RISK CONSULTING

IF'S RISK MANAGEMENT JOURNAL 2/2017

Cyber risks under control

Explosion in a sprinkler control room

Positive results with training

Managing risks together 24/7

Brave new world

THIS EDITION OF Risk Consulting Journal is very much about the new world. Cyber risk, new battery technology and the use of drones are all part of this magazine.

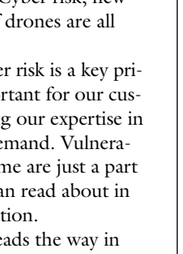
First things first: Managing cyber risk is a key priority area for If, because it is important for our customers. We are therefore increasing our expertise in this area, in line with increasing demand. Vulnerable companies exposed to data crime are just a part of this complex field, which you can read about in our in-depth article in this publication.

It's the American market that leads the way in the purchase of cyber insurance policies. On a global scale, the market is now worth around USD 3 billion, with an estimated growth to USD 14 billion in 2022 – measured in insurance premiums. The main reason for this is that policies for various types of data crime will spread to Europe and other parts of the world, as shown in a report from Allied Market Research.

Knowledge of various risks is a key factor in everything we do here at If. This is also highly applicable to battery technology. Battery fires in consumer electronics and electric cars, for example, show that we must take this risk seriously. We believe that battery technology will become increasingly important, not least in the transport sector.

Something completely dependent on batteries are drones. If has a dedicated drone group that has started to utilise this exciting technology with its customers. Recently, we visited a customer to create a 3D map with a drone. The process is very cost-effective and the map can be used to prevent damage resulting from heavy rainfall.

And while we are on the subject of climate-related damage: At the point of writing, the Irma and Harvey hurricanes have finished wreaking their havoc. If insures companies all over the world and several of our customers have been affected. When such a major event occurs, it is a timely reminder to frequently review the company's insurance policies, not least to ensure that values have been updated and the company is properly insured. Time after time we see companies receiving an unpleasant surprise after major incidents.



POUL STEFFENSEN
Head of BA Industrial, If

4 Coop wants to be challenged on threats and risks

6 When food becomes a threat

8 Cyber risks under control

10 Cyber risk controls

13 Roll-out of cyber insurance products

16 Li-ion batteries – hazards and mitigation

18 Explosion in a sprinkler control room

20 Positive results with training

23 Your data matters

24 Compliance news

26 New If RM-library – managing risks together 24/7

28 A desirable service experience

29 Drones open new perspectives within risk management

30 Hazard Info Sheets – sharing knowledge

31 Internet of things – new visions, new risks

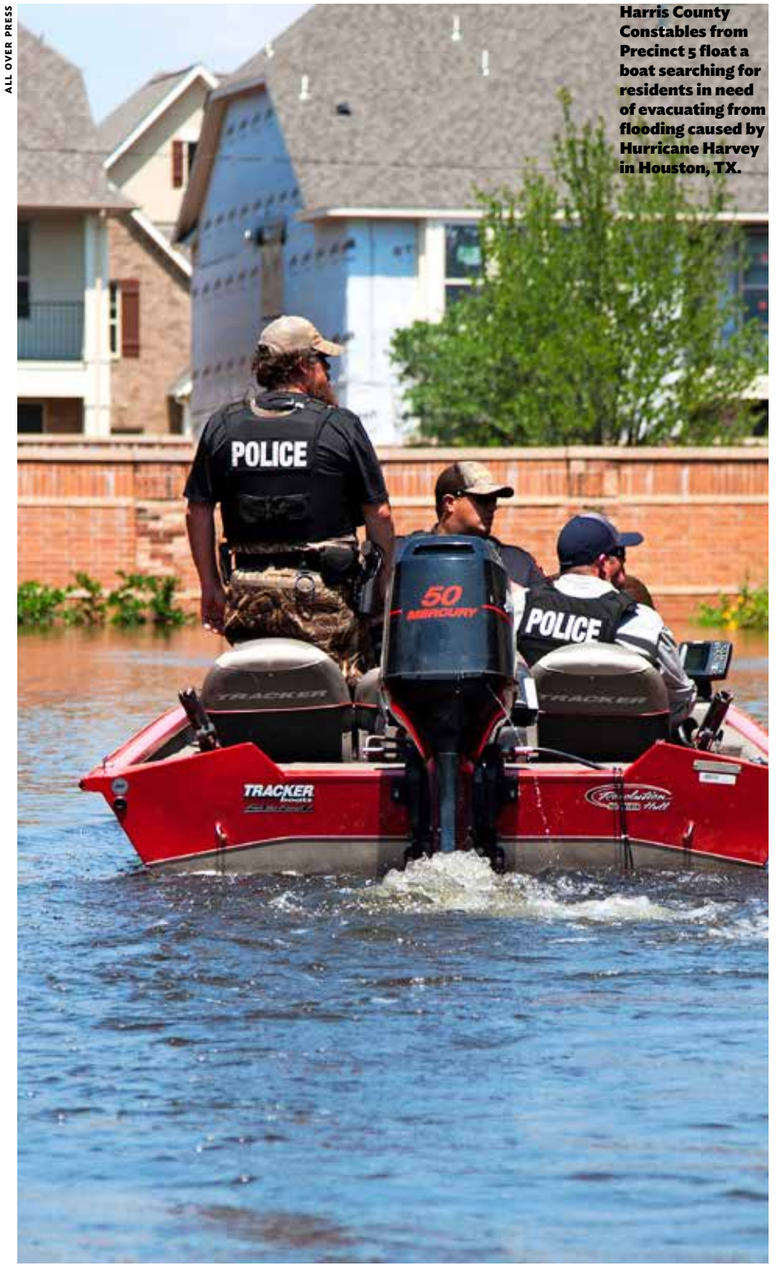
31 Appointments

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** Mats Nordenskjöld **Editorial board** Mats Nordenskjöld, Sigmund Clementz, Ken Henningson, Fredrik Holmqvist, Carita Hämäläinen-Tallgren, Laura Rastas-Jansson, Anders Rørvik-Ellingbø, Pekka Sarpila, Marianne Wiinblad **Production** A-lehdet Oy **Printing** Forssa Print **Changes of address** industrial.client-service@if.fi **ISSN** 1459-3920.
Cover photo: Getty Images **Disclaimer** This publication is and is intended to be a presentation of the subject matter addressed. Although the authors have undertaken all measures to ensure the correctness of the material, If P&C Insurance does not give any guarantee thereof. It shall not be applied to any specific circumstance, nor is it intended to be relied on as providing professional advice to any specific issue or situation.

ALL OVER PRESS



Harris County Constables from Precinct 5 float a boat searching for residents in need of evacuating from flooding caused by Hurricane Harvey in Houston, TX.

Lack of flood insurance

THE LONG-TERM DAMAGE from the catastrophic flooding engulfing the US's Gulf Coast is expected to cost companies, small businesses, and homeowners as much as $100 billion, according to Imperial Capital. While big corporations will probably survive the hit, many individual homeowners in Houston could be forced into debt or bankruptcy because they don't have flood insurance. That's despite the fact that scientists have been warning for years that unchecked development and climate change could cause severe flooding in Houston. As of August 2016, just 15% of the 1.6 million homes in Harris County, where Houston is located, had flood insurance, according to data from the Insurance Information Institute. ■

Increased cost for Italian earthquake

The Mw 6.0 earthquake which impacted Central Italy on 24 August 2016 will now cost the insurance industry €108 million, much higher than the €66 million originally suggested, according to PERILS, the catastrophe insurance data firm and reported by Intelligent Insurer. In the final loss report, the market loss data are available by CRESTA zone and property line of business. The Italian Civil Protection Agency estimates the total economic losses from the event at €7.1 billion.

No need for new liability rules for new technologies

In its responses to the European Commission consultation on the European Data Economy and the review of the Product Liability Directive (PLD), Insurance Europe said there is no need to amend current liability regimes or create specific liability rules for new technologies. This is because there are systems already in place that protect consumers against the potential negative impact of emerging technologies. For example, the combination of specific liability regimes, such as the PLD, and general civil liability regimes already work efficiently in practice for emerging technologies. Specifically, the PLD, which provides a comprehensive, extra-contractual and no-fault liability regime that protects the consumer even in cases of new technological developments, is fit for purpose and does not require amendment at this time.

Grenfell inquiry head pledges to get at truth behind cause of fire

The retired judge leading the Grenfell Tower inquiry has promised "to get at the truth" of what caused the inferno that killed at least 80 people, says Guardian. Sir Martin Moore-Bick said the fire on 14 June was "a tragedy unprecedented in modern times" and he hoped the inquiry would eventually provide "a small measure of solace" for victims' families. The hearings would provide answers to "the pressing questions of how a disaster of this kind could occur in 21st-century London". An interim report on the first phase of the inquiry – into the immediate events of the fire – is due to be published by next Easter. Evidence-taking sessions may not start before the end of the year.

Coop wants to be challenged on threats and risks

"Both Coop and I personally place great emphasis on the attitude of those people with whom we're going to work together," says Ulrik Mester, Chief Risk Officer i Coop.

Coop is Denmark's biggest food retail company. Last winter the company put most of its insurance arrangements out to tender.

With almost 1,200 stores, more than 40,000 employees and more than 45,000 article numbers on the shelves, there were certainly plenty of criteria in the tender material for a new insurance partner to satisfy. The choice fell on If.

Ulrik Mester ran the process together with the insurance broker Marsh and was involved in most of the details of the process.

"In both words and actions, If lived up to what we in Coop believe will be a favourable partnership. We place emphasis on partnerships and on having a sparring partner who can help to boost and optimise Coop. That was the approach and the attitude we met throughout the entire process, and that was one of the most compelling reasons why we switched to If," explains Ulrik Mester.

Coop adopts a serious approach to risk management and can produce a number of results in their setups to support the fact that they stand by their words.

"The fact that If has an active risk management department and a number of risk engineers is a definite advantage for me and for Coop. We believe ourselves that we do a great deal, and we're also recognised for that. But we're always open to the possibility that we might be able to do things better. There's a significant difference between being advised in advance to optimise your loss prevention and having to appear as counterparties after a potential claim.

"I welcome any push from an insurance advisor. We know our internal needs and procedures, but we're not up to date with what new kinds of cover there are or with other ways of doing things. It makes us stronger when we're challenged by the demands we make of ourselves and the way we cover ourselves," says Ulrik Mester.

He views it as his task to channel that knowledge down into the organisation and to make sure that it is implemented.

"It's absolutely fundamental that the technology has to work."

Prevention, prevention, prevention

What does a Chief Risk Officer in Denmark's biggest food retail company think about the threat level of the future?

"Well, being able to enter data in the cash tills is absolutely essential for us. So there's an enormous threat if we're suddenly unable to do that. It's absolutely fundamental that the technology has to work, so that staff can order the products they need to have on the shelves. So there are strict demands on the IT system that supports that part with regard to opening hours, data volumes and data processing, so that in-store staff can enter data into the cash tills and get a receipt out."

One constant consideration in Ulrik Mester's job is whether the current setup is safe enough. He considers fire to be one of the worst kinds of damage, and a lot of emphasis is placed on minimising risks and having guidelines, for example, for the location of cables so that they are not worn by overheating chiller cabinets, the correct location of combustible materials outside the stores, etc.

During the violent downpour in Copenhagen in July 2011, around 60 of Coop's stores were affected by water. That is difficult to prevent, but on the other hand it is the kind of damage that can be dealt with relatively quickly.

"There are few areas of cover that we haven't finally decided on yet. We'll have an extra discussion about the possible scenarios and get a very clear picture of what kinds of risk we have today, and what we can do ourselves to minimise them. And we'll supplement them if we feel that there's a need. This is where you appreciate the value of a competent sparring partner," concludes Ulrik Mester. ■

Coop in Denmark:

- Denmark's biggest food retail company.
- Coop consists of almost 1,200 stores.
- Coop has 45,000 article numbers.
- 1/3 of all food products in Denmark are sold by Coop.
- Processes more than 6 million transactions per week.
- Coop's total retail space is 1 million square metres, which corresponds to approx. 140 football pitches.
- Every year, Coop's trucks drive 30,000,000 kilometres – equivalent to 50 return trips to the moon.
- Coop has more than 40,000 employees and 1,000 students.

Birgitte Ringbæk
birgitte.ringbaek@if.dk

When food becomes a threat

Recalls of food products are on the increase, and social media represent a rising threat in relation to this. This subject was in the spotlight at If's Nordic Food & Beverage conference earlier this year.

Some examples of risks in food industry are: listeria in smoked salmon. Salmonella found in minced beef. Yeast growing in skyr. Excessive amount of campylobacter bacteria in chicken. Pests found in packets of dried pasta. Risk of shards of glass in pasta sauce. Gas being formed in packs of chopped ham. Excessive amount of E coli bacteria in oysters. Risk of metal fragments in packs of chicken fillets.

The list of food products that have been recalled because of a health risk seems virtually endless.

For many food producers, recalls result in lost production and operating losses, as well as harm to their image. This can cripple production and earnings for companies, and ultimately result in closure or bankruptcy, because of incorrect handling, an online backlash or loss of consumer confidence.

Vince Shiers, MD of the RQA Group and international expert in product recalls, sees a rising trend in both Europe and the USA.

"There are more and more product recalls. I can't think of one product category that has been immune to recalls," he says. There are more regulations, more complex supply chains, higher expectations from producers and more channels for complaints thanks to social media, all of which help to create the overall picture of more recalls.

Threats from social media

Social media form a major part of everyone's lives, and this is increasingly a problem for companies when there is a need for a recall. Messages spread at lightning speed, and if a company fails to act correctly, it can actually create its own crisis if it either underreacts or overreacts, explains Vince Shiers.

"There are more and more product recalls."

Vince Shiers

"There are many people who jump on the bandwagon when a potential contamination or recall is made public, and they write negative comments about the company in social media. People can say anything – regardless of whether or not it's correct. It's really important that companies know how to manage these kinds of interactions," he says.

The trend among consumers is that more people are using social media to complain about companies, and the tone of these postings is getting tougher, if there is an ongoing case, e.g. a product recall, against the company.

The trend from companies is that they themselves are increasingly using social media to provide information about recalls. The situation and problem in question must determine how many communication channels are used by the company concerned: If you overreact, there is a risk that you might blow up an issue of less significance. If you underreact, the crisis can engulf you. If the threat is a serious one, the company should be geared up to manage internal communication, social media, the press and the publishing of announcements.

"I feel that the insurance industry, with the aid of recall insurance policies or product liability policies, is increasingly contributing to limiting the level of risk faced by companies in recall situations. Together with RQA, they advise and assist companies in getting an overview of the absolutely essential internal processes that must come into play if the need arises for a recall," says Vince Shiers.

Microbiology, e.g. listeria and salmonella, is the reason for many recalls, although the primary cause is still human error. One example might be production equipment, which is assembled 99.9% correctly following a repair. Small pieces of metal can become detached and are only discovered in a subsequent inspection. The situation might have been going on for several months. So all of a sudden there are huge batches that have to be recalled.

The response is crucial

It is decisive that relevant technicians are brought in quickly to assist in localising and limiting the damage. Professional, open handling of the product recall can contribute to the perception of a responsible, professional company and thus avoid losing the confidence of consumers.

Put it simply, consumers can forgive a company if a piece of plastic has found its way into a product, but they will not forgive the company if it puts its own profit ahead of the consumer's safety.

Research has even shown that correctly handled recalls can actually increase customer loyalty.

Greatest need in the food industry

A report from the Relational Capital Group showed that almost nine out of ten users (87%) would probably buy and remain loyal to a brand that handles a recall in a responsible, praiseworthy manner – even if the error that caused the recall had resulted in a safety or quality problem. 91% of respondents in the report also answered that they understand that safety and quality problems can occur in even the best-run companies. In most cases it is the way the situation is handled rather than the actual problem with the product that has a positive or negative effect on consumers.

By far the majority of companies with recall insurance cover at If are from the food industry. This reflects clearly where the greatest need exists.

Recall insurance cover includes, among other things, around-the-clock contingency help from crisis consultants with experience of food and consumer products, the costs of announcing the recall, costs and transport in connection with the return and destruction of the products. ■

Recall insurance cover includes, among other things, around-the-clock contingency help from crisis consultants.

Birgitte Ringbæk
birgitte.ringbaek@if.dk

Most frequent causes of food product recalls:

The following situations usually occur as a consequence of human error or a failure to follow procedures

- Chemical contaminants
- Problems in the supply chain
- Labelling errors
- Contaminated animal feed
- Inadequate control of foreign bodies (e.g. glass, stones)
- Procedural errors
- Packaging errors
- Criminality/manipulation

PHOTOS: GETTY IMAGES, ISTOCK

Cyber risks under control

10 Cyber risk controls

13 Roll-out of cyber insurance products

Digital development is providing opportunities within the majority of industries. Along with digital development comes the elimination and decrease of some business risks whilst other risks increase and new ones emerge.

It is said to be a life condition that we seek to understand in both the present and the future by using the experiences of the past. If we accept this as a fact, we must also accept that it constitutes a severe challenge when trying to predict the influence of digital development on our business.

We strive to obtain information from various sources to better understand the digital risk we insure against today, and need to insure against in the future. As an insurance company, we have the privilege of working with the digital risks of almost all industries, which provides insight across business Industries. Some of the lessons we learn, we also seek to share in our various articles, this time concentrating on Cyber. The fact that we will of course also provide a brief overview of how insurance in this context can support the business is (we admit) not actually the most interesting part.

Enjoy.

Kristine B. Wagner,
Nordic Head of Casualty & Marine Underwriting

Cyber risk controls

When If started looking into offering cyber security insurance, we carefully considered how our clients currently use IT in their businesses and how it has evolved over time, the risks threatening IT, and the controls available to mitigate the risks.

In the last 10 to 15 years, organisations have been using IT systems at an ever-increasing rate to automate business processes, make staff more effective and efficient, and provide new services to customers. Examples are enterprise resource planning systems, industrial control systems, logistic systems, e-commerce websites, autonomous vehicles, and smartphones. IT systems have also become increasingly interconnected, not only within a given organisation, but also with systems in external networks that can be controlled by third parties.

Organisations have also shifted from buying equipment and having it serviced by its own employees or contractors to increasingly buying that capability from specialised suppliers. This includes using outsourcing or cloud service providers delivering their services from remote locations, or leasing maintenance and equipment placed at their own premises in order to maintain operational control. What are also included here are mission-critical operational capabilities like logistics systems, and the monitoring and servicing of engines. Business drivers such as growth, profitability and competition drive this change to an 'extended enterprise' as it makes organisations better, faster, and cheaper. However, this change also opens up organisations to new risks as they become increasingly dependent on interconnected IT systems and infrastructure exposing the organisation to new threats and vulnerabilities. For instance, industrial control systems (e.g., SCADA, PLC), originally designed to operate in networks physically separated from all other systems, can, in the present day, be connected to various support systems for resource planning or logistics. These interconnected systems may be located in-house or in the cloud, have connections with remote systems managed by other providers, and be accessible from remote networks for remote monitoring and maintenance.

The tools and techniques used in cyber attacks, as well as the threat actors behind them, have also evolved. Nowadays, security breaches in high profile organisations are frequently headline news.

Tools

One of the most frequently used tools in cyber attacks is malware (computer viruses, worms, Trojans, backdoors) which have been around since the 1980s. The destructive capabilities of malware have evolved to corrupting organisations by implanting remotely accessible backdoors into their IT systems, encrypting their files, or stealing their information. Therefore, today, it is a basic requirement to have up-to-date anti-malware programs for systems commonly affected by malware. The analysis process of early anti-malware used to only require a fairly simple check of any executable file's unique ID against a threat database of known bad files. This may still be quite effective, however, in the present day, malware is designed to be unique and is often tested to avoid detection by even the best anti-malware software. This means that in order to be effective, modern anti-malware software needs to have more advanced detection capabilities like behavioural analysis of what software running in a system is actually doing.

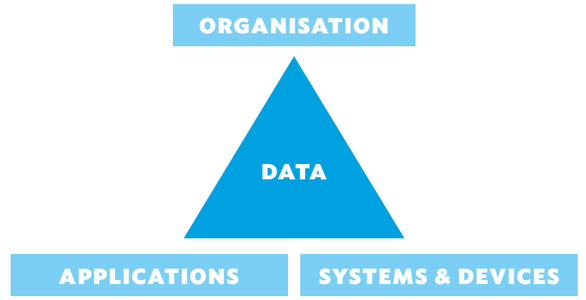
"One of the most frequently used tools in cyber attacks is malware."

Techniques

The techniques used in cyber attacks have also evolved from malware planted in pirated software to employ increasingly sophisticated cyber attacking software and social engineering tactics. For instance, phishing e-mails with malicious attachments or links, have evolved into watering hole attacks, where the attacker guesses or observes which websites the users of an organisation visit. It infects one or more of these websites with malware and simply waits until a user inside the targeted organisation is infected. Computers of compromised users can become remotely controlled in so-called 'bot networks', and used as a stepping stone to further penetrate the compromised organisation, for instance to steal information or plant remotely accessible backdoors in sensitive systems, or launch denial of service attacks towards internal or external targets. As these new techniques often target employees, partners or vendors with a low awareness of security, they have developed into serious hazards even for security-conscious organisations.

Threat actors

Nowadays, the level of cyber skills and funds available for criminal and state-sponsored organisations are high and rapidly increasing. This is driven by a good Return on Investment, while having a low risk for detection and attribution to who's behind the attack. For example, Ransomware is currently a criminal industry with a global turnover of more than one billion USD where separate and highly specialised criminal groups often collaborate to reach their objectives. State sponsored actors can have almost unlimited skills, funds and patience. They may target anything that can provide an advantage to their sponsors, for example, by stealing secret information or infiltrating critical national infrastructure. As seen in the last year's cyber threat intelligence reports, they have the capability to penetrate systems deep within strategic high-value targets and critical infrastructure, and stay undetected for several years.



Cyber risk management

Every organisation should understand that, in addition to basic security controls, like anti-virus and firewalls, their cyber risks may require a whole range of additional cyber security controls to protect applications, systems, devices, and their organisation. Even if systems are separated and placed behind firewalls, and regardless of whether they are private, outsourced, or happily out in the cloud, all systems may be vulnerable to cyber attacks.

In a cyber risk management system, all possible risks to the organisation, partners, and suppliers need to be considered. Examples are financial loss, process disruptions, failure of information technology systems and reputation loss. In the risk assessment, the organisation must consider the perspective of possible attackers and assess which of their assets may have a value to those attackers.

Cyber security is a board responsibility and managing it has become a profession in itself with strategic, tactical, and operational requirements to consider. The IT department is not the most likely candidate to handle cyber risk management

as it could cause a conflict of interest (e.g., availability vs integrity). Appointing a Chief Information Security Officer (CISO) responsible for overseeing the whole organisation's information and IT security posture is a good first step, but may only be the beginning of the journey.

For boards and executives, it is important to include cyber risks in the enterprise risk management framework and regularly assess the impact and likelihood of cyber risks, as well as provide sufficient resources and support to implement cyber security controls protecting the organisation from loss. The operational parts of the organisation must understand its responsibility to properly design, maintain and monitor cyber security controls, regardless of whether the control is located within their own or a provider's direct control.

As cyber attacks regularly prove their disruptive character, authorities are also stepping in and setting out requirements for the protection of Critical Infrastructures (CI), National Defence Capabilities (NDC), Personal Identifiable Information (PII), and other key assets. Recent regulatory requirements have expressed that the security controls must be 'state of the art' in order to be compliant, which means that organisations must regularly review and assess whether the controls are adequate and be prepared to have their security controls challenged by authorities.

Cyber control frameworks and baselines

To help organisations implement risk-driven security controls, security standards have been developed to control cyber risks. One of the most well-known is the ISO/IEC 27001[1] standard, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organisation's defined scope. The latest version of this standard now applies the 'High-Level Structure' used in other ISO standards, for example, in ISO 9001 (Quality Management) and ISO 22313 (Business Continuity Management). Alternatives exist such as the NIST (United States) and COBIT (ISACA) frameworks, and there are also frameworks developed for healthcare and financial institutions.

Having a framework helps organisations to identify their risks and then design, manage and review controls to mitigate the risks, but it does not tell the organisation what they are and how to deal with them. If one takes a phased approach when implementing a standard focusing on key business processes as the first step, it is usually not a lengthy process to assess risk and establish the level of security controls already in place.

Organisations that are in a hurry, or for some reason cannot implement a cyber security standard or framework, should consider adapting a baseline describing a set of concise, prioritised cyber practices to stop the current most pervasive and dangerous cyber attacks.

Baselines defined over time especially for critical infrastructures are often available from national Computer Emergency Response Teams (CERT). As the risks to applications, systems, devices, and operators are more or less common risks, any organisation can profit from them. You can find your national CERT on the internet for example at; cert.dk, cert.fi, cert.no, and cert.se. Baselines and frameworks are also available from (state) sponsored non-profit organisations. One of the most well-known control baselines is provided by the Center for Internet Security (cisecurity.org). They promote their CIS Critical Security Controls. And for operators of critical infrastructure, the NIST Cybersecurity Framework provides private sector organisati ons with a structure for assessing and improving their ability to prevent, detect and respond to cyber incidents.

The value of cyber controls

Did you know, that by applying just the first five (!) of the CIS Controls as 'hygiene', organisations can reduce the risk of a cyber attack by around 85 per cent!

Those top 5 controls are:

- **CSC 1: Inventory of Authorized and Unauthorized Devices**
- **CSC 2: Inventory of Authorized and Unauthorized Software**
- **CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
- **CSC 4: Continuous Vulnerability Assessment and Remediation**
- **CSC 5: Controlled Use of Administrative Privileges**

Regardless of the chosen approach to implement cyber security controls, they must be regularly assessed or tested in order to provide assurance that they work and that current risks are properly mitigated. It's vital to conduct regular audits and tests, preferably by using skilled security penetration testers that simulate a cyber attack. Security penetration testers are trained to use the same kind of mindset, methodology and tools as cybercriminals, but in a controlled and non-destructive manner. ■

Erik van der Heijden
Erik.van.der.heijden@if.se

Peter Granlund
Peter.granlund@if.se

[1] ISO/IEC 27001:2013, an information security management system (ISMS) standard initially published in 2005, revised in 2013, by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC)

Roll-out of cyber insurance products

Why cyber insurance?

Until recentely USA has been the biggest market for cyber insurance. The main reason behind this is the legal development where the starting point was the California Database Protection Act of 2003, which required disclosure of any data security breach to each affected California customer whose Personal Information had been compromised. Following this act, many US States now have similar legislation. And with the new EU General Data Protection Regulation (GDPR), in 2018 Europe will also get a uniformed legislation in respect of Personal Data and Breach Response.

The US legal environment with respect to Personal Identifiable Information (PII) has been the primary market driver for Cyber Insurance in the US. As similar requirements have now been introduced in the European Union by means of the General Data Protection Regulation (GDPR), we are experiencing a similar demand here in Europe at the moment.

The risk of business interruption is another important market driver. We have noted that some executives are failing to recognize a paradigm shift. Where it used to be possible to revert to manual labor when business automation failed, this option is no longer commonly available. Today process automation is integrated by means of robots and technology which can no longer be replaced after a loss by hiring workers at short notice because they will lack the knowledge, skills, tooling, and space to do the same job at the same costs.

The protection of Information Technology (IT) and Industrial Control Systems (ICS) should therefore be given top priority because as the unauthorized operation of IT and ICS may cause serious business interruptions as we have seen in recent cyber-attacks (e.g. WannaCry and NotPetya). During these last couple of years, it has become obvious that "cyber" is part of our everyday life, with more and more things being connected with the internet and more and more business processes being dependent on access to the internet. With this connectivity and accessibility also comes the exposure for malicious tampering with your systems.

With these exposures in mind, the insurance industry has responded with the development of cyber insurance products.

We cannot say that the market for these products would be mature. Therefore, the available limits and capacity are somewhat restricted. However, the products like If's new cyber products are fairly wide in coverage.

The risk is continuously growing and changing. All companies should be working hard to evaluate the IT security of their systems and operations. The results can be seen in improved security and preparedness for attacks and other incidents, although variations in attitudes and goals make all generalisations difficult. For us as an insurance company, it is of paramount interest that we have a realistic view of the probability and exposure of our clients' assets that are at risk. Only then can we contribute to your risk management with adequate products and fair premiums. Cyber risks challenge our skills and ability to provide the needed assistance to customers. If P&C has invested in the underwriting and risk management skills to be able to support its clients.

If P&C's Cyber Insurance Products

If has created three products to cover our clients' cyber risks. The first one was computer crime insurance sold to small and medium-sized companies by If's Business Area Commercial. It has been a success and is being developed further.

For larger enterprises and their specific needs, If provides two insurance products. The comprehensive stand-alone If P&C's Cyber Insurance can be seen as a combination of traditional liability coverage (claims for compensation presented to the insured by third parties) and property coverage (first-party losses sustained by the policyholder itself) though with the difference that a cyber incident is the cause of loss. The policy wording is built up of ten different coverage sections, of which some are part of the basic coverage while others are optional for the client to buy depending on the needs and exposure of the client. Each coverage section has to be tailored to the client's needs. The liability components are:

- confidentiality and privacy liability
- network security liability and
- media liability.

The property component, or more correctly the first-party loss component, is divided into:

- Restoration of data costs
- Incident and breach response
- Business interruption
- Cyber extortion
- Reputation
- Cyber crime and
- PCI-DSS Coverage (PCI-DSS – Payment Card Industry – Data Security Standard)

With regard to insurance jargon: what actually is a cyber incident? In our insurance product, it means a malicious act (e.g., a hacker attack), computer malware (e.g., computer virus), human error (e.g., insured's employee causing a failure of IT-systems), denial of service attack, (unplanned system outage), or theft of data occurring on or aimed at the insured's computer system.

If P&C Property & Business Interruption Programme's Cyber Endorsement

In If's studies, it has become clear that for our Industrial clients the main cyber risks are considered to be attacks or incidents through the client's facility's industrial control systems and consequential property losses and further losses due to business interruption.

If has developed a cyber product as a new endorsement to fit into a property master policy covering also Business Interruption of our client. It covers non-physical loss to electronic data and media and consequential Business Interruption. This product covers only the Insured's own losses to data and media as well as business interruption and is thus a first-party insurance only. The insured causes of losses are:

- Unauthorised access
- Unauthorised use
- Malicious code
- Malicious act
- Denial of service attack and
- Operational and administrative error.

In addition to the actual loss, the insurance covers necessary extra expenses to minimise, avoid or reduce an interruption in service.

Of course, to take out this insurance, the client needs to fill in the questionnaire describing the status of the IT Security. The insurance terms also require the insured to comply with some safety regulations concerning, for example, back-ups and system protection methods.

Risk Assessment

Cyber insurance could not be sold without assessing the client's risk thoroughly. There are great variations between businesses and individual clients and the statistics of historical data in this fast-developing risk area give only a faint picture of the risk of an individual client. The assessment also offers the opportunity to appreciate a client's investments in high-level IT security in the insurance solution.

> *"Cyber insurance could not be sold without assessing the client's risk thoroughly."*

When underwriting cyber insurance, the risk assessment could be divided into three different levels;

- The general level of exposure of the policyholder's industry. What legal environment applies, what kind and how much personal data is typically handled within the industry and how exposed is this data?
- The level of exposure of the policyholder company itself. How complex is the group? Number of subsidiaries, data centres, important suppliers, intra-dependencies etc.?
- The level of IT Security of the company. How does the company work with identifying, protecting, detecting, responding and recovering when it comes to IT risk and data?

If P&C gathers the needed information via a questionnaire where the client responds to these specific areas. It could also be that a meeting or an interview is needed, with, for example, the IT security department of the client, to further elaborate on these topics. Based on the answers If P&C gets the risk profile of the client and this then also could – and should – interact with the policy coverage. Different coverage elements are used, perhaps with additional sublimits and different deductible levels/waiting periods for business interruption coverage, to meet the needs and demands from the client.

Accumulation as the insurer's nightmare

One aspect where cyber insurance causes some extra concern for the insurance industry is the accumulation of risks. Primarily insurers look at each risk separately, considering the coverage and the premium. In some cases, like damage caused by big storms, many policies can be triggered at the same time, causing larger total claims at the same time. However, in cyber risks, there are plenty of new possibilities to trigger many policies that do not even follow the laws of nature. This appears in two ways. First of all, cyber incidents may trigger different products simultaneously. As mentioned above, a cyber insurance policy has elements of both property and liability coverage. Cyber methods can be used to cause traditionally covered fires, machinery breakdowns or other damage, or there could be specific endorsements added to the property or liability policy. The same goes for crime insurance, where one could also have coverage for some of the exposures that cyber insurance addresses.

The other method of accumulation, which is the most complicated to model and monitor, is event exposure. In traditional coverage, like property, it is after all fairly easy to calculate and take into account in premium modelling, even large natural phenomena, since normally they cause damage within a limited geographical area, regions exposed to flooding, earthquake and other known hazards. For cyber however, there are no geographical boundaries for how an event would impact, something we have seen in many examples like global virus attacks. Also, since many companies today use external services, such as cloud services, there is also a risk of accumulation in this respect.

We have built our internal risk control to address this. We are continuing with all efforts to secure both your and our exposures with advanced calculation models in co-operation with our reinsurers.

Conclusions

This short article can only point out some primary features of the cyber insurance products and their underwriting requirements. This risk area with its large loss potential to individual enterprises and dangerous accumulation mechanisms requires full attention from every company to its IT security. We at If can then provide insurance solutions supporting our client's management of risk. ■

Matti Sjögren
matti.sjogren@if.fi

Mats-Ola Jakobsson
mats-ola.jakobsson@if.se

PHOTO: ISTOCK, FFI

Li-ion batteries – **hazards and mitigation**

Lithium-ion batteries have become an indispensable source of electricity and are used in applications ranging from consumer electronics to ferries.

The Norwegian Defence Research Establishment (FFI) has investigated the safety characteristics of batteries for more than two decades. In this article, we look into the hazards of Li-ion batteries and how they are mitigated. Since its market introduction in 1991, the Li-ion battery has become an increasingly popular source of electricity. Its high energy density has been an essential precondition for the introduction of smartphones, tablet computers and numerous other electronic gadgets. During the last decade, Li-ion batteries have also proved themselves as a feasible power source for cars and have made all-electric ferries possible. Recently, battery installations of an even larger scale have been implemented, such as in energy storage for electric grids.

However, the high energy density of Li-ion batteries also has its downside: Several incidents of Li-ion batteries catching fire have been reported: Battery-powered hoverboards start to burn during use, and spare batteries for e-cigarettes flame up in the pockets of their owners. The US Federal Aviation Administration registered 21 Li-ion battery incidents inside airplane cabins during 2016. The recall of Samsung Galaxy Note 7 smartphone/tablet due to battery flaws last year marked the 10-year anniversary of the Sony laptop battery recall in 2006. In applications involving larger battery packs, the incidents are more extensive, as has been exemplified by some high-profile electric car fires. As Li-ion batteries are installed on an even larger scale, the consequences of a fire become more severe and the importance of proper safety measures become even higher. The importance of safety also varies with the type of application: You can step away from a burning car, but leaving a burning ship is not as easy, not to mention planes.

WHY DO LI-ION batteries catch fire? One important difference between Li-ion batteries and traditional alkaline and lead-acid batteries is the flammable electrolyte. Due to the high cell voltage of Li-ion batteries, the traditional water-based electrolytes cannot be used. Instead, Li-ion battery electrolytes consist of organic liquids which are stable under the operating conditions of the cell. Unfortunately, these liquids also have the ability to burn readily if ignited. In addition, the positive electrode material in many Li-ion cells releases oxygen at sufficiently high temperatures. This means that a Li-ion battery fire can sustain itself even without access to ambient air. To obtain high energy density, Li-ion cells have a very compact design, and the electrodes are separated only by a thin polymer membrane. If the electrodes inadvertently come in direct contact in an internal short circuit, the released energy can be sufficient to force the cell into an accelerating heating process known as thermal runaway. As battery manufacturers push for ever-increasing energy density, safety margins are constantly being challenged.

COMMON TO ALL Li-ion battery incidents is that they go through a heating stage. Heating can have several causes: Overcharging, overload, heat exposure and external or internal short circuits. Internal short circuits can arise from physical impact, such as Tesla Model S fires due to road debris penetrating the battery pack. They can also be caused by metal particles from the production line trapped in the cell, as was the case for the 2006 Sony recall or other cell design or manufacturing flaws, as was partly the case for the Samsung recall. Many of these flaws are extremely difficult to detect, and can pass unnoticed through the strictest product quality testing regimes. Internal short circuits can also develop over time until they pass a critical point. This is for instance the case for lithium dendrites, needle-shaped lithium structures that grow on the electrode surface under unfavourable charging conditions. To complicate matters, the thermal stability of cells can deteriorate as they are used. According to recent investigations at FFI as well as other research institutions, some cells exhibit a higher ability for self-heating after repeated charge/discharge cycles. This underlines that the possibility for a Li-ion cell fire cannot be ignored, even for the best cell manufacturers.

"Common to all Li-ion battery incidents is that they go through a heating stage."

If any of these factors cause the cell to heat beyond a certain point, unwanted internal reactions are initiated that in turn release even more heat. The reactions can form gases that increase the internal pressure in the cell. In some cases, the consequences are rather mild: the cell releases its internal pressure through a designated weak spot a process known as ventilation and the cell cools down. In more severe cases, the ventilated gases are ignited, giving fire or gas explosion. Heated cell parts or sparks from the cell are likely sources of ignition resulting in fire or gas explosion. If the internal self-heating reactions continue, the cell can reach thermal runaway with violent fire, gas emissions and even explosion. Emitted gases are flammable and unhealthy and represent a hazard by themselves.

PROPER BATTERY SAFETY is ensured on several levels. On the cell level, most Li-ion cells contain a separator between the electrodes which shuts down the internal ion transport at excess temperature. Some cells are equipped with a safety switch which electrically disconnects the cell if its internal temperature becomes too high. As mentioned, a weak spot in the cell wall releases excess pressure and prevents violent cell rupture. Much progress has been made in finding more stable cell electrodes, less flammable electrolytes, and other material improvements that enhance safety. Many safety improvements, however, come with a performance penalty. The importance of production quality has also received a lot of attention. Thanks to these improvements, the failure rate of high-quality cell manufacturers is appreciably low. The remaining risk can be reduced by the end users, for instance by considering where their electronic devices are stored and recharged. Batteries that have overheated inside plane cabins have so far been safely taken care of by dousing them with water or other available liquids.

On the battery level, safety can be enhanced by sufficient space or insulating/cooling plates between the cells. Most batteries also include a battery management system that prevents overcharge, over-discharge and overload and ensures proper operating temperature.

On the battery system level, as for instance on large maritime batteries, additional safety features are necessary. Batteries are installed in battery rooms with proper ventilation, gas detection and fire extinguishing equipment, gas ducts, fire walls, etc. According to FFI's experience, a critical aspect in large installations is identifying the representative worst-case behaviour of a failing cell and design the battery installation to handle this scenario. This includes ensuring that a cell fire does not propagate to neighbouring batteries.

Even with sporadic fires, Li-ion batteries have maintained their popularity. As this technology enters new and larger applications, it is crucial that the battery hazards are well understood and mitigated throughout the lifetime of the battery. With proper knowledge, severe consequences can also be avoided in the future. ■

Helge Weydahl
Senior researcher, PhD
Maritime Systems Division, Norwegian Defence Research Establishment
helge.weydahl@ffi.no

About the Norwegian Defence Research Establishment

The Norwegian Defence Research Establishment (FFI) is the prime institution responsible for defence-related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI is the chief adviser on defence-related science and technology of the Ministry of Defence and the Norwegian Armed Forces' military organisation. A particular task for the institute is to investigate aspects of the development in science and military technology that can influence our security policy or defence planning. FFI operates within a broad spectrum of research topics ranging from the assistance of operational units to the support of national security policy via defence planning and technology studies. The institute has been involved in battery safety research since the 1980s.

FFI was founded in 1946 and is organised as an administrative agency subordinate to the Ministry of Defence. It is located in Kjeller and Horten in Norway and has about 720 employees.

Website: www.ffi.no

About the Norwegian Forum for Battery Safety

The Norwegian Forum for Battery Safety is an informal forum for industrial users of batteries, government institutions and research institutions in Norway. FFI is the secretary and organiser of the forum. The goal of the forum is to distribute knowledge that can enhance safe use of lithium batteries, Li-ion batteries and other high-energy batteries.

More information about the forum and battery safety in general can be found on its website: www.ffi.no/batterisikkerhet

FFI Forsvarets forskni i i

PHOTO: GETTY IMAGES

The unknown problem with sprinkler systems

An explosion in a sprinkler control room. Flame tongue bursting out from a sprinkler pipe when drilling a hole in the pipe. Pipes are bursting apart at the joints.

These are recent examples of dramatic incidents caused by the chemical process of forming flammable hydrogen gas in galvanised sprinkler systems. Systems designed to limit or stop a fire were suddenly reported actually being the cause of hazardous situations. This has until recently been an unknown problem in the sprinkler industry, and investigations were initiated to bring clarity to these incidents.

Galvanisation is a common process to protect steel from corrosion in atmospheric conditions and ensure a long life span. A thin layer of metallic Zinc is added to the mild steel construction. The hot dip galvanisation protects steel from corrosion by providing a thick, tough, metallurgical bonded zinc envelope, which completely covers the steel surface and seals it from the corrosive action of its environment.

The benefits of using this technology for sprinkler pipes were seen as obvious, being suitable for installing outdoors and in harsh environments to prevent the steel from corrosion. It also allows mild steel quality and thinner piping. Press-fitting installations and lighter pipes could then decrease the installation time on site and system weight compared to the more traditional threaded couplings. These benefits were also seen as favorable for indoor use in wet sprinkler systems.

"Dramatic increase could indicate accumulation of hydrogen gas."

The pros of this technology used in wet sprinkler systems however have proven unfavourable after all. The investigations following the losses described earlier have shown formation of hydrogen gas as being the root cause. The chemical reaction creating hydrogen in a reaction between oxygen, zinc and iron is not new knowledge. Under certain conditions, these materials will react, creating hydrogen gas. This knowledge was not familiar in the sprinkler piping industry where the galvanised, closed wet sprinkler systems are filled with stationary water.

Filling up wet sprinkler systems with water, there will always be some air-pockets left above the water level. Dissolved oxygen in the systems will react with the metals causing a corrosion process until the oxygen is consumed, a condition called dead water. In traditional black-steel piping, a protective layer of Magnetite will protect the steel from further corrosion until adding fresh oxygen when replacing the water. When galvanised pipes are pressurised with water, the dissolved oxygen will react with the zinc surface, forming zinc hydroxide, a pulverised corrosion product with poor protection characteristics. As with all corrosion products, the zinc hydroxide can accumulate in the lower parts of the pipes, blocking pending sprinkler heads preventing water from reaching the seat of the fire or reducing the water discharge. When all the dissolved oxygen is consumed, a cathodic reaction will cause increased production of hydrogen gas, which gathers in the air-pockets above the water level in the pipes. This can be revealed by reading abnormal pressure increase at the pressure gauges.

Hydrogen gas has a wide range of flammability limits, between 4% and 75%. Obviously, accumulation of considerable amounts of the flammable hydrogen gas can be hazardous when exposed for sparks, i.e., by drilling holes or cutting pipes. The excess pressure itself has also shown to be substantial in some systems where the design criteria allows a maximum pressure of 12 bar (EN 12845). Galvanised pipes are used in press-fitting installations. A well-known loss driver in such systems is pipes bursting apart due to inadequate or faulty workmanship when pressing the fittings together. Another theory, however one that is not verified for some of these losses, is that accumulation of hydrogen gas has caused an increase of the static pressure beyond the design criteria of the systems, followed by bursts in the joints.

Given the right circumstances, the Zinc will be consumed by corrosion during a relatively short period of time, 2-3 years. After this, the pipes will be considered normal, however thin-walled.

Galvanised sprinkler systems are commonly used in Norway. Preferably, the systems should be replaced by another steel quality. However, some mitigating actions can also be made in existing systems;

- Weekly monitoring and logging the static pressure above the sprinkler valve. Dramatic increase could indicate accumulation of hydrogen gas. This periodic monitoring is not more than described in the maintenance process in the European sprinkler standard EN 12845.
- Replacing air with nitrogen has proven to be successful in preventing the corrosion process and will increase the life span, but will have limited effect on the formation of Hydrogen.
- Personnel maintaining the systems and especially when mechanically working with the pipes, needs to be aware of the problem.
- Different material quality should not be mixed in the sprinkler systems; this might increase the corrosion and the cathodic process.
- Flushing the systems before pressurising. However, this is not recommended for systems in use.
- Venting of excess pressure has proven to be effective.
- Adjusting the pH of the water. The zinc corrosion rate has been shown to be the lowest at around pH 10, however, not above 11.5, which may cause etching of human skin. ■

Anders Rørvik Ellingbø
anders.ellingbo@if.no

Facts about the process

- **The anodic reaction:** $Zn \rightarrow Zn^{2+}+2e^{-}$
- **The cathodic reaction (water) is:** $O_2+2H_2O+4e^{-} \rightarrow 4OH^{-}$
- **The process itself will continue as long as there is oxygen present in the system. When the oxygen is used, the cathodic reaction will continue, producing hydrogen from the water:** $2H_2O+2e^{-} \rightarrow H_2\,(g)+2OH^{-}$
- **76.1 mm of pipes can, through reaction, create 17 liters of hydrogen gas annually for every meter of pipe. Depending on the thickness of the zinc layer, up to 35 liters could be created annually.**
- **This creates a pressure increase which could amount to up to 49 bar.**
- **The pH will affect the rate of zinc corrosion.**

The quality of the water will have an effect on the process.

PHOTOS: GETTY IMAGES, SFPA

Positive results with training

Fire from hot work in a hotel.

How to better manage the risks of hot work in different workplaces and environments.

Hot work is a collective term for work with heat-generating or spark-generating tools that entails a risk of causing fires. Welding, cutting, soldering and work with high-speed rotary tools are performed in a number of areas such as industrial work and construction, agriculture and shipping to name but a few. When hot work is performed at a temporary workplace and is also deemed to represent a fire risk, Swedish insurance companies require the work to be carried out by certified personnel. Heta Arbeten® (Hot work) Certificates are issued by the Swedish Fire Protection Association (SFPA) after completion of a course. But this has not always been the case. Björn Wennerholm, expert in Heta Arbeten® at the SFPA explains:

"In 1990 we launched the loss prevention concept Heta Arbeten® in collaboration with insurance companies. The companies were all experiencing a continuous increase in costs relating to fires following hot work and realised that something had to be done, the sooner the better. The SFPA was already cooperating with the insurance companies, and with our expertise and experience it was natural that we were tasked with producing training materials and implementing the loss prevention concept throughout Sweden", says Björn Wennerholm.

The fact that the insurance companies united on this issue and agreed on mutual safety regulations was fundamental to the success of the concept, according to Björn Wennerholm.

"The major insurance companies laid the groundwork – Folksam, If, Trygg-Hansa, Länsförsäkringar, Zurich, etc. The other, smaller insurance companies followed The SFPA's safety regulations matched the insurance companies' demands and were soon accepted by the main insurance companies. To this day, they refer to the SFPA's safety regulations when asked about hazardous hot work at temporary workplaces", shared Wennerholm.

THREE POSITIONS MUST be staffed by persons with valid Heta Arbeten® Certificates: the permit issuer who gives permission and is responsible for the work being carried out in the appropriate way, the hot work operative who carries out the work and a fire-watcher who monitors the work. Once the safety regulations and roles were defined the SFPA produced

Fire from hot work in a hotel

In the early hours of the morning of 23 June 2010, a man calls 112. "The wall's on fire, you need to come at once". He is calling from a heritage-listed hotel in Sweden and was working for a local company hired to remove old paint from the wood façade before repainting. To remove old paint, he used his normal heat gun and heating pad before scraping off the paint. But the wooden façade was old and dry, and the heat from the tools soon made the wall catch fire. The fire spread quickly through the exterior wall further on to the attic and part of the building was severely damaged. The final cost of repairing the hotel was SEK 25 million, a job that took more than six months.

The hotel's insurance company claimed that the contractor was responsible for the damage as they had disregarded the safety regulations to which the insurance conditions refer and which reduce the risk of fire, and hence sued the contractor for SEK 12 million. The subsequent investigation showed that the job of removing paint had been performed by a person who did not hold a Heta Arbeten® Certificate and had not completed the required training for heat-generating equipment. The court therefore approved the claim and ruled in favour of the insurance company.

14 safety regulations

The Heta Arbeten® loss prevention concept is based on 14 regulations, which cover:
- **Permits**
- **Competence**
- **Fire watcher**
- **Flammable product**
- **Cleaning and wetting down**
- **Combustible material**
- **Concealed combustible structural elements**
- **Unsealed areas**
- **Fire-fighting equipment**
- **Welding equipment**
- **Raising the alarm**
- **Drying and heating**
- **Drying underlay and applying waterproofing**
- **Melting asphalt**

the education material and built a functional training organisation. By training instructors and allowing them to offer courses in Heta Arbeten®, it was possible to disseminate the concept quickly across the country. Today there are around four hundred certified training organisations and one thousand certified instructors around the country. The SFPA is responsible for ensuring that the instructors receive regular competence development. When the concept was rolled out it soon produced positive results.

In the early '90s, between 20 and 25 per cent of the total cost of fire damage was caused directly by hot work. Since then, this number has dropped by 75 per cent. Not only have the costs fallen, the number of fires has also decreased significantly. Unlike other common causes of property damage, the stricter rules have shown that this type of loss can be prevented.

"People are generally better now at managing the risks of hot work at workplaces. Everyone's aware that there are requirements imposed. There are fewer and fewer fires, that's the big difference. We should be proud of that. The Heta Arbeten® loss prevention concept is the largest Swedish fire loss prevention initiative of the past 30 years", says Björn Wennerholm.

As the concept was nearing its 25th anniversary, the SFPA and insurance companies realised that the situation at workplaces throughout the country had changed. To better meet the expectations and demands of the workplaces, they decided to modernise, improve the quality and streamline the training. As many professional hot work operators currently have a language other than Swedish as their first language, the training material was translated into several languages and both the training and the certification test were digitized. All instructors were trained to use the new concept and the SFPA improved its data collection and analysis of fires caused by hot work to better integrate new knowledge into the training.

Part of the success of the Heta Arbeten® loss prevention concept is that the base, which consists of the safety regulations, has changed very little over time. This has allowed for continuity and has resulted in the concept being well established and well known. These days, the SFPA's Heta Arbeten® certification is an essential and established requirement for those who work professionally with hazardous hot work.

Björn Wennerholm does not expect the need for the concept to abate.

"There's so much planning and construction taking place in Sweden in 2017. New materials and new methods give rise to new needs for knowledge and risk assessments. The Heta Arbeten® loss prevention concept allows us to offer exactly this. Denmark, Norway and Finland already have similar courses. The insurance companies want a controlled system to be maintained, namely that the people performing these types of jobs have the right knowledge and certification. Heta Arbeten® has given them this", concludes Wennerholm. ■

Anna Karin Källén
AnnaKarin.Kallen@brandskydds-foreningen.se

HOT WORK 2016 - FACT BOX

Number of active instructors: 778
Number of active organisers: 433
Valid certificates: 353,000
New certificates in 2016: 73,669

In 2016 there were
6 instructor training courses
65 quality assurance inspections in connection with training sessions

If P&C and hot work

Hot work and the risks associated with this type of high-hazard work is an important focus area in our partnership with clients, for example, during risk surveys and other site visits.

A well-managed hot work procedure should be a well-established part of the risk management system for any company. However, the effectiveness of the management from a safety perspective varies considerably. We see large differences between different countries, companies and industries, ranging from very well-organised locations, with well working systems and procedures to locations with no system or safety considerations at all. Failure to properly control hot work will result in a significantly increased fire risk.

A systematic hot-work procedure covering what must be done before, during and after the work is key to managing risk. The procedure should include training of personnel, risk assessments, hot work permits, fire watchers, etc. A systematic approach will reduce the probability of a fire loss considerably and hence reduce the risk of a long interruption to business, with potentially very large consequences for the company and even the entire group.

If has hot-work permit forms and guidance available in several different languages for our clients. We recommend our clients to use these, or a similar management system that is in line with safety regulations, such as SFPA permit/checklist.

For further information, you are welcome to contact us.

Contact information is available at www.if-insurance.com

Tobias Widell
Tobias.widell@if.se

Your data matters

Data protection is more than a compliance issue. We know you care about your privacy and respect that.

On 25 May 2018, the General Data Protection Regulation will be enforced across Europe. The law provides citizens more control over their data and creates a uniformity of rules to enforce across the continent.

Our business is to protect our clients for all events. This also applies to the personal information we share. We exchange a vast amount of personal data with our customers on a daily basis. It can be any information connected to a person, directly or indirectly.

There is no difference whether the data are private, work-related or online identifiers - if they can be linked back to a person.

The General Data Protection Regulations (GDPR) is a new set of rules governing the privacy and security of personal data laid down by the European Commission. The Regulation requires that personal data has to be kept secure.

The rules are very complex and we build them into our whole organisational culture to manage data safely and more effectively, internally and externally.

They are designed to ensure citizens control over how their data is processed and used. The basic rules can be described as:
- Know what you have, and why you have it
- Manage data in a structured way
- Know who is responsible for it
- Encrypt what you wouldn't want to be disclosed
- Design a security awareness culture
- Be prepared!

We have worked within national regulations for some time and welcome this common EU regulation as an opportunity to improve the way we handle personal information.

In November2015, If launched a Data Privacy Project to ensure that our systems are compliant with GDPR requirements. The initial phase of the project mapped the existing Nordic and Baltic IT systems and development projects to identify systems handling personal data. The findings have resulted in a number of comprehensive measures with regard to the deletion and/or anonymisation of personal data and sensitive personal data.

Concurrently we established retention periods for different information categories, e.g., customer information, claim information, insurance policies, prospects, and employee information. These retention periods are currently in the process of implementation.

In addition, the project focus is on the necessary activities to create and implement Data Privacy throughout If's organisation. The purpose is to:
- Increase the level of awareness throughout the entire organisation through a mandatory training program for both employees and consultants
- Map and review all business processes to ensure that our current manual processes handle personal data in a secure manner and revise and implement measures where needed
- Improve our guidelines and instructions for processing/storing personal data other than in IT systems, e.g., emails and sharing of files

Our continuous efforts focus on whether that personal data within will remain secure and through implementation date, we will report data breaches to our supervisory authority and any affected individuals will also be notified directly.

We want you to trust us with your information. In the future – just as in the past. Any concerns or questions – do not hesitate to contact us. ■

Linda Häss
Linda.hass@if.se

PHOTO: GETTY IMAGES

Compliance news

Non-life insurance can be considered to be one of the most regulated businesses in the world.

It is common knowledge that well over 140 countries in the world do not allow insurance activities to exist within their borders unless a local legal entity has been established. In addition to which there needs to be a local operational license, the granting of which is subject to the legal presence having the required solvency capital. This is not the only requirement that insurers have to comply with.

Even within European Union, where one passport should allow non-life insurers to provide services cross border, there are e.g. mandatory lines that limits the options for centralized and flexible risk management. Moreover, local standard terms and conditions and many other practical issues may also apply.

If P&C has through own offices and a network of international insurance partners in 150 countries covered your risks all over the world. We also actively search out a partner that best suits your needs when you enter a market in which you are not already present. Our partners are top ranked amongst their peers in most markets.

Insurance premium taxation (IPT) in European Economic Area (EEA)

A major trend in recent years has involved the introduction of new and increased premium-related taxes. For example, the current taxes have meanwhile been increased in the UK and France. In addition, the number of tax audits is increasing, with clients' internal allocations being reviewed and insurance premium allocation may be dimensioned in proportion to cross border insurance solutions. The only exemption is Romania, which recently decided to decrease the payments applicable to locally established insurers. Let us see what is announced at the year-end.

All premium related taxes in EEA are calculated, accounted and remitted by If as direct insurer (local of cross border insurance solutions) or our local partners.

Finland

This year we have a very special celebration: Finnish IPT has now 50th anniversary. It was supposed to be a temporary tax, but currently it has the highest overall tax rate in Europe at 24%. It hits all entities insuring risks located in Finland. In a case the insurer is a third country company (outside EU/EEA), the client becomes liable to report and pay the IPT.

Slovakia

Slovakia introduced 2017 a new 8 % IPT which covers all lines of non-life line business.

The Netherlands

The Netherlands has recently issued a new law. The most interesting part concerns co-insurance as according to Dutch legislation the leading coinsurer should handle the IPT. In The Netherlands that is the case, however, the new law has tightened the specific conditions pertaining to this. In the Dutch market, however, also the broker may be subject to obligations to pay IPT.

IPT in coinsurance solutions has been argued in the industry as some insurers consider IPT payment as a liability of the leading insurer, others argue for the other way around. It is evident, that each country has its own set of rules or the rules are silent on this issue.

Greece

In recent circular the local tax administration confirms that tax cannot be paid back on return premiums as tax should be returned on refunded premium as technically it is not due. This practice is similar to Italy.

Foreign Account Tax Compliance Act (FATCA), new obligations

The Foreign Account Tax Compliance Act (FATCA) is a U.S. law aimed at preventing tax avoidance by U.S. taxpayers through the use of offshore accounts. It entered into force in July 2014. Since then well over 100 countries have now signed up to Intergovernmental Agreements (IGAs) with the US to implement FATCA.

Premium payment from US

For non-life and risk life insurance (other than life savings) FATCA was not a huge burden at the beginning. It applied to risk premiums paid from the US to a foreign entity. Based on this US insurers, brokers and direct clients have requested the so called W-8BEN-E form that discloses the foreign insurer's status. In the event that no such form is furnished, the US withholding agent (i.e. local insurer, broker or client) has an obligation to withhold 30% from the insurance premium paid to off shore insurer. If P&C has naturally delivered the requested forms and is therefore compliant with FATCA.

"A US source risk has a wide definition."

New obligations, US-source risks

As from the 1st January 2017, the transitional period for the FATCA regulation lapsed and it now also applies to foreign to foreign insurance premium payments in regards to US source risks. A US source risk has a wide definition. A quick answer is when the insured property or person is, or can be, based in the US. Currently the London market brokers and some US origin brokers have reacted to this new rule and have communicated it to their clients and advised their clients to consider with their tax and compliance advisors how they may be impacted by FATCA. Also a few of the big four accounting entities have published letters around this issue, especially in the UK.

If's FATCA compliance

If P&C is compliant and If's clients / brokers can be compliant as well with the said amended regulation. Under FATCA, all of the If Group's entities and their branch offices are considered to be Non-Financial Foreign Entities that are subsidiaries of a listed entity. If provides W-8BEN-E forms, which disclose and prove its status under FATCA on request. In order to facilitate requests for the receipt of the information, W-8BEN-E forms for all of the If Group entities are also made available to you online **if-insurance.com/web/industrial/about/pages/fatca.aspx**

Federal excise tax (FET)

FET is a tax imposed on insurance premium payments from the US to offshore insurers: 4 percent on direct premiums and 1 percent on reinsurance premiums.

If P&C has entered into a so called closing agreement with IRSD, a US tax administration and all of the insurance premiums paid to If P&C are exempt from this tax based on the US double tax treaty with Sweden.

A list of approved companies and countries is published on IRS web pages **irs.gov/businesses/international-businesses/exemption-from-section-4371-excise-tax** E.g. Norway and Denmark are not in the list of eligible countries, but branch offices locating in these countries may be covered by the exemption granted to the head office.

Reinsurers have closely followed the so-called Validus case, which removed FET from foreign-to-foreign reinsurance transactions in connection with the so-called cascading effect. According to advice received by If, this will not, however, remove the FET obligations of direct insurers or first-layer reinsurers to calculate FET in cases where reinsurance premiums are ceded to a non-tax treaty country.

OECD Base Erosion and Profit Shifting (BEPS)

An OECD project to avoid double non-taxation has proceeded rapidly and is important to all international businesses. It has raised concerns to export business and I'm sure this has been closely followed by the tax departments.

The assessment of its implementation and importance to insurance business is ongoing. The original proposal was even stricter in regards to insurance activities than the final versions. Perhaps two issues could be highlighted at this stage. Firstly, it is claimed that the number of registered permanent establishments will increase. Secondly, as regards international groups and captive solutions, even more attention needs to be paid to the allocation of income. ■

Jari Ostrovskij
Jari.ostrovskij@if.fi

PHOTO: GETTY IMAGES

New If RM-library – **Managing Risks Together 24/7**

If is enhancing risk management services by providing online support for our clients. Irrespective of when and where you need us, you can now get information and tools to help you in everyday loss prevention and safety management.

Consider a company HR manager that has employees in various locations all around the world. What to do in case of a human-induced or natural disaster, in order to get all employees to safety? How about being a new risk manager in a Nordic company that has factories and other premises in distant locations, all over the world? What kind safety measures should you follow to manage everyday safety and prevent losses successfully? Alternatively, think of a company operating with industrial services. The employees are in clients' premises, performing varying tasks in various locations. What kind of industry-specific risks are there? What kind of safety information is available to prevent accidents and incidents?

Disasters, accidents and incidents do not give warning that they are coming. If and when something happens, quick, yet well-advised actions are required to prevent further harm and damage. Information, approved and applicable, is also needed when managing everyday safety and deciding which actions should be implemented in order to prevent losses and manage safety effectively.

To support our clients in various challenges in risk management, If has established an online library. This RM-library is a place where we can provide relevant and useful information. This service is new, aiming to provide help and advice to our clients whenever and wherever it is needed.

The RM-library has been elaborated in co-operation with our clients. It completes our on-site risk management services by providing advice and tools that can be applied independently for successful everyday loss prevention all over the world. The library is not only a novel and evolving service – its groundings have been built in cooperation with If's clients.

Where did it come from?

If's Risk Management Services launched an internal project called EB RM Nordic in spring 2016. EB RM stands for employee benefits risk management, referring to all of the services that help our clients protect their personnel at work, during travel and expatriation, and in leisure time. The aim of the project was to extend our EB RM services to all If countries in the Nordic region, as the services have previously been available primarily in Finland. The history of the risk management service portfolio is linked strongly to Finnish workers' compensation insurance. However, there are major differences in mandatory personnel insurance between countries. We also want to help our clients identify and manage risks that relate to travel, expatriation and leisure time, in addition to those that appear at work. In addition to accident prevention, we also want to promote safety and health, both at work and at home.

> *"Disasters, accidents and incidents do not give warning that they are coming."*

The project had two main goals, namely 1) establishing a truly Nordic service model to fulfil personnel insurance, and 2) enhance the Nordic service portfolio with new person risk management tools and services that meet the Nordic clients' needs in a holistic way. Within this new mindset, it was obvious that the current tools and services need adaptation. Secondly, it was clear from the very beginning that we need to develop new tools and services in order to support various needs, in all countries.

What do clients *really* expect from us?

In order to focus the development work on the right things, it was decided that we will involve our key stakeholders at an early stage of the project. The identified stakeholders included internal ones, i.e., underwriting, sales & client servicing, and the claims department. Respectively, the external stakeholder interviews were targeted to a group of brokers and client companies in Denmark, Finland, Norway and Sweden.

The actual interviews charted what kind of risk management services the clients would like to get from the personnel insurance provider and what the current/forthcoming issues are that the personnel risk management service providers should focus on. The companies represented various industries, so that the findings gave us a good overview of expectations towards If. In addition, we got valuable information regarding current and forthcoming challenges that clients are facing and/or see as emerging issues in personnel risk management.

Evolution of the If RM-library

A major finding from the interviews was that the clients expect information and support in addition to the approved face-to-face on-site services and consulting. The ideal relationship between an industrial client company and the insurer was described, e.g., as "communication partner", where the role of the insurer is rather communication and reflection, instead of acting as an authority.

Based on the findings, it was concluded that we need a Nordic media that helps to deliver information between If and the clients, such that media can also work as the place for such services that the clients can apply independently. This kind of a platform helps us, for example, to provide support in risk management to those clients that operate in various locations (consider travel risks!) or need just information instead of face-to-face service on site.

What is included?

The RM-library was originally a project spinoff from EB Risk Management Nordic. Thus the aim was, during the first stage, to focus it solely on personnel insurance in Denmark, Finland, Norway and Sweden. In that context, the RM-library would and does improve our service capability while helping the clients to have some support in risk management irrespective of the time and place.

In order to serve our clients in a holistic way, it was soon decided that the library should be extended to also include support for our clients for other types of insurance as well. Therefore the library will have separate areas for:

- Personnel insurance types, including
  - travel and expatriation,
  - leisure time,
  - health, and
  - workers compensation (where applicable)
- Property damage & business interruption
- Marine cargo
- Liability

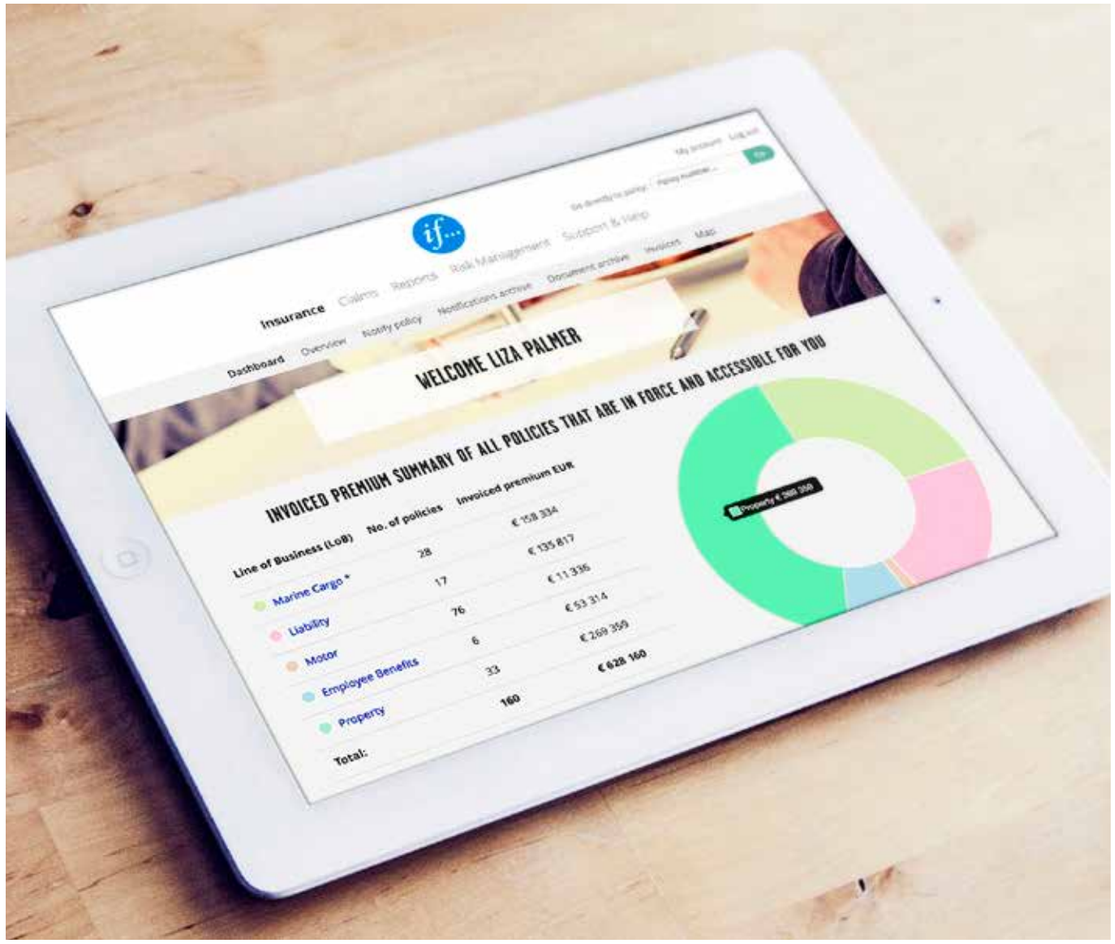
In personnel insurance, for example, the library provides self-assessments for the companies and travellers, in order to support safe travel and advice in sufficient and well-advised actions in case of incidents and emergencies. The library includes information and instructions, such as hazard info sheets, for loss prevention within all types of insurance. The library also includes also numerous links to various external sites that provide good information and additional advice for risk management and loss prevention. The links include both country-specific webpages and other sources of information.

What next?

The first versions of RM-library have been tested internally during autumn 2017 in order to gather feedback and user experiences within If. We have added content that our clients frequently look for. In personnel insurance, specific interest has been paid to meet those expectations that stakeholder interviews and other feedback has indicated. The technical structure has been harmonised and grouped so that the contents are easy to use and manage. Now the RM-library is ready to be published externally, to let it evolve over time and user experiences.

As the project manager of EB RM Nordic, I want to use the final lines of this article as an opportunity to thank all interviewees in each country: your input is highly appreciated. We want to be better than ever to manage risks together with you, now 24/7. ■

Salla Lind-Kohvakka
salla.lind-kohvakka@if.fi



A desirable service experience

If launched this fall its new self-service portal for large corporate clients and brokers.

It is designed to be mobile and tablet-friendly and usability experts have been involved from the very beginning to make sure If will provide a service that is as easy to use as possible.

The New If Login self-service portal, mixed with the open web and our co-branded extranets provides the capability to show information on all levels, from open, to semi-open, to a protected level. This means that all persons at a company will find useful information from us: from the employee who is interested in finding needed information of coverage for health insurance, to a fire engineer, or the payroll officer and of course the risk manager.

"The requirements for a self-service system for large corporations is complex as it must take into account many different users with different needs and access to information. We must provide a system that can differ amongst the users on many access levels, but still be easy to understand and use. I think we have succeeded in this", Technology Leader Anastasija Krjukova says.

The New If Login contains all needed policy documents, invoices with payment status, overview of master programmes, reports and several notification possibilities – and more will come such as our library service, enhanced information of If's international network, and new risk management tools.

The vision is 'a desirable service experience'. "This means the users should not log in simply because they have to find some important document. Our services must be interesting, valuable and even fun to use", shares Project Manager Kristofer Palm. ■

Marianne Wiinblad
mw@if.dk

The Norsk Folkemuseum in Oslo has problems with heavy rainfall. If's drone group has made a 3D-model of the Museun.

Eye in the sky

Drones open new perspectives within risk management.

It is summer, but it is pouring down with rain. Heavy rainfall, surface water and flooding create problems in towns and urban areas.

At the Norsk Folkemuseum in Oslo, cultural treasures have been affected by large volumes of water and flooding for two years in a row. Even though heavy rainfall and weather changes have been subject to much attention in Norway and the rest of the Nordic region in recent years, water, as an unwelcome visitor, is nothing new to the museum. Water has been a regular guest over the decades.

What measures can be implemented to minimise the risk of water that yet again threatens historical buildings and artefacts that are irreplaceable?

In collaboration with the museum, If's new drone group is thoroughly assessing the museum area square metre by square metre. A drone is flying steadily in a coordinate system above the museum's stave church, courtyard with timbered houses and old apartment buildings. The data collected by the drone will be used to create an advanced 3D model of the area. The model may be able to provide some answers regarding which measures are required to tackle heavy rainfall in the future.

"We've only just started using drones at If and are currently in a phase in which we are focusing on experimenting with new areas of application, developing our expertise and gaining experience," explains Cathrine Fjeld Ytreberg, head of If's drone group. In her daily work, she works on solutions for mapping and handling property damage at companies and industrial enterprises.

No one at If is a full-time drone pilot, but this could happen one day. This is because drones can be used in so many areas, both before and after damage has occurred. The Nordic drone group includes employees working with risk management, claims processing and investigations in the private, business and industrial market.

"It's not just films and photographs from a bird's-eye view that can be useful in the work to prevent damage," explains drone pilot Tor Arne Breivikås from If's investigation department.

"We can install other sensors on the drone to measure, for example, the presence of gas or take photographs and films with thermographic or infra-red cameras. And, not least, we can create 3D maps and models simply by flying over an area. This paves the way for looking at areas in which it may be dangerous to enter. We have used this type of mapping following a major landslide. In this instance it was possible to take surveys and calculate the mass volume safely, all based on images and data from the drone," says Breivikås.

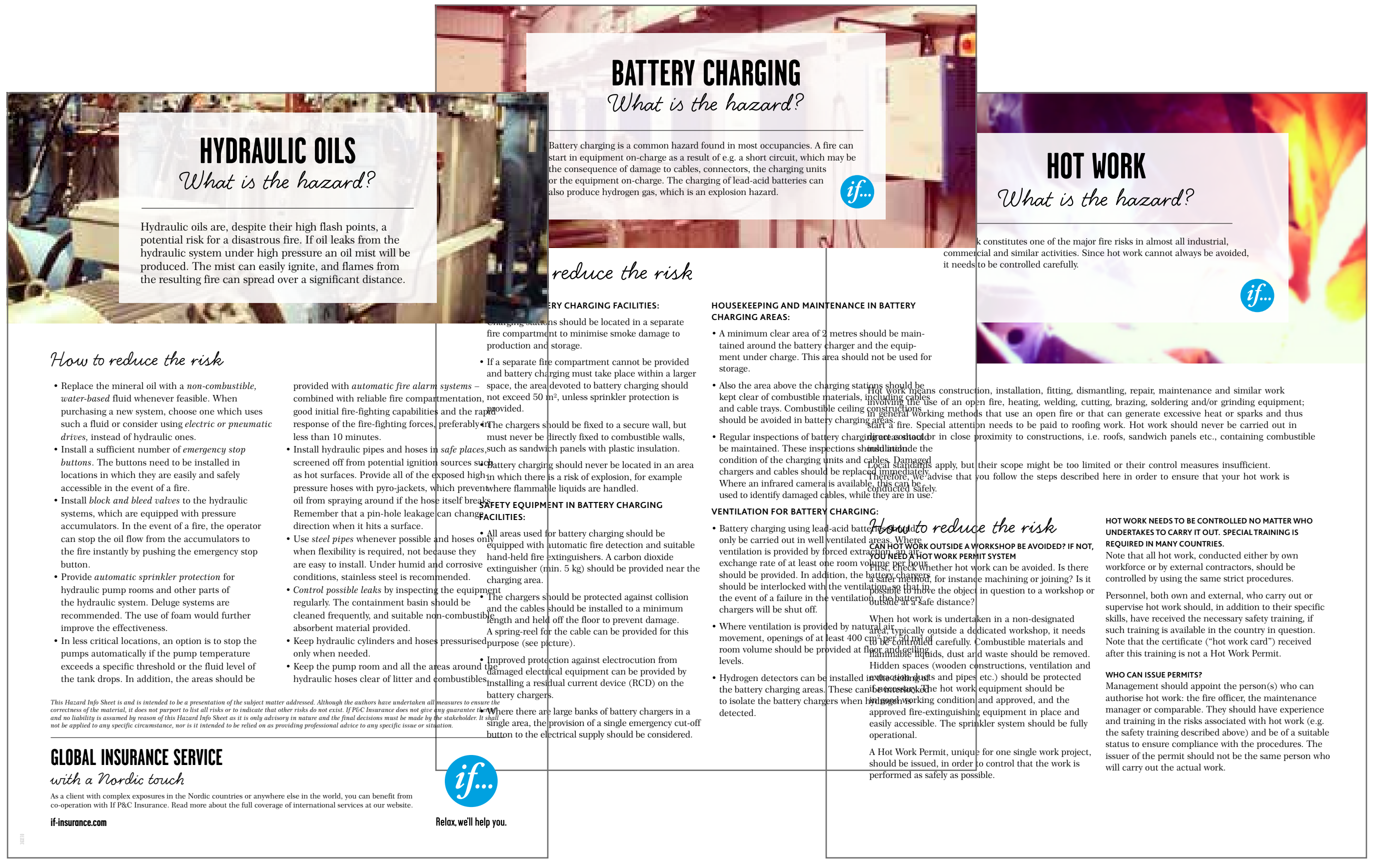
In an incident that is unfolding, like a flood, forest fire or landslide, drones can provide insight that enables the implementation of damage-limiting measures on the spot.

Drone pilot Johan Lunde Wilman adds: "In a few years, we may be using small drones indoors, for example, in production halls, in which it could be useful to have a good overview from a high perspective. We have actually already started experimenting with indoor flights," he says.

Drones are currently being used all over the world in risk-management work – by everyone from contractors to energy companies. Skilled drone pilots fly over large industrial plants, bridges and power lines, in order to detect weaknesses at an early stage and prevent damage.

Cathrine Fjeld Ytreberg believes that the data and visual material collected by If's drone pilots in risk management work will provide useful insight for If's industrial clients. ■

Sigmund Clementz
Sigmund.clementz@if.no



Hazard Info Sheets – **sharing knowledge**

If P&C has a dedicated team of engineers who provide guidance on risk mitigation in a range of disciplines and occupations.

To share our knowledge and facilitate communication with our partners and clients, we provide Hazard Info Sheets that deal with some of the risks common to almost any industry. The sheets briefly describe the risk in question and give clear and easily understandable advice on how to reduce it.

You can browse our Hazard Sheets and other helpful documents and checklists on our website.

The aim of the Hazard Sheets is to spread awareness of typical risks – general information on how to avoid and mitigate them. We encourage companies and partners to distribute the sheets within their organizations. The documents can be used as discussion materials in morning meetings, published on information boards in factories and intranets, or distributed to employees and contractors assigned to your premises.

Hazard Sheets are compiled by our expert engineering team to help clients of all types better understand the risks in whatever industry they are working. Among the Hazard Sheets we currently hold in our library is the Battery Charging Sheet, which explains why battery charging is a common fire hazard. Another example is the Hot Work Sheet, which outlines why Hot Work is a major fire risk in almost all industries, while the Hydraulic Oil Sheet describes the common risks facing hydraulic oil installations. We intend to develop our library of common hazards, drawing on experience of losses that we have processed here at If P&C and in dialogue with our partners. Hazard Info Sheets are advisory in nature, provide a general introduction to risks and should not be relied on as a source of professional advice on any specific issue or situation. Our engineers will elaborate on the related topics in more detail with our clients, to find the most suitable solutions for specific situations.

Please visit our internet page to see if there are any Hazard Info Sheets that could be informative for your organization. The documents will also be available in our RM-library, and you are welcome to contact your If contact person and we will be happy to provide you with the Hazard Info Sheets that you are interested in. ■

if-insurance.com/web/industrial/riskmanagement/propertyandbusinessinterruptionrisks

Fredrik Holmqvist
fredrik.holmqvist@if.dk

GETTY IMAGES

Internet of things – new visions, new risks

Consultant company Gartner defines Internet of Things (IoT) as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."

There could be up to 80 billion devices connected to the internet and each other by 2025. The prevalence of wireless connection makes it attractive to connect to the internet all manner of devices, ranging from industrial processes to home appliances like webcams, refrigerators and smart TVs. This leads to unprecedented automatization and improved efficiency and also new business models and opportunities through enormous amounts of data created and collected from all these sources.

This is part of the revolution in digitalized information and network-based computing. The connectivity will enable mobility, remote control and information flow paving the way to new applications like autonomous vehicles.

There is a price to these visions. The connected devices form new risks from the individual gadgets to cloud services. In 2016 there were several denial-of-service attacks conducted also by hacking IoT devices, affecting the availability of several large service providers like Amazon, Netflix and Spotify. This shows that devices with communication capabilities may have security vulnerabilities that could be misused and cause serious harm.

Besides the manufacturers, also the regulators are working on the cyber risks of IoT, but the standards are still undeveloped. It has been said that IoT will stand or fall depending on cyber security.

The traditional liability regimes are also trembling. Of course tort law on compensations due to injury or damage caused to others is valid, but the causal links may be difficult to establish. Currently product liability is the responsibility of the manufacturer of the physical product. But there is no systematic way of handling damage caused in the net through other mechanisms. The risks increasingly involve financial losses, which makes it even more difficult.

The EU is working on these themes on several levels. The Commission arranged a study on whether the current Product Liability Directive is sufficient in terms of new technological developments, such as the Internet of things and autonomous systems. The European Parliament is conducting a study on European civil law rules on robotics.

The manufacturing industries or the insurance industry have not been so enthusiastic of new regulations or liabilities because of the complexity of the issues and uncertainties of the developments. But somehow we must go forward and try to sort out the new risks and their prevention. ■

Matti Sjögren
matti.sjogren@if.fi

PETER GRANLUND
IT Security/IT Risk Management Specialist, Nordic

SVEN THESSÉN
Property Underwriter CAR/EAR and Energy, SWE

CHRISTINA WIKLUND
Liability Senior Underwriter, SWE

MIKAEL MØLLER-HANSEN
Head of Property UW, DK

KRISTOFFER REUSCH TANDSTAD
Liability Underwriter, NO

CLAUS FORBERG
Liability Underwriter, DK

HENRIK KARLSSON
Risk Engineer, SWE

"As an insurance company, we have the privilege of working with the digital risks of almost all industries."