RISK CONSULTING

IF'S RISK MANAGEMENT JOURNAL 2/2019

Climate change impacts preparedness

Anything but 'business as usual'

NO MATTER WHERE you look, the business landscape across many industries is becoming increasingly turbulent and complex. Depending on the industry, operating landscapes are changing, or have already changed, however clients must be able to grow and build for the future.

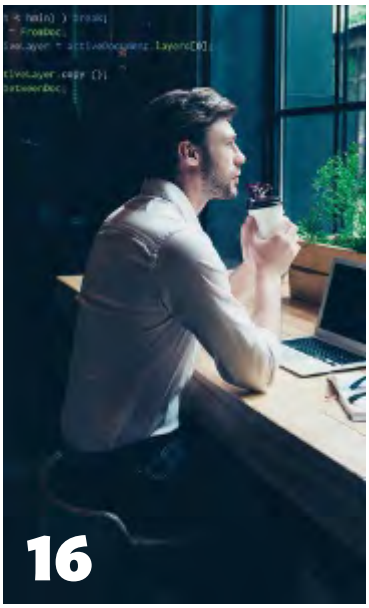
Today it is clear that 'business as usual' is anything but usual. Technology is enabling new services, as well as fuelling disruption across multiple industries. At the same time, these changes are coming faster, and 'speed' is becoming a new standard for what 'normal' should look like in today's competitive environment.

In this issue of Risk Consulting magazine, we take a look at the findings from a recent study from Norway on how the changing climate is impacting cities and businesses, and what municipalities can do to be better prepared for extreme weather events. We also provide insights into managing risks relating to solar panel and hydraulic oil fires. Be sure to also read what the If Login risk map can offer clients by way of data and insights into their operations around the world.

Companies need to prepare for the future, take advantage of the latest technologies, manage their external dependencies as well as consider opportunities outside of the traditional ways of working. To survive, companies need to be both resilient and flexible in order to be competitive and maintain or grow market share in a way that will future-proof their business for whatever is hiding behind the corner.

As a leading insurer, we work together with our clients, to help manage risks and support their daily operations.

POUL STEFFENSEN
Head of BA Industrial, If



If P&C Insurance, contact information

Finland +358 10 19 15 15 **Sweden** +46 771 43 00 00 **Norway** +47 98 00 24 00
Denmark +45 7012 24 24 **France and Luxembourg** +33 1 42 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 9800
www.if-insurance.com

Publisher If, Niittyportti 4, Espoo, FI-00025 IF, Finland, +358 10 19 15 15, www.if-insurance.com **Editor-in-Chief** Kristian Orispää **Project Editor** Carita Hämäläinen-Tallgren, **Production** A-lehdet Oy, **Printing** Forssa Print, **Changes of address** industrial.client-service@if.fi **ISSN** 1459-3920. **Cover photo:** iStock

GETTY IMAGES

Hurricane paths difficult to predict

Recent studies show that hurricanes are becoming increasingly dangerous, as it is becoming increasingly common for hurricanes to slow down upon landfall. Recently, Hurricane Dorian stopped for a 24-hour period in the north-western Bahamas, causing havoc as strong winds and heavy rain fell relentlessly over the Abaco and Grand Bahama islands. Spinning at speeds around one mile an hour at its slowest, Hurricane Dorian's next move became difficult to predict. In fact, according to the NOAA, North Atlantic tropical cyclones are slowing down on average by some 17% compared to their average speed of 11.5 mph in 1944.

In related news, in the United States, hurricane season is expected to extend into October, while previously the peak of hurricane season came in late August, early September.

New Editor for Risk Consulting

Risk Consulting magazine has a new editor, as Kristian Orispää joins the publishing team. With some 20 years' experience in external communications, Kristian has previously worked in oil & gas, as well as technology and IT industries in various communications and editorial roles.

Board oversight increasingly important

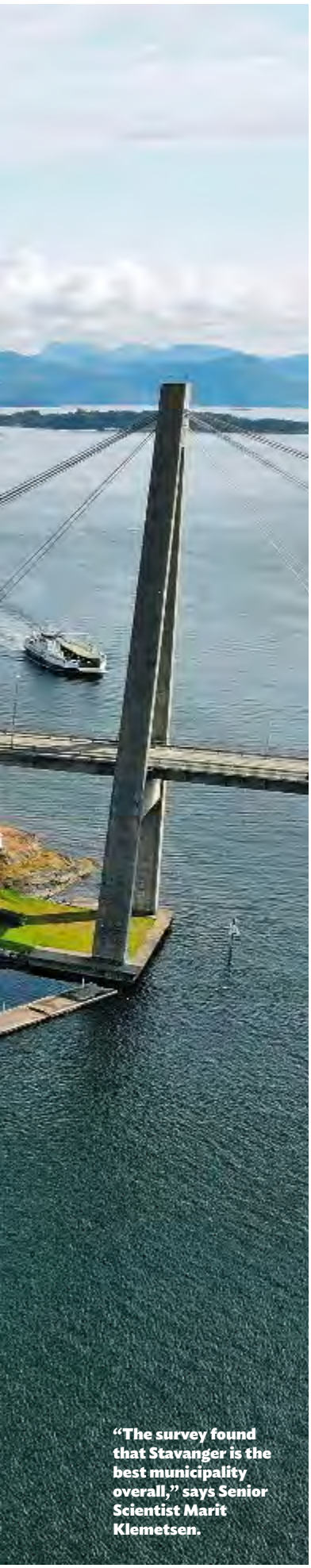
Board members play an increasingly important role in risk management and actively participate in the processes relating to the monitoring of strategic risks. Having visibility into strategic processes from a risk awareness perspective will help board members to prepare and act swiftly when risks materialise.

83%

Technology is transforming third-party risk management

Gartner researchers found 83% of organisations that work with third parties have uncovered third-party related risks after due diligence reviews. Technology is changing the way third-party risks are assessed. For example, understanding IT security vulnerabilities is increasingly critical. Such external dependencies can in fact lead to crippling business interruption risks.

ISTOCK



"The survey found that Stavanger is the best municipality overall," says Senior Scientist Marit Klemetsen.

Are Norwegian cities prepared for extreme weather?

A large survey carried out by If P&C Insurance in Norway, together with the CICERO Centre for Climate Research has found that Stavanger is the country's best climate-adapted municipality.

According to data from If, over the past eight years more than NOK 10 billion has been paid for damages following torrential rains in Norway. Putting this into perspective, there were 19,543 claims between 1990–2000. However, there were 67,009 claims in the following decade (2000–2010) relating to water damage caused by heavy rains to buildings. Over the last nine years, there have been 158,298 such claims. This increase is significantly higher than that of water damage in general.

Data tells the story of a changing climate

"We have investigated how well-prepared Norwegian municipalities are for extreme weather, which climate researchers believe will be increasingly common in the coming years. Although many municipalities did well, far too many have not started in this important work," says Ivar Martinsen, Executive Vice President at If.

"Although many municipalities did well, far too many have not started in this important work."

Through a comprehensive questionnaire, municipalities across Norway responded with regards to what they are doing to prepare for a wilder and wetter weather climate, which results in an increased amount of damage. The result of this study was gathered into a report: Hvor godt er norske kommuner rustet til å håndtere følgene av klimaendringer ("How well-prepared are Norwegian municipalities to deal with the consequences of climate change").

99 municipalities participated

Working together with the CICERO Center for Climate Research, in collaboration with the IVL Svenska Miljöinstitutet, the survey uncovered how well-equipped Norwegian municipalities really are to deal with the consequences of climate change.

The objective has been to guide and inspire Norwegian municipalities to get started on the increasingly important climate adaptation work, to secure both the municipality's residents as well as protect business activities.

While Stavanger scored best overall, Nedre Eiker was ranked the best among municipalities that had between 20,000 and 50,000 inhabitants. As for medium-sized municipal- →

ities, Nord-Odal came in first place, while Sirdal municipality was best among small municipalities.

In total, 99 municipalities responded to the survey, reflecting almost 50% of all the inhabitants of Norway.

Extreme weather experience counts

"There is a clear trend in the survey that those municipalities that have been exposed to extreme weather are far more aware about the need for being prepared for extreme weather events in comparison to municipalities that have so far been spared from such incidents," says CICERO Senior Scientist Marit Klemetsen. "This means that many municipalities only take action when they are hit, and do not work preventively."

"The most common extreme weather event is increased rainfall."

Ivar Martinsen states, "we believe that the key to safe communities lies with the municipalities. We hope that the answers in this report will inspire those who are not prepared to adapt, so that even more municipalities have started to create plans and develop their preparedness when we complete this survey again next year."

Climate adaptation measures can range from technical efforts (such as water and drains), to administrative actions (such as guidelines on locations where building permits are issued) and so-called 'blue-green' measures (such as green lungs, wetlands and water levels to avoid increased rainfall).

Preparedness demands recources

The report shows that there are significant differences between large and small municipalities, specifically major municipalities have come much further in their climate adaptation efforts.

Municipalities that have fallen short in their work, including several smaller ones, should increasingly seek help and information from central authorities to prepare for extreme weather. Both expertise and advice, as well as resources, are needed for them to be able to safeguard their communities.

"At the same time, municipalities facing similar challenges should also work together to a greater extent," says Marit Klemetsen.

A total of seven out of ten municipalities in the comprehensive municipal survey state that they have already experienced extreme weather events over the past ten years. The most common extreme weather event is increased rainfall, in fact 70 per cent have been affected by this.

"On the negative side, it is disappointing to see that large municipalities such as Oslo and Bergen have not progressed further in climate adaptation work. One would think that, for example, torrential rain and subsequent costly damages should have led to increased focus on preparedness, but this has not been the case," says Martinsen.

The study shows that there are 11 municipalities ahead of Oslo, which ranked number 12 in the survey. Meanwhile, the municipality of Bergen came in 19th in the climate report results.

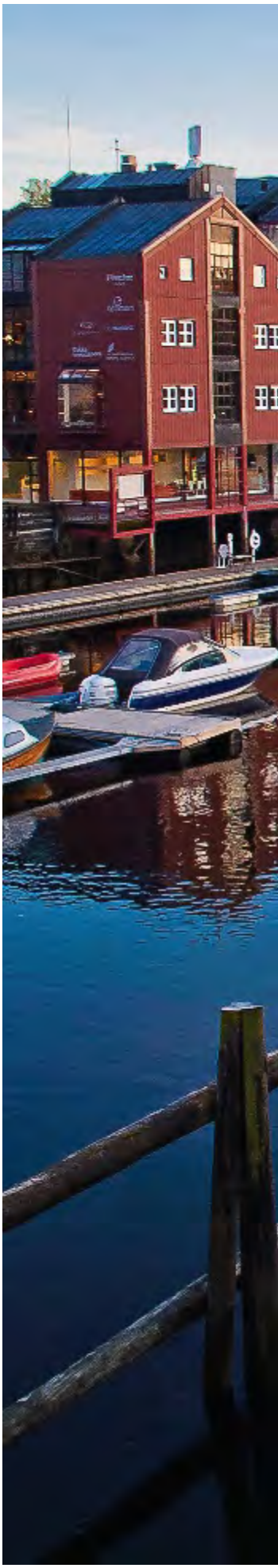
The climate will continue to change

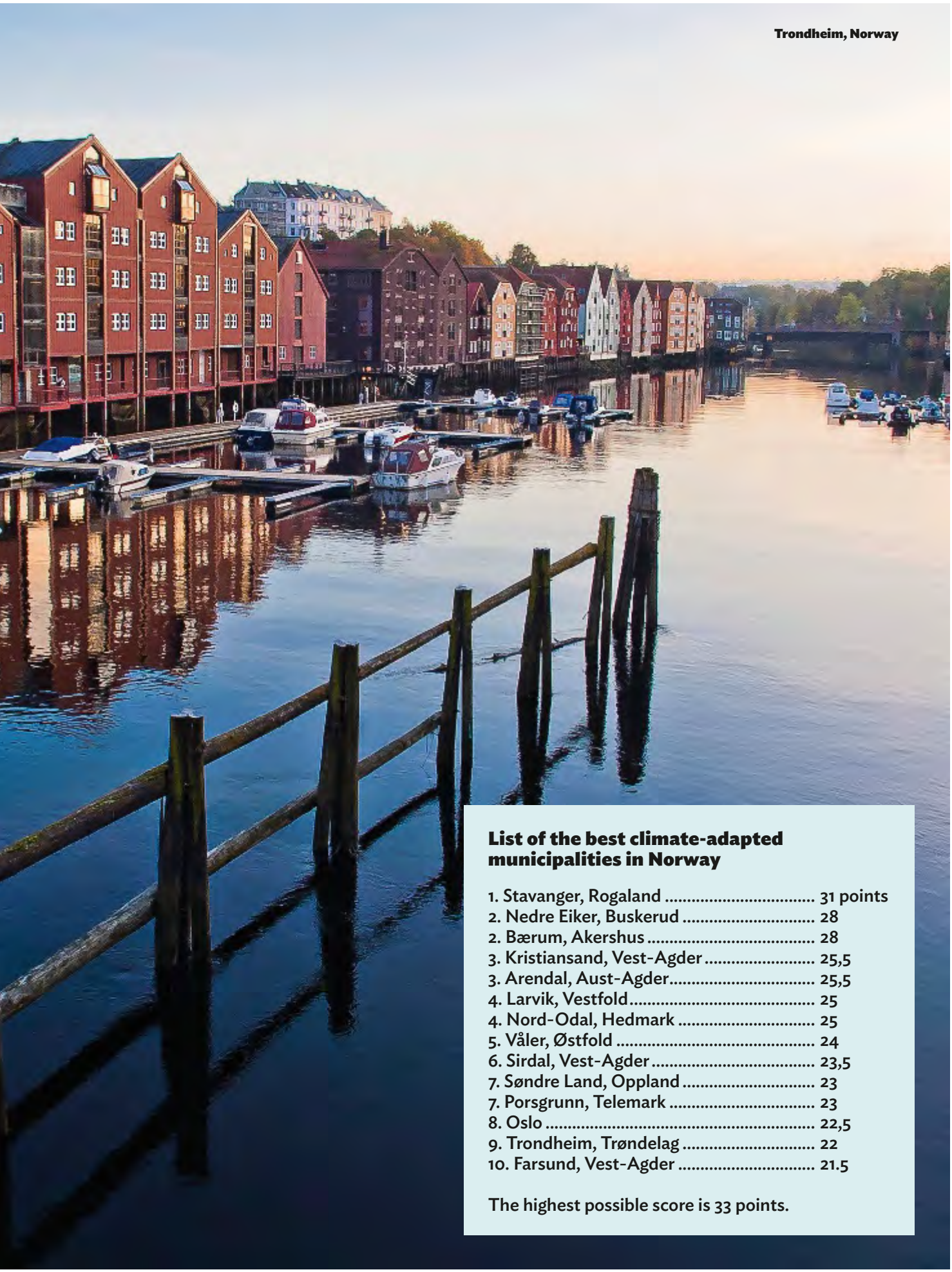
According to another report from CICERO and Western Research in Norway, the country is likely to experience even more heavy rainfall, as well as be impacted by rising sea levels with more landslides and floods expected. In light of these predictions If Industrial, together with CICERO, is seeking to raise awareness on the needs and challenges Norwegian municipalities will face in the future.

In the end, four out of ten municipalities achieved such a low overall rating in the assessment, that this may indicate they have only just begun the climate adaptation work.

As Ivar Martinsen concludes, "It is also important to point out that extreme weather is not just about roads that collapse, or stores that are damaged by water flooding into the building. It is about the safety of the community."

Read the full report at: https://www.if.no/om-if/barekraft/klimatilpasning (available in Norwegian)





Trondheim, Norway

GETTY IMAGES

List of the best climate-adapted municipalities in Norway

1. Stavanger, Rogaland	31 points
2. Nedre Eiker, Buskerud	28
2. Bærum, Akershus	28
3. Kristiansand, Vest-Agder	25,5
3. Arendal, Aust-Agder	25,5
4. Larvik, Vestfold	25
4. Nord-Odal, Hedmark	25
5. Våler, Østfold	24
6. Sirdal, Vest-Agder	23,5
7. Søndre Land, Oppland	23
7. Porsgrunn, Telemark	23
8. Oslo	22,5
9. Trondheim, Trøndelag	22
10. Farsund, Vest-Agder	21.5

The highest possible score is 33 points.

GETTY IMAGES

Preventing solar panel fires

The changing climate, the demand for renewable energy sources, and the call to action for individuals and companies alike to take a stand for greener solutions, have fuelled the exponential growth of solar cell technology around the world.

When properly installed, used and maintained, solar cell technology is an incredible solution. Utilising an infinite power source, solar power is helping people make the transition to a cleaner and greener energy source to run their homes, cars and a plethora of devices without sacrificing the standards and comforts of modern-day life.

Recently, media outlets from Japan to Norway have raised questions around fire safety and solar panels. Even when fires occur for reasons unrelated to solar panels, these modules can in fact play a role in both the intensity and speed of a spreading blaze.

A 2018 UK government report, which investigated 80 solar panel fires in the country, found that 58 instances were caused by the photovoltaic system itself. The study notes that some of these fires took place in buildings, while just six occurred on solar farms. In total, these incidents resulted in over a dozen injuries and three fatalities. The report concluded that 38 instances escalated to 'serious fires' however only 22 of these were directly caused by the solar panels. Furthermore, the majority of these fires originated in DC isolators with "the most likely cause of fire as electrical arcing". Electrical arcing is the electrical breakdown of a gas that produces a prolonged electrical discharge leading to combustion. Effectively, the fire will start by a live wire sending electricity into the air. The temperature of an arc flash can reach several thousands of degrees Celsius.

Renewable technologies carry risks

According to Anders Rørvik Ellingbø, Head of Risk Management Norway at If Insurance, "generally, one expects that purchasing high →

1. UK government report, "Fire and Solar PV Systems, Investigations and Evidence", was prepared in May 2018 and released by the Department for Business, Energy & Industrial Strategy (DBEIS).

quality solar panels will mean lower maintenance costs and better overall efficiency. Buying from a reputable brand owner commonly will ensure reliable installation, spare parts availability, user training, as they seek to protect their business, brand and customer base. This can be seen for example in the robustness of cables and components that better withstand regular wear and tear, reducing the probability of failure."

Buying an expensive system alone will not bring sufficient protection, for example installation plays an important role. From a fire safety perspective, using non-combustible materials between the panels and the roof will help to create a slight buffer, similarly coupling connections need to be covered securely, to keep the fire from escalating quickly. Anders notes that, "non-combustible plates can mitigate somewhat, but if the fire and temperature accumulate then this is not enough, so we also recommend using non-combustible insulation, (e.g. mineral wool) to help mitigate the spread of fire. This has been proven in tests completed by If Insurance with clients."

"Building materials are evolving, and new techologies provide smart solutions."

Another recommendation is to install a shut-off switch to disconnect the solar panels from the electrical system. This will not de-electrify the panels, however in case of emergency, shutting off the power will help firefighters manage the fire.

To date, most research in the area of solar panel fires has focused on rooftop installations, with very little research having been done with façade installations. It is important to understand that the challenges are not the same, however.

"Regularly panels are mounted on the roof, where the accumulation of heat radiates back down to the roof, leading quickly to increased temperatures. The role of insulation is also significant here. If the façade features combustible installation, the fire holds a risk of spreading across the entire wall, due to possible chimney effect behind the panels. Use of combustible materials in the vertical construction, i.e. wood, combined with combustible insulation will dramatically increase this risk."

Industrial scale solar panel installations

From an industrial perspective, businesses are generally very focused on fire safety, adhering to local standards and guidelines. Companies also invest in training their personnel to maintain and use solar cells effectively. Anders explains that, "it is critical to understand the fire safety related issues when making decisions to install extensive energy efficient solutions, many of these technologies are new and with that comes new challenges."

Globally, China has the largest number of solar power plants, reaching a capacity of some 80GW. This is twice the number of the installed base in the United States.

"Many of the world's solar panels in use today feature old technology, and this existing installation base is aging quickly. All mechanical equipment deteriorates over time, which means there is an increased fire risk in older panels. For this reason, regular inspections and proper maintenance completed by qualified personnel are important to ensure fire safety," Anders states.

Simultaneously, building materials are evolving and new technologies are providing smart solutions for businesses and homeowners alike. More research is needed to truly understand these from a fire safety perspective.

"Digital solutions, both in private smart homes or in industrial scale properties also raise some questions. For example, cyber risks include several barriers that must be protected to ensure that these systems are functioning in a reliable and secure way. When extinguishing systems are dependent on sensor technology, the connection between these systems are key components of the smart home or office. There is a risk that these can be hacked or malfunction due to software errors."

Clean technology challenges

In May 2019, the Research Institute of Sweden (RISE) released the results of two studies relating to fire safety challenges with solar cells and photovoltaic technology. Some of the most important findings were on the ignition, spread and fighting of fires. These included for example the age and condition of installed solar panels and the possibilities of malfunctioning as a cause of fire. The studies include recommendations to minimise the use of combustible materials as roof covering beneath solar panels to stop the spread of a fire. Firefighters need to be equipped with the correct training when battling a fire that involves photovoltaic systems. As an example, the report found that there must be adequate distance between the solar panels. According to Laura Rastas Jansson, Head of Property Risk Management at If Insurance, "Clean technologies are important new developments; however, they may also bring new types of risks. For pioneering technology companies to be successful in the long run, they need to properly identify and mitigate the potential risks, preferably sooner than later."

"We at If want to be proactive and support our clients in managing these future risks together," Laura highlights. "We can do this for example by cooperating closely with our clients, as well as by participating in research projects, in cooperation with universities and other expert organisations to better understand the risks associated with solar panels."

Understanding the risks

Beyond the obvious issues with using water to extinguish electrically charged panels, roof cavities also trap heat. During a large fire event, commonly in commercial and private dwellings, the fire brigade will seek to create openings in the roof to 'ventilate' the building. With solar panels installed across the rooftop, it can be more difficult to execute this activity.

2. *Source: International Energy Agency market analysis, "Renewables 2018" https://www.iea.org/renewables2018/*

GETTY IMAGES

GETTY IMAGES

Protecting your industrial control systems from cyber risk

It is important to understand that hacking of Industrial Control Systems (ICS) may cause injuries, loss of life, material damage or business interruption. A Denial of Service (DoS) attack or a ransomware spreading across your organization can make production systems unavailable or misbehave.

Industrial Control Systems are most typically found within manufacturing and utility production, but similar challenges exists in other embedded systems. Examples can not only be found in utility companies or the manufacturing industry (PLC, DCS, SCADA) but also in retail, logistics, healthcare, etc. Consider for example the use of Building Management Systems (BMS), Warehouse Management Systems (WMS), Medical Scanning Devices (MSD), or common equipment such as elevators, locking systems, domestic heating, air compressors etc. All this equipment is vulnerable to cyber-attacks if connected to a network for example for reporting, controlling or updating.

It is important for all of us to understand the risks of our industrial control systems and the obligation to build and operate them in such a way that they offer maximum protection against an attack.

"We have been studying industrial control systems for several years now."

As an insurance company we have been studying ICS risks for several years now. Recently we have seen many incidents at major industries resulting in large losses, adding up to hundreds of millions. Hereby malicious software gained access to the business network and encrypted all data. More sophisticated versions made an inventory of all data repositories including on-line back-ups first, before starting their destructive work. Without their data victims were paralyzed, and their options were limited to paying the ransom and hoping for the best or re-building their →

systems from scratch using off-line backups, if available.

Because ransomware can spread rapidly, a global company network could be affected within minutes. So far, the preferred response has been to cut all connections, effectively shutting down the network. And in today's world, enterprise resource planning systems are key and without them business operations are impossible. Even when industrial control systems are not compromised themselves all activities will stop sooner or later as in manufacturing plants production numbers and demands for raw materials are no longer processed. In hospitals, patient data is no longer available and findings can't be reported. In distribution centres it's no longer possible to find pallet locations, to print address labels or to complete forms for customs. However, with the ICS themselves not being compromised they will operate as planned. They would shut down safely without physical loss. In the insurance business this is therefore commonly referred to as non-physical risk.

However, the hacking of ICS is considered a physical risk as it may result in injuries, loss of life or material damages! Examples are less known to the general public and include events such as hacking into the controls of a New York dam (2013), setting a German steel mill on fire (2014), breaking down the Ukraine power grid (2015), compromising the safety of a refinery in the Middle East (2017), and the attacks on the Russian power grid (2019). These examples may seem a little extreme for an average organisation as they involve state-sponsored hackers and high-profile targets. But make no mistake! As it happened with malware targeting common IT systems we have no doubt that the tools used in the above attacks will trickle down and become available for use by common criminals.

For ICS, integrity is key! Processes must be completed in a strict order depending on input provided by sensors. Users can select the order required using a Human Machine Interface (HMI). For example, a manufacturer of paper cups will have a strict order for producing their cups, which should always have the same appearance. Should they want to produce another product they must select different parameters. Within the production process the users may have a bandwidth to adapt the process because they are using a raw material that may differ in quality. However, the ICS will control the upper and lower limits to prevent, for example, overheating.

"For ICS, integrity is key!"

When we visit organisations as part of our risk management surveys we find that automated solutions are replacing part of the human workforce. This takes away the possibility for human intervention in case the process order is disrupted. We also see a lot of system integration. Where we used to have multiple machines on multiple lines, today a single more complex machine is combining their activities. With the equipment becoming more complex, the number of people understanding them is reducing. Finally, we see that safety systems, which used to be independent (mechanical) devices, are moving along the same lines and sometimes are even merged with the very systems they are supposed to protect!

We recommend

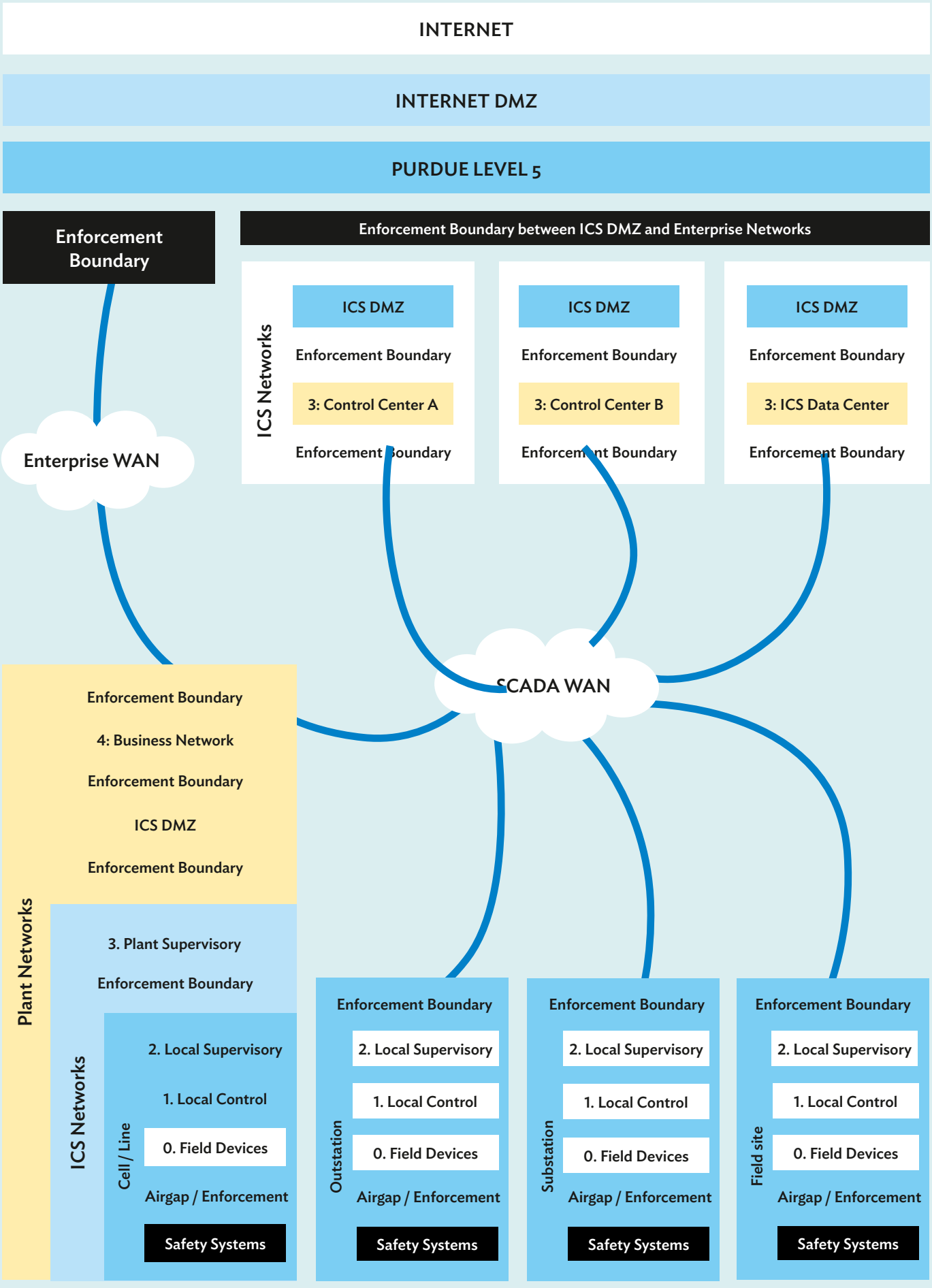
- When working with connected ICS make sure the control network infrastructure design addresses cybersecurity. For an example, please see SANS ICS 410 illustration.
- Make sure you know what equipment is connected, what software you're running and keep your access control up-to-date with access granted only on a need to know basis.
- Assess vulnerabilities in ICS systems regularly by scanning assets for vulnerabilities or conducting a penetration test on networks.
- Back up all key systems regularly and store at least one recent, complete, backup set in a remote site.
- Consider deploying an ICS-aware Intrusion Detection / Prevention System (IDS/IPS) or Next Generation Firewall (NGFW) to gain visibility and control on your production network segments
- Protect critical information in your ICS from unauthorized access and keep off-line copies and backups.
- Create visibility of your network and maintain routines and capabilities to act in case of a disruption.

To protect your organisation from future cyber-attacks causing loss of life or material damage we believe it is very important to keep a grip on the matter. We propose you start asking the below questions;

1. Are our operations dependent upon the operation of machines or equipment connected to IT systems or networks?
2. Could a disruption or manipulation of our operations' IT systems or underlying networks result in loss of life or physical damage to our products, goods, machines or facilities?
3. Are our operations' IT systems connected to the company network or accessible remotely over internet by employees or third parties?
4. Have we conducted a recent security test of our operations' IT systems and associated network connections?
5. Could a disruption or manipulation of our operations' IT systems or underlying network result in any form of business interruption? ■

ERIK VAN DER HEIJDEN
Senior Risk Engineer

SANS – ICS410 REFERENCE MODEL



How your employees can help prevent cyber-attacks

Cyber-attacks can cause serious business disruptions. Your own employees play an important role in fighting cyber threats every day. Unfortunately, employees often fail to consider why hackers might want to target them.

Today, attackers often carefully profile the employees of the company they are targeting. This is done for example through social media and by researching publicly available information. Once a target has been selected, one of the most common ways to execute a cyber-attack, is to send phishing e-mails directly to employees in a targeted company. These emails usually contain either a link or a Microsoft Office document embedded with malicious code. Thus, employees can unintentionally help cyber-attackers break into an organisation.

Phishing emails are tailored to the recipient as meaningful and interesting. The emails can appear to be genuine, triggering victims to click on a link or open a document on their work computer. This action could lead to a web site designed to lure the UserID and password from the victim or release a computer virus or program and allow attackers to control their computers remotely. Usernames and passwords can then be easily hijacked by installing malicious programs that log all keyboard events.

What are the warning signs?

When it comes to phishing emails, it is important for your employees to be wary of emails or phone calls from unknown persons requesting them to act. These can be requests to provide information or open attachments in an email. Be vigilant and consider the following factors if you are unsure how to act in these situations:

1. Does the sender's e-mail address look legitimate and is the content of the message well-written (e.g. using proper grammar) and logical (e.g. featuring a reasonable objective or statements)?
2. Does the message contain an attachment or link?
3. Does the sender ask you to take immediate action or take action in one way or another?

Be careful not to use the same passwords across multiple platforms. This is common practice among people however it is also a serious risk, making things much easier for hackers.

> **"Phishing emails are tailored to the recipient as meaningful and interesting."**

How your IT-security team can help

Keeping up-to-date on the most recent threats is vital to enforcing a secure environment. Security awareness actions and training of employees are just as important. Raising awareness among employees for example through webinars, on-site events, as well as proper onboarding of security policies, training manuals and pamphlets, refresher trainings for existing employees, as well as regularly producing intranet articles on IT security topics and practices.

IT security teams are also responsible for ensuring the robustness of the corporate network. This includes implementing of new technologies such as Multifactor authentication (MFA). This requires at least two separate verification methods to authenticate the user's identity in order to login to their account.

Know your vulnerabilities

Invite your different business area, project and product line management teams to consider their vulnerabilities. What is the confidentiality level of the material they are using and how is this information used by employees? For example, it may be common practice in your company to use online services to share material, send large files, translate information into local languages, or host meetings. It is important to remember, that these services can pose a serious security risk.

It is important to understand the terms and conditions of any online service that is being used by your employees.

As an example, translating sensitive information using a free online translation service may risk the release of critical details to hackers. This can include information that may impact stock price, jeopardize joint venture agreements, or otherwise compromise confidential information.

Consider the following:

- How is the online service provider managing the information your employees send and receive on their platform?
- What rights does the online service provider have to this information?
- What are they doing to protect your information from cyber threats?
- What happens if the service providers data is compromised, who is liable for possible damages?
- How robust are the security measures the online service provider has in place?

Every day, your employees can provide an important line of defence against potential attacks or be your weakest link in the fight against online threats.

To successfully fight cyber-crime, your employees need to know what they are looking for - as only recognised risks can be managed.

"Patching human vulnerabilities through security awareness training is just as important as patching technical vulnerabilities," says Peter Granlund Chief Information Security Officer at If P&C Insurance. ■


var perc = 99.0, wmin = 1920, hmin = 1080, w, h, w1, h1, ratio;
var FromDoc = open (File ("D:\FromMacro.psd"));
var IntoDoc = open (File ("D:\IntoMacro.psd"));
app.preferences.rulerUnits = Units.PIXELS;
w = FromDoc.width.value;
h = FromDoc.height.value;
ratio = h/w;
app.activeDocument = FromDoc;
activeDocument.activeLayer = activeDocument.layers[0];
var shapeRef =
[[Math.floor ((w-1920)/2), Math.floor ((h-1080)/2)],
[Math.floor ((w-1920)/2)+1920, Math.floor ((h-1080)/2)],
[Math.floor ((w-1920)/2)+1920, Math.floor ((h-1080)/2)+1080],
[Math.floor ((w-1920)/2), Math.floor ((h-1080)/2)+1080]];
app.activeDocument.select (shapeRef,SelectionType.REPLACE);
app.activeDocument.selection.copy ();
app.activeDocument = IntoDoc;
activeDocument.activeLayer = activeDocument.layers[0];
IntoDoc.paste ();
while (1) {
if ((w < wmin) || (h < hmin)) break;
app.activeDocument = FromDoc;
activeDocument.activeLayer = activeDocument.layers[0];
app.activeDocument.activeLayer.copy ();
app.activeDocument = betweenDoc;
betweenDoc.paste ();
w1 = w;
h1 = h;
w = w * perc / 100;
h = w * ratio;
}

Understanding external dependencies

In this issue of Risk Consulting, we take a look at external dependencies, focusing on third-party factors from outside of the company. Dependencies on suppliers and partners, or any other parties outside the company can be impacted by perils such as fire, machinery breakdown or natural hazards, which can have an impact leading to serious business interruption, losses and increased costs.

Defining external dependencies

External partners are considered to be companies, service providers or other stakeholders supporting the client in delivering their business products and solutions to the market.

Be aware, the insurance industry uses a variety of terms to refer to the same things, these include but are not limited to e.g. unnamed and named dependencies, contingent business interruption, as well as first tier or multiple tiers insurance.

Tiers below 1st Tier (supplier's suppliers) are not commonly part of the insurance program and are considered on a case by case basis.

It is common for companies to be dependent upon some suppliers directly, sometimes these can be combined into one category, for example Public Utilities (water, electricity and data), Named Supplier´s and Customer´s, etc. Another example is Denial of Access, where no physical damage has occurred at the insured location, however there may be business interruption losses due to other circumstances (e.g. inaccessibility to premises due to fire in a neighbouring facility).

As an example, finding a secondary supplier may be more expensive, may have an impact on the quality and can cause possible delays in production and/or delivery. In the worst case, this can lead to a loss of market share or even bankruptcy.

External dependency claims are commonplace

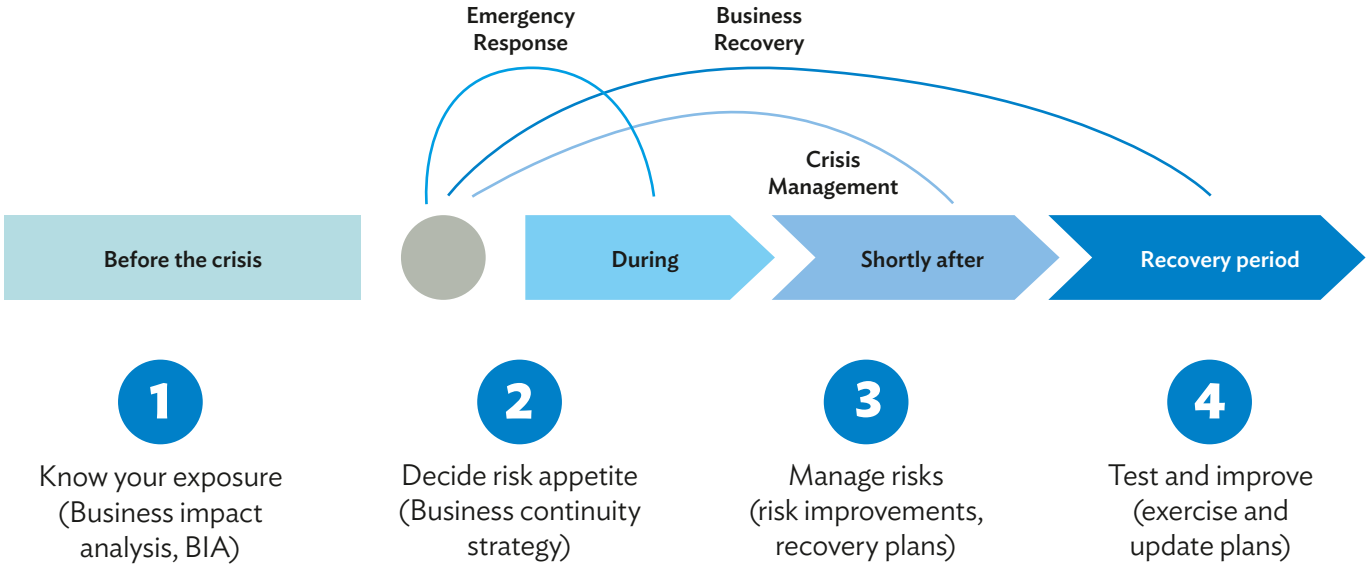
As companies manufacture increasingly complex products, they also require more and more levels of suppliers. In addition to this, lean production methods enable cost savings by way of on-demand production, reducing the size of inventory and

GETTY IMAGES

Contact If, for a copy of the Business Continuity Planning quick guide.

Business Continuity Management (BCM)

Business Continuity Management consists of three parts: Emergency Response (ER), Crisis Management (CM), and Business Recovery (BR).



therefore cutting the stocking of products which in normal situations will save costs in the short-term. However, the downside to this is that in case of a serious business interruption when production is impacted, there can be an immediate consequence by way of suppliers and companies having an insufficient amount of products available in stock to fulfil orders.

External dependencies can also play out as a chain reaction. Delays and issues with one supplier can have a ripple effect across the entire market. In cases where a few suppliers are maintaining the availability of specific components or resources to support production, there is little room for interruptions. When these basic materials or services are not available, the impact of this shortage can be substantial.

Insurance solutions to help manage risks

Insurers must estimate what could be the 'worst case scenario' in the case of a claim. External dependency issues are often more expensive and take longer to process, when comparing with interdependencies that occur within the Group. This is due to not having direct access to all parties involved which can delay the initiation of loss mitigating actions.

To keep up to date with external dependencies, it is recommended that a thorough business continuity management plan is in place. This should be regularly updated and maintained to stay on top of potential Business Interruption risks coming from external partners. Following a thorough assessment, you are better positioned to face possible external dependency losses. Only then can mitigating these risks begin in earnest.

Examples of reducing single source supplier dependencies are:
– deep collaboration with your network
– continuity planning
– diversifying customer network

Consider the following:

- Who are your most critical suppliers from a business continuity perspective?
- What are the financial implications of these relationships?
- How much of your suppliers' capacity does your normal order account for?
- Are you an important customer to your supplier?
- Are you using single source supplier strategy?
- What is the likely duration of the interruption in potential scenarios?
- Do you have knowledge of alternative suppliers, if your current suppliers are not able to deliver on-time or up-to-standard quality products, raw materials and/or services?
- In case you need to change the supplier, what certifications are required by relevant authorities and how long will this take to complete?
- What can you do now, that will improve the risk standard in critical processes?

When you understand the risks, know their potential financial implications, and have plans in place to mitigate these, a clear and transparent starting point will support discussions on selecting the right insurance solutions for your business.

Preparation is key to managing business interruption risks

At If, external dependency effects can be included in a business interruption solution for your company. When both parties understand the types of risks we mutually face, we will be able to serve you better, offering the solutions that best meet your specific business needs. We seek to understand the risks and we write the risks we understand!

JUHA JANTUNEN
Property Underwriter

ISTOCK/IF

All-in-one view

The natural hazard map in If Login is a game-changer

At If, we continue to add valuable functionalities, share more data and improve the usability of our online services through continuous development efforts.

The new risk map in the If Login client portal now highlights natural hazard risks from around the world.

The updated map brings value to the users providing them with the possibility to see all the risks that may impact their company's various sites and locations in a single map. As an example, the map now helps users see how a specific location can be exposed by floods or earthquakes. By coupling the data relating to natural hazards with that of our client's insurance solutions, we can offer a world map view, through the customers eyes.

Preventive risk management

Known natural hazard risks affect both the availability of cover and pricing of insurance solutions. It also helps customers to plan and develop preventive risk management actions to help prepare for any such hazards, should they materialize.

The purpose of the added functions in If Login is to increase awareness and understanding of the potential risks as well as engage with clients in continuous dialogue to help them manage the potential risks.

According to Fredrik Holmqvist, Head of Risk Management, Denmark "Being prepared to prevent, respond to, and recover rapidly from natural catastrophes can save lives and protect your assets. Knowing your exposures is the first step in securing your preparedness and developing an Emergency plan and Business Continuity Plan. The hazard maps provided in If Login have proven to raise awareness about potential exposures and encourage our clients to evaluate potential risks in more detail, together with our underwriters and risk engineers. Often a site visit and the use of more detailed assessment tools are needed to get a comprehensive understanding of the overall exposure. Many of our clients have learned that emergency preparedness requires attention not just to specific types of hazards but also to steps that increase preparedness for any type of hazard."

Value-adding data

The natural hazard information is provided using the Swiss Re CatNet® Web Map Services (WMS). Clients can view all their Marine Cargo locations with storage values and Property locations with their insured sums. It is also possible to manage information concerning expatriates and their families from around the world.

We have recently also included Liability policies on the map, giving a quick view of all clients' business locations and insurances around the globe.

The natural hazard map in If Login is currently on trial.

For more information, visit the client portal today!

Hydraulic oil fires - what to look for?

The most simple and reliable way to prevent a hydraulic oil fire is to replace mineral oil with non-combustible fluid. Naturally, using electric or pneumatic drives instead of hydraulic drives will also prevent hydraulic oil fires. Although there are some fire risks related to these technologies, they are not as fierce and difficult to control as oil fires.

GETTY IMAGES

There are clear differences between electric, pneumatic and hydraulic systems. For example, pneumatic systems (shown here) operate at 8 bar pressure, while hydraulic systems operate at 200 bar.

Fluids considered to be non-combustible consist of water-based solutions, featuring less than 20% oil. Control of fluid leakages is important for several reasons: fire safety, the functionality of the machines and soil protection. With water-based solutions, however, it is important to understand that the residues are combustible, when water has evaporated.

However, the transition to water-based solutions has been slow. As this requires component changes, including valves for example, there are costs involved and thus water-based solutions are seen as unattractive. After the replacement of hydraulic oil, the manufacturer of the respective machine may cancel the warranty.

From a fire safety perspective, this would be an important upgrade to help reduce the risk of hydraulic oil fires.

How can clients understand where the potential risks are? In some situations, conditions that can cause a hydraulic oil fire will include the presence of hot surface or momentary high temperatures such as a flame or electric arc, which come in contact with pressurized oil. In most cases, such conditions can be identified at the hydraulic cylinders and motors, as well as at the hydraulic hoses and pipes at the processing line, rather than at the hydraulic pack, which can be in a segregated room or further away from process equipment.

"What are the risks?"

Understandably a hydraulic aggregate in a separate hydraulic room can catch fire although such fire losses are rare. Common causes of such fires are pump breakdowns and burning rubbish at a hydraulic aggregate.

Another loss scenario, although rare, is a pin hole leak, which creates an oil mist cloud. If this cloud is met by an ignition source which appears on the scene, the oil cloud will easily catch fire, resulting in a flash-over.

Oftentimes, insurers may simply state that if a single hydraulic system contains less than 100 gallons of hydraulic oil the consequences of an oil fire are considered low. In these cases, the priority is in the fire protection at the hydraulic unit, rather than the fire safety of the process equipment, where hydraulic oil is utilized.

There is no direct dependency between the volume of the oil tank and the severity of potential loss in case of an oil fire. More determining factors are the vulnerability and criticality of the items, which

are exposed. Almost in all oil mist fires in industrial facilities some power cables, data cables and electrical components will be destroyed. If the destroyed electrical components belong to an obsolete electric control system, the restoration of the system can be difficult. In the worst case, the old control system needs to be replaced with a fully new process control system.

To assess the consequences of an oil fire within a separate hydraulic room with no reliable extinguishing system is rather simple. If the hydraulic pack consists of standard pumps and valves with no special components, the hydraulic pack can be restored within 4 to 6 weeks. Should the hydraulic pack have tailor made servo valves and similar components, the restoration could take 3 to 5 months.

There is no simple formula, even less than 100 gallons of hydraulic oil will burn fiercely and cause damage to the unit, as well as the immediate environment in which it is situated.

Other points to consider, include:

1. The hydraulic unit itself; how expensive will it be to repair, what are the delivery times for key components, are there any tailor-made components in the unit?

2. Discharging high-pressure oil poses risk to people. Hydraulic hoses should therefore be introduced in fire protection hoses, also known as fire jackets, which must be fixed with wire rope and clamps to steel pipes to keep them in place. In the event of a hose burst fire jackets will restrain oil discharge and let it run on the floor.

3. Slowly progressing contamination of floor and soil must also be considered. Control of oil leaks is important not only from fire prevention standpoint, but also from environmental standpoint. When an old hydraulic system will be removed, contaminated concrete and soil may also be necessary to be removed and treated. The treatment of oily soil and concrete is expensive.

The use of hydraulic oil with a higher ignition temperature will not much reduce the risk of a hydraulic oil fire. Practically in all cases, the ignition source is well over 300 degrees thus overriding the fire protection properties of such hydraulic fluids. Exposed power cables and mechanical components will be damaged although the energy of the flames can be lower than in mineral oil fire. ■

EERO KANKARE
Risk Engineer

GETTY IMAGES

Consequences of aging infrastructure

Continuous monitoring and maintenance of infrastructure is critical to minimise risks and prevent losses.

Risk management, when working properly, is almost invisible. The same applies even clearer, to the modern infrastructure like roads, energy grids and pipelines. The discussion on deteriorating infrastructure has been heating up after shocking accidents like the Ponte Morandi bridge collapse on A10 motorway in Genoa, Italy last year.

Aging infrastructure needs continuous follow-up and maintenance. It is not a surprise, that the deteriorating structures will start failing at some point even without any unidentified defects in new materials. The problems arise from the long lifecycle of the infrastructure.

The accidents directly caused by failing infrastructure include serious injuries, fatalities, large property damages, not to mention lost income, reputation risk or even bankruptcy. Think about the risks involved in energy production and distribution, water management, transport like roads, ports and airports or in communication infrastructure. Consider the significance of these systems, and the impact bursting pipes or collapsing structures can have from both social and economic perspectives.

Keeping up the infrastructure and updating it in time is a persevering effort. The structures may endure 30 to 100 years and “nothing” happens, even if some measures are postponed. As financing of public installations is often done through tax money, e.g. political preferences may delay necessary maintenance actions. But this maintenance should be based on lifecycle assessment. Otherwise, the cumulative investment gap easily exceeds any funds available. Research studies show that timely actions are cheaper

than waiting for a catastrophic incident to occur first.

The risks are also constantly evolving. Digital operation and monitoring systems, such as smart power grids are taken into use while the hardware may be old. This leads to new, possibly unidentified risk exposures to societies and companies. Digitalization of earning methods and the increase of immaterial values in new business models aren't less exposed to interruptions of the common infrastructures like communication or cloud services.

But the risks aren't limited to the direct consequences. The global supply chains are ever more complex and interconnected. The business interruption risks are among the highest ranking in studies among business leaders.

Climate change and the extreme weather events require extra resilience from the infrastructure and accelerate the maintenance challenge. In October 2019 the power company PG & E started to shut down their power grid in Northern California due to weather forecast of offshore winds prone to causing wildfires – the company has been criticized of deteriorated equipment igniting fires resulting in massive catastrophe in 2017.

Similarly, companies need to implement their deteriorating infrastructure related risks into their risk management. This is nothing new. Both direct exposures and supply and delivery chain as well as IT risks have to be taken into consideration. ■

MATTI SJÖGREN
Liability Risk Management Specialist

MARKUS MESIMÄKI
Risk Engineer / FI

RIKARD SAHL
Cargo Risk Specialist / SWE

MIKKO PELTONEN
Head of Digital Risks & Cyber/Nordic

MATTIAS ROSENGREN
Risk Engineer / SWE