for high emission firms, the picture is more refined once climate risk disclosure indicators are taken into account*
- *Helping investors capitalize on the increase of climate awareness – AI-driven indicators can help to inform investment policies aimed at making the most of forward-looking metrics of climate change during the transition to a low-carbon economy*
- *Helping investors better articulate their view on climate risk-return tradeoffs – investors could use AI-based indicators to specify competing constraints in their portfolio optimization engines, to identify portfolios achieving their desired risk-return tradeoffs*
- *Helping companies understand how climate risk disclosures can add shareholder value – climate disclosures can reduce the cost of capital*

This report, the second on climate risk and financial innovation, combines Ping An's expertise in financial technology with the Brevan Howard Centre's academic research on investment risk. The research partnership focuses on developing methodologies using artificial intelligence (AI) and big data to assess the risks for investment assets from climate change and other ESG-related factors.

PADERC is a professional institution specializing in macroeconomics and policy research, using big data and artificial intelligence to provide insights on macroeconomic trends, including developments in ESG disclosure. The Brevan Howard Centre connects the financial economics expertise of Imperial College London Business School with other disciplines, including engineering and computational finance. Its three streams of research include financial stability and financial regulation, comparative financial systems and designing new financial structures, and financing development, environment protection and medicines.


GETTY IMAGES

For more information, please read the full report by scanning this QR-code.

Cyber criminals target the energy sector

The energy sector is increasingly targeted by cyber criminals whose goal is to steal data, disrupt or even shut down power production and distribution operations. There are different factors that can increase the sector's vulnerability and attractiveness towards cyber criminals.

By Caroline Bødkerholm, If

One of the factors, that affects the vulnerability of the energy sector, is that all other industry sectors rely on the availability of energy. The stability of the energy sector is what keeps the wheels of the economy spinning and this makes energy companies a vital supplier to businesses, communities and individuals. Enabling heat and electricity, the sector is thereby targeted by criminals looking to cash in.

Mikko Peltonen, Head of Digital Risks & Cyber at If P&C adds; "The energy sector is also part of the critical infrastructure that underpins national security." For that reason, cyber-attacks against the energy sector are often perceived as attacks on the country itself."

The number of threats from nation-state actors has increased immensely over the previous years.

In fact, Microsoft highlights in its Digital Defense Report for 2020, that "nation-state actors are engaging in new reconnaissance techniques that increase their chances of compromising high-value targets, criminal groups targeting businesses have moved their infrastructure to the cloud to hide among legitimate services."

Although an exact figure regarding the increase in nation-state attacks is difficult to validate, it is clear that cybercrime has exploded during the COVID-19 pandemic. In fact, in the aforementioned report, Microsoft identified 16 different nation-states, "targeting customers involved in the global COVID-19 response efforts or using the crisis in themed lures to expand their credential theft and malware delivery tactics."

The energy sector is also targeted to get sensitive data on power grids, locations of power stations, generators, substations and transformers for the purpose of espionage, sabotage and hybrid warfare. This kind of cybercrime is often rooted in political and economic motives.

A third factor, that puts the sector into a vulnerable position, is the many emerging innovative technical solutions, that are being put into use every day. The industry is getting smarter, more digitalised, as well as increasingly connected. At the same time, there is a rise in sophistication among cyber criminals who are exploiting complex vulnerabilities in companies' supply chain.

Mikko Peltonen comments: "I am sure that we will see much more of these contemporary supply chain cyber-attacks in the future."

SUPPLY CHAIN ATTACKS

A supply chain attack is an attack where hackers have identified a weak link, which can be open-source tools, suppliers or even service providers. This weak link becomes the hacker's entry to the company. A known example of a supply chain attack is NotPetya that happened in 2017 where Maersk Tankers suffered severe consequences and an extremely costly down time. The most recent example of such contemporary supply chain cyber-attack is the SolarWind attack, that was discovered by FireEye, one of the world's top cybersecurity firms, in December 2020. SolarWind has despite its company name (SolarWind meaning – flares from the sun), nothing to do with the energy sector. It is a network monitoring system used by, among many others, large energy companies to monitor traffic and uptime. The SolarWind attack was complex and required substantial preparation from cyber criminals. The infrastructure of SolarWinds was compromised and malware was maliciously installed into a software


GETTY IMAGES

update. So, when users of SolarWind's software solution Orion accepted the new update, they unknowingly updated their system with the compromised software. The code created a backdoor to the users' information technology systems, which was used to install even more malware to spy on companies and organisations.

The malicious update went undetected for months and up to 18,000 of SolarWind's users installed updates that left them vulnerable to hackers (Business Insider, 2021).

The SolarWinds attack was not targeted against the energy sector. However, since many large energy companies are using the SolarWinds network monitoring system, it is safe to say, that their data has been on risk for espionage.

SPEAR-PHISHING ATTACK

Another attack, where the energy sector was the ultimate target, was the phishing attack on the Ukrainian power grid.

The attack was a spear-phishing attack, which entails that hackers are sending emails to carefully selected employees in a company, and that the emails looks like they are from a trusted sender. The purpose of such attack is to either infect devices with malicious malware or to force victims to hand over money or data.

Within the Ukrainian power grid, the campaign was targeting their employees working in IT and system administration. The spear-phishing campaign delivered a malicious email to these carefully selected employees, who when clicking on the attachment, opened a backdoor to the hackers. On December 23, 2015, one of the employees experienced that his cursor on his computer began to move around the screen on its own. It was not possible for the employee to take back the control as the attackers had already logged him out. The consequences were immense as 230,000 customers lost power. (Ukrainian Power Grid Attack - Blog | GlobalSign)

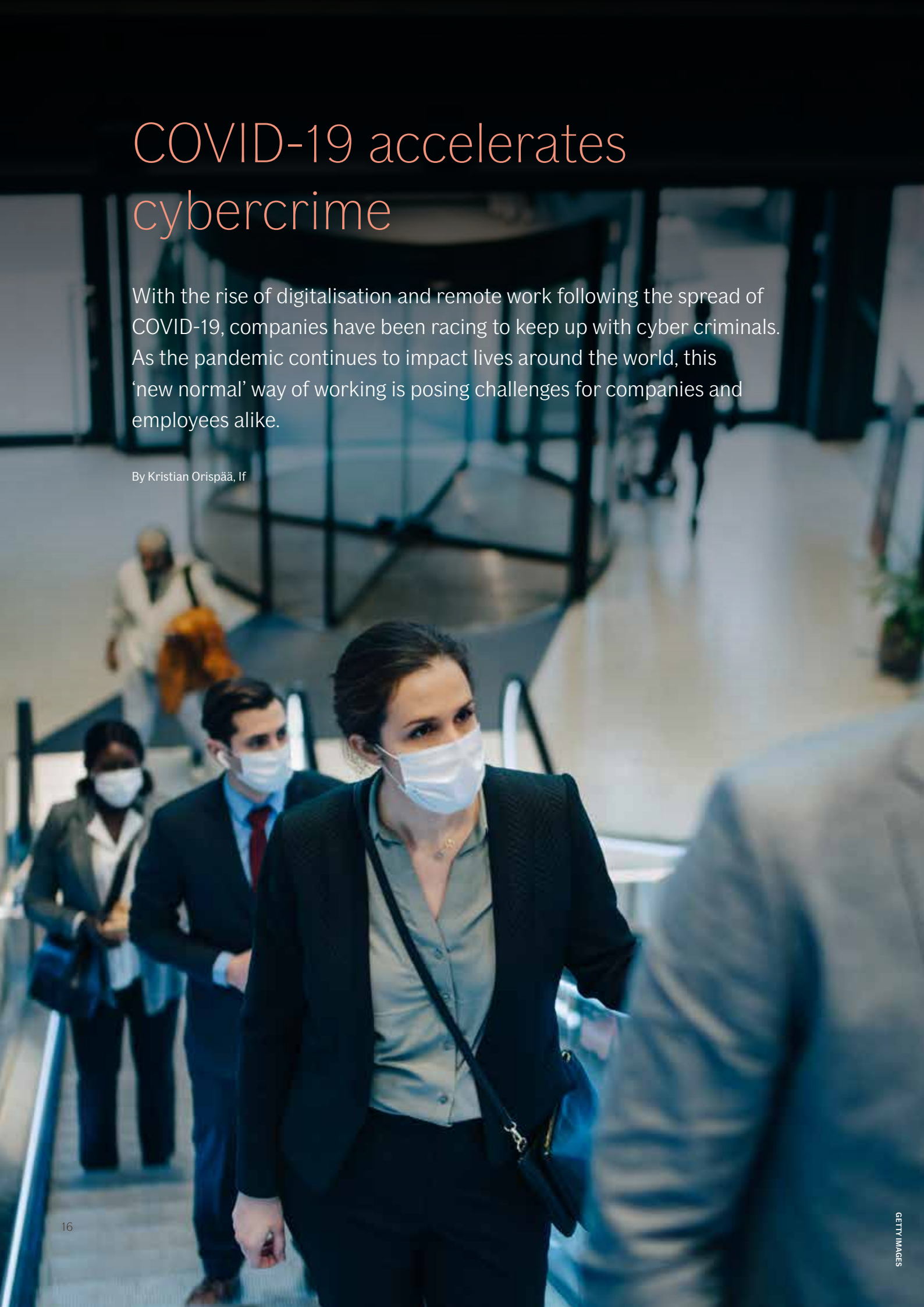
DUE DILIGENCE

"Cyber threats are here to stay, and there are multiple stakeholders that can be a part of the solution to this growing problem. To maintain the production and distribution of energy and power services to businesses and communities, we must remain diligent and continue to focus on cyber and IT security as a priority," says Mikko Peltonen.

COVID-19 accelerates cybercrime

With the rise of digitalisation and remote work following the spread of COVID-19, companies have been racing to keep up with cyber criminals. As the pandemic continues to impact lives around the world, this 'new normal' way of working is posing challenges for companies and employees alike.

By Kristian Orispää, If



GETTY IMAGES

In the fourth quarter of 2020, McAfee, the device-to-cloud cybersecurity company, reported in their McAfee Threat Report (April 2021) that "COVID-19-themed cyber-attack detections increased by 114%." The report highlights that the complexity and number of IT security threats continued to evolve during the coronavirus pandemic. One key additional element has been the rise of remote workers. Wi-Fi networks at home and family laptops with elementary passwords put organisations at heightened risk to fall victim to a cyber-attack.

> *"Out-dated systems are a serious cause for concern."*

FREE VACCINES FOR ALL

Phishing is increasingly targeted, and as an example, one key problem has been the availability of vaccines. Criminals are reaching out by email, promising direct and accelerated access to coronavirus vaccines, all the while pushing malware to unsuspecting recipients. Vaccines can also be purchased on the DarkNet, some are real, others are fraudulent.

A key concern has been the vulnerability of home Wi-Fi routers. As criminals actively and systematically are scanning home networks, IT security teams struggle to keep the routers of company employees up to date.

One example that has stood out during the past year, has been Microsoft Remote Desktop. This software has been the source of headaches for many companies, as several cases of malware entering corporate networks have taken advantage of vulnerabilities in this software.

Computers and networks are developing all the time. Out-dated systems are another serious cause for concern. A highly publicised case in the media comes from Florida, where an old computer in a water treatment plant was hacked by exploiting the Windows 7 operating system. Adding insult to injury, the computer was 'protected' with weak passwords. In this instance, criminals came dangerously close to succeeding in their attempt to poison the local water supply.

What we see as a common shortcoming is that people are simply unaware of the risks, and how to manage them. Working from home, whether you enjoy it or not, brings an added threat level to the equation.

IT'S NOT ALL DOOM AND GLOOM

On a positive note, solid planning, alongside proven security practices, coupled with common sense and basic network / computer hygiene will go a long way when it comes to protecting your network.

Below, at If's Risk Management Day, held in Norway in April, Mikko Peltonen, Head of Digital risks and Cyber at If P&C, highlighted some recommended practices and tips to help prevent, and aim to mitigate the impacts of, an attack on your company network.

1. *Know your environment and data*
   What assets do we have? Identify the most critical data, applications and systems, and be aware of the vulnerabilities that exist with these. To simplify, you cannot protect what you don't know you have.

2. *Threat modelling*
   Who could benefit from breaching those assets? What do they have to gain? As a preventive action, model the potential threats to gain an understanding of who might come after your valuable assets. Don't forget that technical failures and insiders also pose a threat to your data integrity, confidentiality and availability.

3. *Plan and implement*
   Plan and implement your security controls around your threat model. Execute these efforts on a well-established framework, such as NIST CSF or an Adaptive Security Framework. You need to establish deep understanding into your current controls, and the strength of these to sufficiently deter attacks and counter the modelled threats.

4. *Test your controls*
   It is good practice to test your controls before the hackers do, to ensure their effectiveness against the modelled threat. Simulate and test your readiness, validate disaster recovery and consider penetration testing.

5. *Detect, respond and evolve*
   Detect, respond and evolve means; execute your plans and practice in order to effectively be able to detect and respond to cyber incidents. Feed any findings back to the beginning of the process and repeat in order to evolve and strengthen your defences.

Don't forget the importance of Detection. Respond to incidents as they come. Learn from the mistakes and have a feedback loop.

Keep in mind, that not all of cybersecurity is highly advanced and there is no single solution that will work for everyone. Knowing yourself and your enemy does go a long way. ▭

GETTY IMAGES

Driverless vehicles on the road – how close is our autonomous future?

The majority of traffic accidents are caused by human error, which can be related to conscious acts such as speeding, alcohol, mobile phone use as well as stress or even simple distractions. Although human errors can be minimised or even prevented with advanced driver assistance systems, the question remains: are autonomous, self-driving vehicles safe? And there are plenty more questions, from legal concerns to insurance matters, alongside technical issues that are essential to consider. We have gathered specialists at If P&C Insurance within the field to talk about the possibilities and the risks involved.

By Caroline Bødkerholm, If

WHY LOOK AT INSURANCE DATA?
Insurance data provides unique insight into the safety and development of advanced driver assistance systems on the way to fully autonomous vehicles. The quantity, availability, and representativeness of insurance data offers extensive insights into traffic safety. This data provides valuable information when evaluating real-world conditions, the reliability of traffic safety systems, as well as the safety of the vehicles on our roads.

> *"Drivers tend to **trust the automation** beyond its actual capabilities."*

If's Research Leader in Traffic Safety, Irene Isaksson-Hellman, comments:

"There is a general lack of crash data around vehicles equipped with the latest technology as the number of such cars involved in accidents is low. However, one enabler for early evaluations is insurance data to obtain the amount of data required to make this assessment accurately."

WHERE ARE WE TODAY?
The industry is moving at an accelerated pace towards autonomous solutions. Anders Lindström, Casualty Underwriter at If P&C Insurance comments;

"Google is moving fast with the development of their robotaxi service, Waymo. One of the reasons is that the State of California is permitting fully driverless vehicle testing, and has since 2018. Currently, there are seven companies who have permits for driverless vehicle testing in California, with one company (Nuro) also being granted a permit for the use of driverless vehicles in their commercial delivery services. Further, we have China and the US that are in a race to finalise the techniques and both countries want their companies to be the world leaders within this field."

Despite above examples, there is widespread doubt about the vision of a completely driverless traffic system becoming a reality any time soon.

Irene highlights, "the preferred environment for AVs is a fully-automated one, without pedestrians, cyclists and manually driven cars. Clearly, today's big cities constitute a very complex environment for AVs, as the behaviour of pedestrians, cyclists and manual driven cars is impossible to predict."

STILL SOME WAY TO GO
The Society of Automotive Engineers has developed a classification system that defines the degree of autonomy by which a vehicle operates. Ranging from level 0-5, the driving automation begins with manually controlled vehicles and ends with a fully autonomous traffic system that does not require any human attention.

Today, the second level on this scale can be seen, in the technologies that are included in manufacturing and production, for ordinary vehicles operating on public roads. Level 2 is defined as having partial driving automation, which means semi-autonomous vehicles with advanced driver assistance systems including steering and brake/accelerating support. However, at this level the driver is fully responsible and is expected to take control of the car at any time.

Cars are increasingly equipped with these systems that help the drivers prevent accidents. Functionalities, such as lane keeping aid and autonomous braking, combined with Adaptive Cruise Control, help drivers stay in their lane and optimise distances, for example to the car in front of you. These are collision-avoidance features, that are already common in modern cars.

CHALLENGES IN THE SEMI-AUTONOMOUS PHASE
One of the emerging central issues in the semi-autonomous phase, is that humans have begun to rely too much on these systems. A lot of research is being done in this exact area, as drivers tend to trust the automation to beyond its actual capabilities.

According to Irene, "one example, is that drivers in semi-autonomous vehicles are more likely to distract themselves by using their mobile phone or reading, because the car is driving itself. This obviously affects the driver's needed situational preparedness, should the driver be asked to take control over the vehicle. The driver must be able to immediately evaluate the traffic, understand the risk or dangerous situation ahead, decide on a safe course of action, and react quickly."

In other words, there is always a risk of human error and it is critical to be alert and careful when operating a vehicle. It is vital that the driver takes the warnings seriously and reacts to these to avoid an accident. The human driver remains responsible for their actions on the road in all traffic situations

LEGAL ISSUES REMAIN
Each country has its own regulatory statutes relating to vehicles on public roads. In many cases, a human driver is a fundamental requirement. In some environ-

ments, such as airports, autonomous transportation already exists, in the form of automated trains and busses. Nonetheless, it is vital to have a common framework on the legal matters relating to autonomous vehicles.

If's Senior Legal Counsel, Sonja Dyrhage, highlights; "it is difficult to give detailed rules before something is on the market. In Sweden for instance, the legislator has suggested several regulations in order to enhance the testing and development of different

LIFESAVING TECHNOLOGIES

Research at If has contributed to the understanding of new safety technologies where results have been referred to also globally. The research highlights that, according to statistics, the automatic emergency break (AEB) has been proven to be very effective. This together with similar findings by e.g. the Insurance Institute for Highway Safety (IIHS) has led 20 automakers to a voluntary commitment, to add automatic emergency braking (AEB) systems as

> *"Overall, traffic safety has improved and vehicles are **safer and more intelligent than ever before."***
>
> *– Irene Isaksson-Hellman, If*

levels of automatic driving. However, no changes have been made in Sweden with relation to the general considerations regarding liability and rules concerning the requirement of a driver and driving licenses. Any change to legislation is not going to come quickly, however further changes in the regulations, within the EU and globally, must be introduced and keep up the pace with the technically developments."

FROM A TECHNICAL VIEWPOINT

If P&C Insurance has expertise in mobility trends and follows the legal aspects, technology developments and social considerations surrounding autonomous vehicles.

Irene states that, "we are studying advanced driver assistance systems and estimating the benefits from these. From our perspective, the ultimate aim is to prevent accidents, and reduce the number of fatal and serious accidents. Fortunately, the number of deaths in traffic accidents continues to decline. We can say that traffic safety has improved and that vehicles are safer and more intelligent than ever before."

Some of the latest vehicle safety and driver-assist technologies include:

- *Pre-sense or collision-avoidance, which automatically brakes the vehicle in a critical situation – recognising more and more things beyond cars including wildlife such as a moose or a deer, as well as pedestrians and cyclists.*
- *Lane keeping aids, which help keeping the vehicle in the lane.*
- *New technologies that are around the corner include monitoring the status of the driver, alertness and attention to the driving task.*

standard equipment by September 1st, 2022 in the United States. The commitment is brokered by IIHS and the National Highway Traffic Safety Administration (NHTSA). This represents more than 99 percent of the US auto market. Similarly, the European Union has reached a provisional political agreement on the revised General Safety Regulation. It is noted that, as of 2022, new safety-related technologies will become mandatory in European vehicles to protect passengers, pedestrians and cyclists.

Irene notes, "the industry and its stakeholders, including insurance companies, need to be able to prove that these driver-supporting technologies and systems are effective and support the development and implementation of these life-saving technologies to the market faster."

FROM AN INSURANCE PERSPECTIVE

It is important to have balanced and functional rules and guidelines about sharing information and storing data with regards to accidents and the technical solutions involved.

Sonja explains, "there is plenty of work to be done, for example, clarifying the definition of a driver and the driver's responsibilities when needed, and rules regarding civil and criminal liability."

Sonja continues: "in 2018, an official report by the Swedish Government suggested several possible changes in different legislation areas, but so far, changes in legislation have only aimed to further allow and extend exceptions that will enhance testing and developing activities. Within the EU there is an interest to consider changes in the Product Liability Directive due to developments in automatic driving."

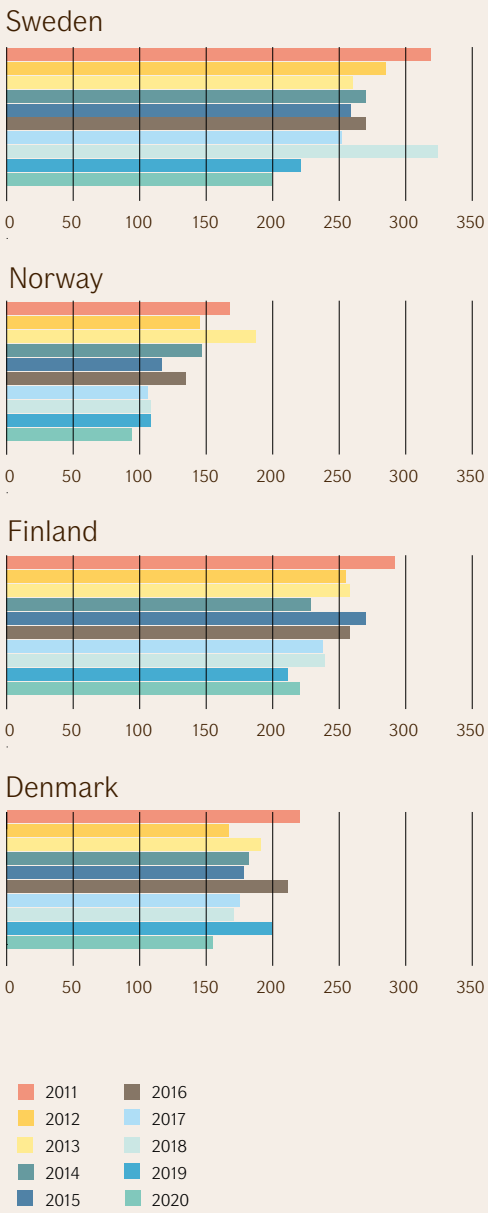
As of today, the existing mandatory traffic insurance system, such as the one in Sweden, can be accurate and

functional with small changes once autonomous vehicles take to the roads. It will be important that insurers and other parties, are given a right to receive and store data in order to be able to develop accurate liability, as well as recourse mechanisms, and to continue promoting safety, through better solutions in the transportation and traffic infrastructure.

REALISING THE VISION

Irene concludes with a look into the future, "I believe that technology and the dialogue surrounding autonomous vehicles will continue to evolve opening up more possibilities and applications. In the future, more driverless vehicles will be taken to the roads, though with limitations and restrictions that will remain until the legislation and technology is mature enough to truly open the way for autonomous vehicles in city traffic, for example. Advanced driver assistance systems will become more and more intelligent as they move towards full automation. As stated, technology is not the only challenge, this is also a matter of trust and acceptance across society as a whole. The social aspect is very important. Are we ready to change how we look at mobility and transportation, do we really want to buy a new expensive autonomous vehicle, or will we prefer to drive the car ourselves?"

Road traffic fatalities in Nordic countries 2011-2020



Source:
SSB, Statistikcentralen, Vejdirektoratet and the Swedish Transport Agency

GETTY IMAGES

Getting to grips with electrical fire risks

By Jussi Lehtonen, If

Managing electrical fire risks can be a major challenge for clients who own and operate electrical equipment and installations. In the worst case, failing to understand the risks or neglecting to carefully address electrical risks can lead to situations where learning by trial and error becomes too commonplace. To prevent losses, it is vital to understand electrical fires and mitigate fire risks effectively.

LACK OF DATA

In order to understand electrical fire risks, one key factor is that there are very few comparable data collection and operating models for collecting statistics on electrical fire risks. Further to this, a major challenge is also posed by the fact that smaller electrical fires and serious near misses are not always investigated and reported to the necessary extent. Often, it is very difficult to compare different statistics related to the topic of electrical fires. The downside to a lack of consistent and reliable data is that this can lead to a distorted sense of safety regarding risks associated with electricity.

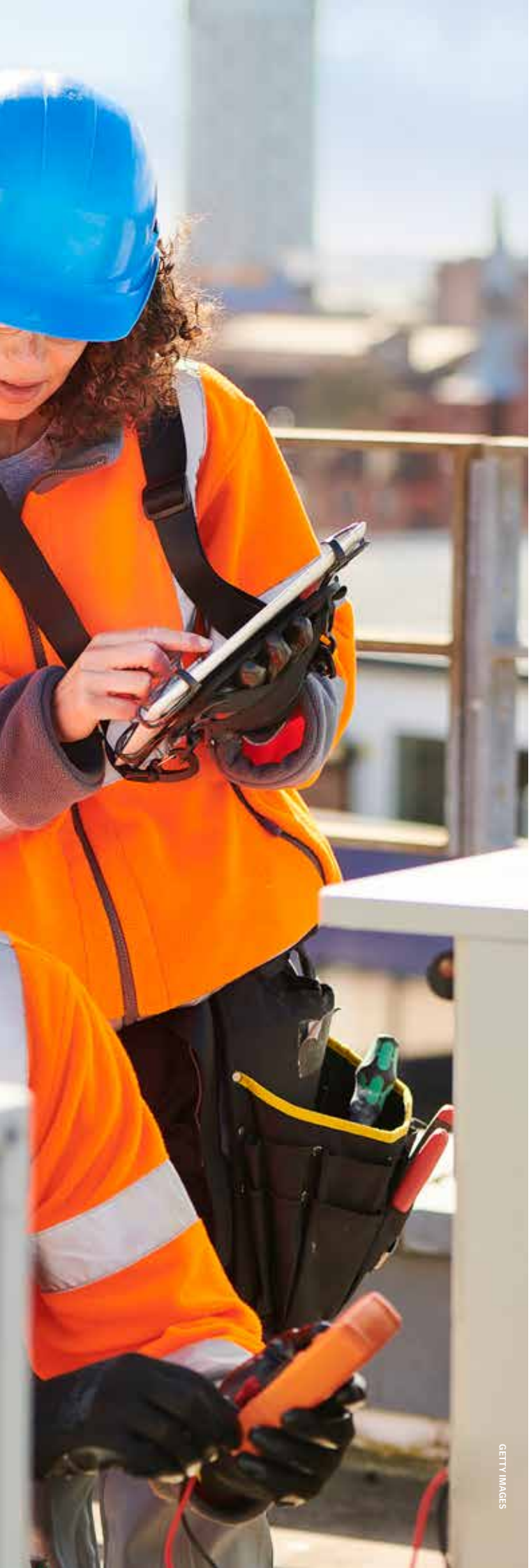
Naturally, having consistent and comparable statistics would clearly benefit both the owners and operators of electrical installations, as well as persons maintaining these installations, to better manage their day-to-day challenges.

COMMON ISSUES

Issues with electrical safety and related problems often result from a lack of planning and failures in the flow of information between different parties involved. It is quite common that the electrical equipment is owned, operated and maintained by separate parties. Different responsibilities are broken down into smaller tasks, then divided for example between several teams. These teams may be working in shifts while electrical contracting, maintenance teams and purchasing teams all own some task or responsibility relating to the same equipment. Overall, this leads to the fragmentation of overall responsibility.

For example, the electrical compatibility between technologies designed over different decades should always be taken into account as part of the overall planning, from purchasing to upgrading and so on. Sometimes, this can be a level of detail which is beyond the understanding of the purchasing organisation. In the worst-case scenario, lack of proper oversight on such matters can constitute a high risk for incident or accident with respect to the electrical installation.

In addition, frequent changes in responsibilities within organisations (subcontractors and own activities) can add further challenges. The risk of an electrical fire is further increased in cases where processes and quality maintenance have not been adequately documented or described. When detailed information about how certain electrical equipment has been maintained is known by a single person or contractor, detailed knowledge-sharing becomes critical to a successful transition from one partner to another.



GETTY IMAGES

UNDERSTANDING SAFETY RISKS

Although clients generally have a good overview of potential electrical fire risks, there are some details which are commonly overlooked. For example, equipment failure situations are commonly omitted or considered from a fire risk perspective. The understanding of electrical equipment failures by a layman and often also by an electrical engineer or other professional, is limited to general awareness on the life and health risks or of facts relating to the equipment itself, e.g. in relation to troubleshooting the technical malfunction.

For example, experience is vital in recognising the basic conditions that exist prior to a fire igniting, this requires extensive practical knowledge and expertise. Working with a capable and reliable partner will help owners, operators and maintenance teams appropriately interpret the risks associated with their electrical equipment and installations, as well as in the immediate surroundings of these with regards to nearby combustible materials, for example.

ENABLING BUSINESS CONTINUITY

Looking at concrete examples, sudden changes in temperature and risks posed on the environment in which the electrical equipment is installed, such as the splashing of molten metal, can be associated with equipment failures but are often perceived as unrealistic threats.

Proper maintenance is vital to protection against electrical fires. The electrical installations and equipment must be regularly maintained and kept clean, properly encased and used correctly. These steps would help in the prevention of electrical fires, as well as help to ensure that when fire breaks out, the damage is limited to smaller areas. As a further benefit, the equipment will also work as intended by the manufacturer in the event of failure or fault situation.

With the demand for electricity on the rise, it is important to keep abreast of standards and regulations. It is important to replace obsolete, under-sized installations and equipment that do not meet current demand. Aging installations and equipment pose a serious risk of electrical fires.

Not all repaired faults are documented. Therefore, even repeated near misses may only be known by the contractor or even a single electrician.

SURVEYS PREVENT LOSSES

In electrical risk surveying, a major role is played by identifying the operating culture. How, and by whom, is the equipment operated and maintained? What is level of skill and experience of the contractor and other persons working with the installation and equipment? These are important questions that will help in assessing the potential risks that exist on-site.

An electrical fire risk survey consists of multiple stages, including careful preparation before visiting the location, informing the parties involved about their responsibilities and agreeing on the roles of persons participating in the survey, occupational safety during the survey, possible preparation of equipment e.g. by starting process equipment or lighting and ventilation equipment, for example.

Conducting the actual survey, which can last from a few hours to several days, can lead to precisely defined training sessions with the client's maintenance organisations. Of course, sometimes surveys will also find that no follow-up actions are required. Each survey is unique and can have a different outcome, depending on the results of the study.

4000 SURVEY VISITS

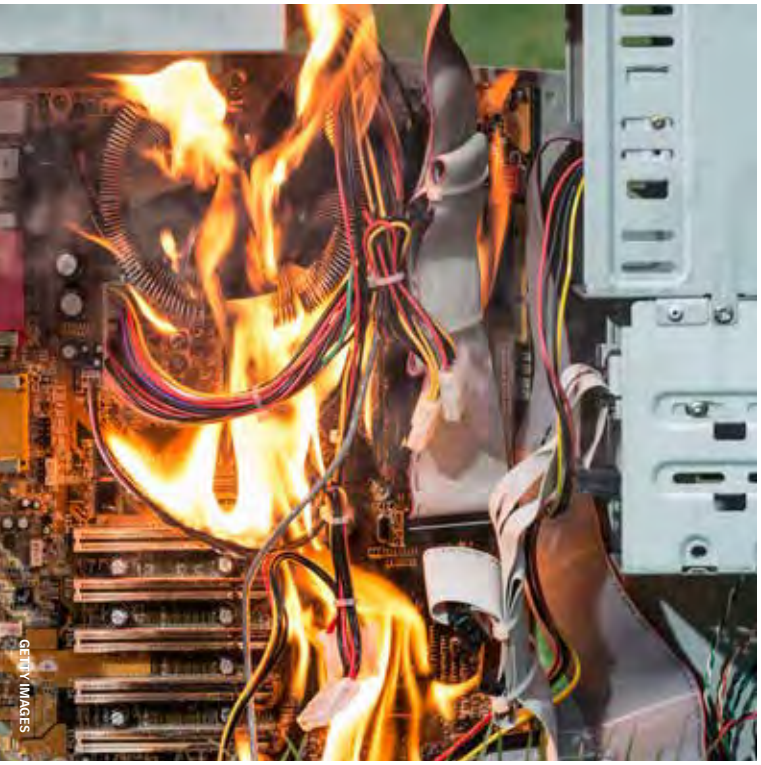
It is understandable that not all electrical engineering professionals have been involved with electrical fires. Therefore, they may not be able to identify electrical fire risks in their day-to-day activities. Continued and open dialogue on this topic is therefore key to safer operations, a survey visit is often beneficial to all parties. It is not uncommon that If's Safety Academy experts will uncover faults in electrical equipment or installations that are not only hazardous but potentially about to fail with serious consequences.

When it comes to increasing our client's understanding of electrical fire risks we work by their side, and in close cooperation, to manage risks, share knowledge and support their individual requirements. Thanks to dedicated work on this important topic, we now have experience of some 4,000 electric fire safety inspections, with more than 40,000 operational switchboards reviewed.

An essential part of the survey process is the active involvement of the client or the electrical subcontractor in the survey. It has been our experience that this way of working brings multiple benefits from knowledge-sharing to smoother execution of the survey.

Working together, we gain a solid understanding of existing maintenance practices, operational issues and more. This helps everyone involved to develop solutions for identified issues that will help to ensure that the equipment is safe and secure, providing reliable operation into the future. ▭

> *"In Finland, If's Safety Academy conducts electrical fire risk* ***surveys to prevent fires caused by electricity****, and to ensure business continuity for clients."*



GETTY IMAGES

GETTY IMAGES

If's Safety Academy in Finland

An electrical fire is the most significant preventable factor that can disrupt a company's business. In the spring of 2013, If Insurance launched a major electrical safety study to investigate the acute fire risks of electrical systems across 1,000 Finnish small and medium-sized companies. This study focused on industries where the use of electricity is critical to the continuity of operations. If's Safety Academy was established as part of this study and the work continues to this day with encouraging results.

If's Safety Academy provides support to Commercial customers in Finland in relation to electrical risks, including training events and risk management survey services to ensure electrical fire safety and increase knowledge-sharing on electrical fire risks.

Our aim has always been to help build a culture that is focused on active loss prevention. From the very beginning, we have worked towards establishing a systematic and consistent operating model that ensures both the quality of electrical equipment inspections as well as the quality of the data collected. Focusing on quality and taking a critical approach to what we do has been our speciality.

Drones take their place in the insurer's toolbox

By Kristian Orispää, If

Today, drones are used by individuals, industry, as well as government entities, to execute a variety of tasks and purposes. From conducting building safety inspections to gathering data over disaster areas, drones are becoming an essential tool for various industries for a variety of purposes.

Unmanned aerial vehicles (UAVs), commonly known as drones, also take to the skies more and more often to support insurers in their daily work. Serving specific purposes, such as data collection to support claims handling, drone technology is utilised around the world in insurance related fieldwork.

From risk management, to investigations and claims, there are many opportunities for drones to increase efficiency and accuracy for insurers. Alongside expediating the collection of information, drones offer a cost-efficient way to cover a lot of ground.

When investigating an accident, dozens of man-hours are saved with aerial support as difficult terrains are easily traversed and unsecure areas can be investigated by insurers, without having to physically reach them.

GROWING DEMAND

According to Tor Andre Breivikås, Head of Task Force Intelligence in If's Investigation Unit, "The use of unmanned vehicles such as drones (air), robots (land) and ROV (subsea) has increased in recent years. In particular, we have seen a growing interest specifically in large industrial, commercial and private claims, as well as in investigations where there is a special need to document and collect the facts. If P&C Insurance is most commonly utilising drones,

UAVs have proven to be very versatile, for example when inspecting sites with environmental impacts. Flying over landslides or flooded areas, drones can capture 360-degree video, still images and more. When equipped with sensors, they can be used to measure various parameters, such as heat, or collect data for 3D modelling.

GETTY IMAGES

robots and ROVs in Norway, however we also see that Sweden and Finland have started to use drones in various cases."

Tor Andre Breivikås explains that typical cases with very successful results are in connection with major fires and natural disaster events. "Within investigations, the use of drones and robots has been absolutely crucial in order to be able to make the correct decision in cases related to both fire investigations and traffic incidents. If has also had the crucial benefit of drones entering dangerous areas that are life-threatening to enter."

"The use of drones and robots has taught us, that they not only provide very good, high-resolution images from any position or angle, but a drone can also be used to map terrain, buildings and areas. The collected data can then be used to create completely fresh and up-to-date maps and 3D models."

As noted earlier, advantages go beyond high-resolution images. Tor Andre continues, "drones can also be mounted on other types of sensors such as thermal, IR or gas sensors to detect heat leakages or dangerous gas concentrations, they can also be used to transport objects from A to B, or we can use a robot to pick up or deliver an object where it is not possible or justifiable for one human to enter."

DRONE EVOLUTION

Drones are commonly operated by service providers who are highly specialised experts, that can conduct demanding operations with UAVs that carry the latest technologies. According to various sources, this market is expected to exceed 50 billion euro by 2025. Meanwhile, UAV technology continues to evolve at an accelerated pace. While the early UAVs featured a basic remote-control solution with a fixed mount camera, the latest technologies include automated operation (e.g. take-off and landing) and safety modes, full autonomy and more. Smart drones today include safeguard mechanisms and self-monitoring functionalities, with added safety and efficiency features.

Sustainability report 2020 published

We are committed, together with customers, employees and partners, to constantly develop our sustainability work.

Some of the sustainability issues If focuses on are strongly connected to each other. Therefore, the originally defined sustainability issues have been summa rised into five key sustainability issues: Climate; Supply chains and materials; Work environment; Diversity, equity and inclusion; and Responsible business practices. These sustainability issues and focus areas define If s sustainability work and form the basis of the Sustainability report 2020.

You can download and read the whole report by scanning the QR code.

Short news

Manage Motor claims in If Login

Clients can now benefit from digital claims handling efficiency also for Motor claims in If Login.

The If Login claim service was first introduced in 2019 for Property, Liability and Marine Cargo. Now we have added Motor to this service. We are committed to providing a user-friendly and transparent claims handling service, where everything is available in a single view. For more information, watch our digital claims handling video at *if-insurance.com/iflogin*

Reader Survey 2021 – we want to hear from you!

This year, the Editorial team of Risk Consulting would like to hear from our subscribers and readers of the magazine. Please take a few minutes to complete the survey by scanning the QR-code and let us know how we are doing!

Appointments

Mark Welsh
Head of Employee benefits UW, Norway

Kristian Møller Smidt
Head of Sales, Denmark

Tomi Pursiainen
Network Manager, Finland

Anne Lautamäki
Employee benefits Underwriter, Finland

Lasse Otzen
Account Executive, Denmark

Brita Palmu
Network Manager, Finland

Ghita Meyer Lagouarde
Nordic Head of Casualty underwriting and Risk management, Denmark