RISK CONSULTING

IF'S RISK MANAGEMENT JOURNAL 1/2019

Li-ion batteries – a fire hazard

Physical security controls for IT and ICS

Sustainability in Claims and Loss Prevention

Making complex business simpler

IN AN INCREASINGLY complex and fragmented world where risks, activities, responsibilities, and employees are located all over the globe, services enhancing the ease of doing business are crucial.

Our client and broker platform, If Login, provides an overview of your risks all over the globe. An interactive world map gives a simple and easy overview of expat locations, stored cargo, and all insured sites – globally. With a quick zoom and a click, all the documents and policies in a selected location are shown.

Claim statistics, claim status, correspondence, and actions on all claim cases can be followed in If Login, and specific claims can be followed for updates. All this in a secure environment.

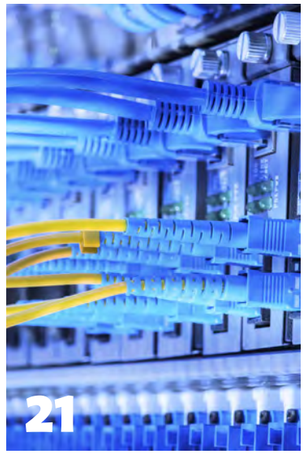
Nothing beats personal contact. A full overview of all If employees working with your business is available in If Login – from your dedicated account executive to the underwriters and your local insurance providers around the world.

We strive to be the partner who creates an overview and simplicity in your insurance-related activities. Our ambition is to manage risks together with you.

We would like to explore If Login with you. But right now, we thank you for exploring Risk Consulting Magazine. In the magazine, as on if-insurance.com and at our client events, we share knowledge so that corporations can learn from best practices and avoid large losses.

We hope the magazine provides useful insights into a simpler future.

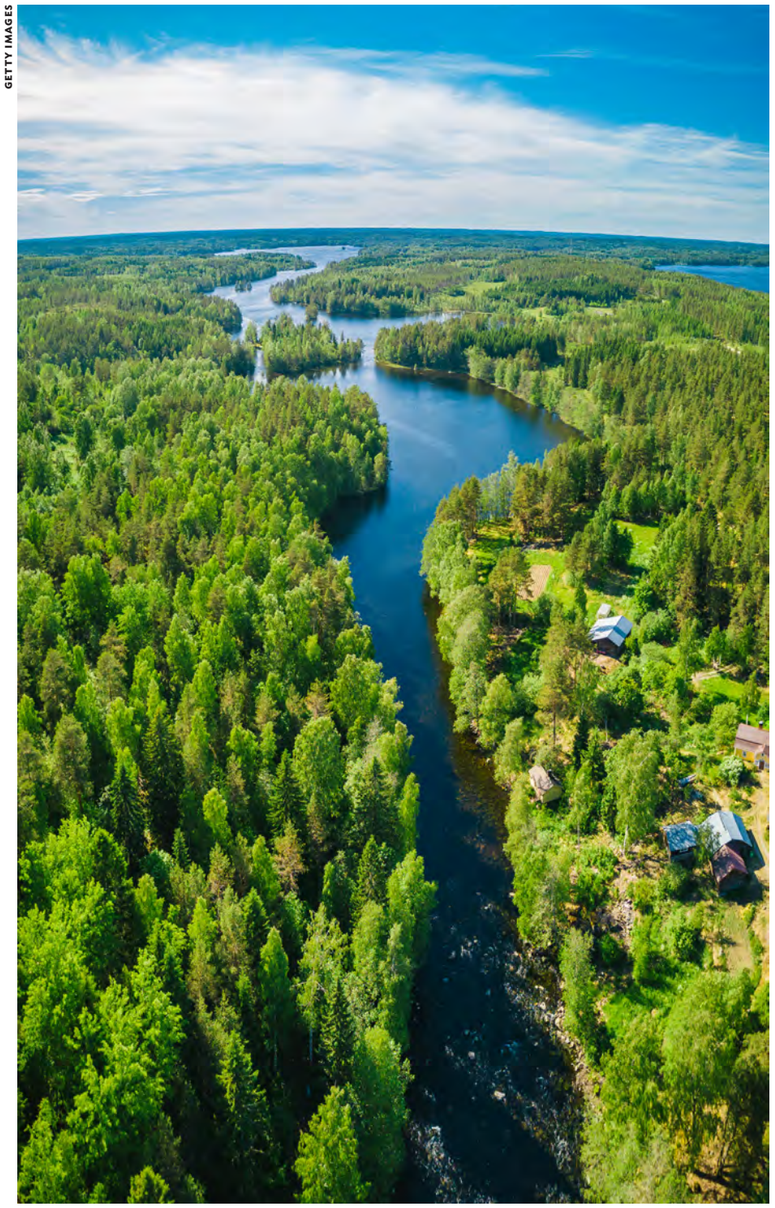
POUL STEFFENSEN
Head of BA Industrial, If



If P&C Insurance, contact information

Finland +358 10 19 15 15 **Sweden** +46 771 43 00 00 **Norway** +47 98 00 24 00
Denmark +45 7012 24 24 **France and Luxembourg** +33 1 42 86 00 64
Germany +49 6102 710 70 **The Netherlands and Belgium** +31 10 201 00 50
Great Britain +44 20 7984 7600 **Estonia** +372 6 671 100
Latvia +371 7 094 777 **Lithuania** +370 5 210 9800
wwww.if-insurance.com

Publisher If, Niittyportti 4, Espoo, FI-00025 IF, Finland, +358 10 19 15 15, www.if-insurance.com **Editor-in-chief** Sigmund Clementz, **Sub-editor** Carita Hämäläinen-Tallgren, **Editorial board** Fredrik Holmqvist, Andreas Kräling, Reija Laatikainen, Anders Rørvik-Ellingbø, Pekka Sarpila, Ida Tuononen, Marianne Wiinblad, **Production** A-lehdet Oy, **Printing** Forssa Print, **Changes of address** industrial.client-service@if.fi **ISSN** 1459-3920. **Cover photo:** Boliden.



GETTY IMAGES

Trees reduce flood risk

PLANTING TREES CAN lessen flood risk, but a high intensity forest land use, such as grazing, can counteract the positive effect of the trees, a new study suggests. When rainfall exceeds the rate at which water can enter the soil it flows rapidly over the land's surface into streams and rivers. Trees can help to reduce the risk of surface runoff by increasing the number of large pores in the soil through which water can drain more easily. The study, undertaken by Lancaster University and the Centre for Ecology and Hydrology and published in the journal Geoderma, investigated the rate that water infiltrated the soil under trees at an experimental agroforestry site in Scotland. Researchers found that infiltration rates were between ten and a hundred times higher under trees, when the forested area remained relatively undisturbed, compared with adjacent pasture. ■

Fire protection on the rise worldwide

The global fire protection materials market size is anticipated to grow to around USD 9.9 billion by 2026. This market is anticipated to grow with 8.6 percent during the forecast time period, according to Acumen Research and Consulting. The market is foreseen to develop with the execution of fire safety regulations and strict construction regulations. There are additionally different authority models built up to neglect and guarantee item adequacy. Enhancing frame of mind toward building safety codes, alongside expanding fire danger occurrences, is foreseen to support offers of flame insurance materials around the world.

Keys and chips are vulnerable hardware

Researchers have developed an algorithm that safeguards hardware from attacks to steal data. In the attacks, hackers detect variations of power and electromagnetic radiation in electronic devices' hardware and use that variation to steal encrypted information, according to researchers at the University of Wyoming and the University of Cincinnati. Devices such as remote car keys, cable boxes and even credit card chips are all vulnerable to hardware attacks, typically because of their design.

Attack traffic up by 32 percent

New research from cyber security provider F-Secure reports a significant increase in attack traffic last year. But while attacks are increasing, it seems many companies are struggling with incident detection. Attack traffic observed by F-Secure's network of decoy honeypots in 2018 increased by 32 percent over the previous year. The companys survey found that 22 percent of companies did not detect a single attack in a 12-month period. 20 percent of respondents detected a single attack during that time frame, and 31 percent detected two to five attacks.

■ ■ 2018 was the fourth-costliest year since 1980 in terms of insured losses from natural distasters for the insurance industry, according to Munich Re. The figure for insured losses – 80 billion US dollars – was significantly higher than the 30-year average of 41 billion dollars.

GETTY IMAGES

Powder coating
What are the risks?

The process of applying powder coating is a potential fire hazard. Therefore, a company installing or operating a line must ensure that the equipment meets local regulations and good practice guidelines.

In workshops throughout the world, spray painting is performed on a range of products, from small, individual items to full car bodies and other large items, on continuous production lines. The paint can be in liquid form and can be either solvent or water based. Coating can also be applied through an electrostatic powder coating process, which has been popular in the metal manufacturing sector since it was first introduced in the 1960s. Manufacturers can apply the powder coating efficiently, and the cured coating provides good corrosion protection while also being cosmetically attractive. Risk engineers at If see many varieties of paint-shop installations when visiting our clients, with paint being applied both manually and automatically by robots.

The hazards associated with paints and solvents are toxicity and flammability. Even though there might be a lower level of hazards associated with using powder coating compared to conventional solvent-based paints, the process of applying powder coating is a potential fire hazard. Therefore, a company installing or operating a line must ensure that the equipment meets local regulations and good practice guidelines.

The dust cloud

AVK Holding A/S is a family-owned company headquartered in Galten, Denmark, with subsidiaries manufacturing different types of valves used in water and wastewater distribution, fire protection water supply, industrial applications, and gas distribution. AVK operates throughout the world with factory footprints on most continents.

If P&C took over the property insurance for AVK some years ago. There are many different work processes at the AVK sites, including metalworking with surface treatment, such as electrostatic powder coating, epoxy coating, and enamelling of metal components. Before the coating process is carried out, the components are typically blast cleaned before being painted.

Many of the paint lines at AVK are electrostatic powder coating lines, where a fine dust is sprayed onto a grounded workpiece. The spray application system is complete with electrostatic charging of the powder coating to charge the particles and effect a high level of transfer to the grounded workpiece. During the coating process, the components are heat-treated in a pre- and post-cure oven, where operating temperatures are 190-200°C.

"A fine dust cloud can form an explosive atmosphere."

One of the hazards involving powder coating is that a fine dust cloud can form an explosive atmosphere when mixed with air, and this can cause an explosion and fire under unfavourable conditions.

AVK is very much aware of the risks involved with the powder coating processes, and according to ATEX 137, workplace directive 99/92/EC, states the minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres. It is important to handle the risk with respect, even in small paint units, as powder coatings, being fine organic materials, can give rise to dust explosions and contact allergies.

The ATEX directive consists of two EU directives describing what equipment and work space are allowed in an environment with an explosive atmosphere.

The ATEX directive covers explosions from gases and also from solid dust, which, contrary to common belief, can lead to hazardous explosions. Hazards relating to explosion risks are: gas/vapour/mist and powder/dust. All equipment used in hazardous (zoned) areas must be 'ATEX Compliant' and must be suitable for the zone in which it is used.

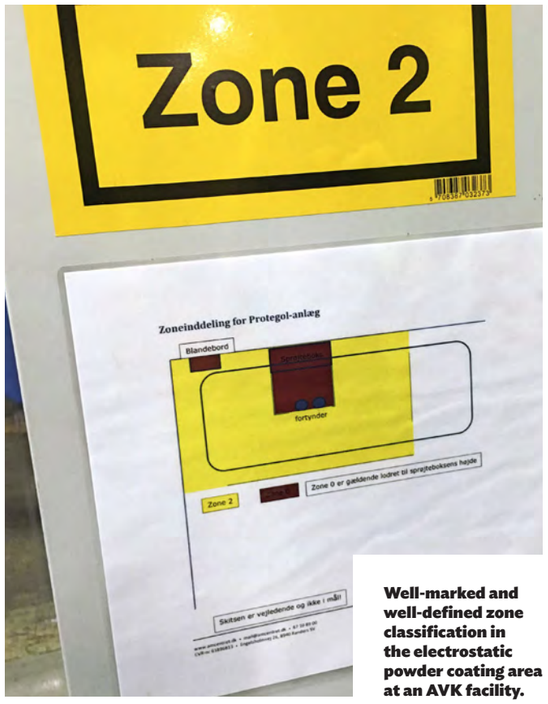
Identifying risks

AVK runs a strict routine to identify potential hazard zones and potential ignition sources, and to provide adequate ventilation and powder collection systems. Ignition sources can include all open flames and welding activity, hot surfaces, and mechanically generated impact sparks; for example, a hammer blow on a rusty steel surface compared to a hammer blow on a flintstone. Electric sparks are also common ignition sources, for example, a bad electrical connection or faulty electrical equipment. It is also important to control the electrostatic discharge risk. Static electricity can be generated by air sliding over a wing, or a non-conductive liquid flowing through a filter screen, and so on, and there are many more potential ignition sources. It is therefore important that a skilled professional is consulted when evaluating the hazard zones and the potential ignition risks. Earthing of equipment is a focus area when installing a paint unit or preventing the formation of static electricity, among other things.

The risks vary

The layout of the paint facility is also highly important, to ensure safe escape routes, good ventilation and extraction systems, and good access for emergency services in the event of fire. →

Valve components on conveyors after the powder coating and heat-treatment process.



Well-marked and well-defined zone classification in the electrostatic powder coating area at an AVK facility.

When it comes to the ventilation and powder collection systems, it is important that the systems are designed to minimise the amount of overspray, and excess powder is removed by exhaust extraction and collected for re-use or disposal.

Enclosed filter membrane collectors and cyclone collectors should be provided with explosion relief unless the openings that are provided give sufficient protection. The collection unit should preferably be located outside in a safe place, with the minimum enclosure required for weather protection. If it is necessary for the dust collection unit to be sited indoors, it should be in a separate area away from the working area.

"The potential risks involved with paint shops are many and they vary."

"The potential risks involved with paint shops are many, and they vary from site to site", says Bo Johansen, Group Production & Supply Chain Director at AVK Holding A/S. "It is therefore important that a thorough risk assessment is carried out on a case-by-case basis. It is the local production and facility managers' responsibility to, among other things, ensure the necessary ATEX assessments in this context".

AVK also works with automatic fire detection and suppression systems to detect, extinguish, or control a potential fire in paint lines that are of vital importance for their business. This is something our engineers acknowledge as highly effective in limiting loss in the case of a fire.

Another focus area when visiting a plant is whether the surrounding construction material encapsulating the paint area is made of the right material. We sometimes see clients using steel sandwich panels with combustible foam insulation for this kind of construction, especially for noise and dust reduction purposes, which in our opinion is a bad choice. Non-combustible steel sandwich panels are preferable. An AVK subsidiary with a production site in Spain planned to establish a new spray-painting cabinet with steel sandwich panels including PIR insulation, and in connection with a recent risk survey, an If engineer recommended that AVK should use non-combustible insulated steel sandwich panels instead. This led to alterations in the choice of material, to a non-combustible solution, without compromising the function of the design and without further costs to AVK.

Bo Johansen at AVK also points out that human elements are of great importance and employees need special training when working with explosive atmospheres. Wearing high-quality protective clothing and equipment is also vital when called for. AVK is fully aware of the need for good housekeeping and runs a strict housekeeping and maintenance regime in connection with their paint shops.

The list of hazards and risks related to paint shops and powder coating is long and only briefly touched upon in this article. As Bo Johansen concludes, it is important that a risk assessment is carried out by qualified technical personnel on each individual production site, and in this context, If has been able to provide valuable additional input. Risk engineers at If also emphasize that it is important to keep up with new knowledge and solutions that can help to avoid accidents and losses. Even if spray painting is a common practice and powder coating has been around since the 1960s, the equipment and surrounding protective applications are constantly evolving. ■

HANS RAEDER
hans.raeder@if.dk

Are cement-bound wood boards really **non-combustible?**

Compared to pure wood products, cement-bound wood boards have improved fire properties.

Cement-bound wood boards have been manufactured and used for construction purposes since early in the 20th century, and widely used throughout Europe since the 1930s. The boards are composite materials and come in several forms. Common to these are wood fibres bound with cement to create good insulation properties, durability, and improved fire-resistant properties of the wood-based material.

Fire ratings are often significantly better than pure wood panels, with approvals B-s1, d0, meaning difficult to ignite and a slight contribution to fire growth. Some panels can even be classified as A2-s1, d0, which signifies no contribution to fire growth, non-combustible, with combustible material to a minor extent. However, the tests used for such a classification are the approved "Reaction to fire test", in which the material is exposed to a relatively small fire source for 600 seconds, after which the energy source is removed. In a real fire, the energy source cannot be removed, and would instead grow rapidly, and in our experience, even cement-bound wood boards contribute to the fire.

The boards are often only part of an insulating construction, and roof constructions, in particular, can consist of a layer of cellular plastics above or in between wood panels. Any penetration or damage to cement-bound boards will expose the cellular plastics, which can create fierce fire conditions. Cellular plastics such as EPS and XPS normally melt when presented with temperatures above 150°C, creating pool fires that penetrate the wood panels. We have also seen real-life fires in which the structural wood bars used for mechanical strength inside the boards are damaged by heat exposure from a fire, with the risk of collapsing elements.

Compared to pure wood products, cement-bound wood boards certainly have improved fire properties. However, the boards are nonetheless flammable, and will burn in a real-life fire and flashover. Other factors, such as aging and drying of the components, but also accumulated oil vapours on the panels, are likely to have a negative effect on the combustibility of the panels.

In line with all other construction materials with a grading of B or D (combustible), we recommend taking actions to prevent fire from becoming established in the construction element. Strict guidelines and limitations for hot work, awareness of electrical installations, and the location of waste bins should be addressed and implemented when such boards are used. ■

ANDERS RØRVIK ELLINGBØ
anders.ellingbo@if.no

PHOTO: XXXX XXXXX

Li-ion batteries – a fire hazard

Physical damage to battery cells, pollution in the electrolyte or the poor quality of the separator may cause a fire in li-ion batteries.

Investigators from If checking li-ion battery cells that started the fire.

In June 2018, a client of ours experienced an explosive fire in a Lithium-Ion battery used for a custom-built electric bike. The owner of the bike was about to show the battery to his family when it suddenly caught fire lying on the kitchen table! The battery was not connected, neither to the charger nor to the bike. The fierce fire, experienced by our client as being like fireworks, could not be extinguished, and the fire spread to the interior and the building structure, causing a near total loss of the building. Our own investigators have done technical studies of the damaged battery and the battery cells. The probable root cause of the fire is physical damage to the battery, causing thermal runaway in the battery. The built-up pressure was released through cracks in the first battery cell affected, causing thermal runaway in some of the other cells.

Root cause of the fire

Senior researcher Helge Weydal, at the Norwegian Defence Research Establishment (FFI), explained the hazards of Li-Ion batteries in an article in Risk Consulting issue 2/2017. Fires can be caused by physical damage to battery cells, such as that which our client experienced, or they might also be caused by pollution in the electrolyte or the poor quality of the separator.

Countless numbers of devices

The number of devices using Li-Ion batteries in households and businesses worldwide is enormous. We are surrounded by billions of devices: mobile phones, laptops, radios, cameras, flashlights, radios. Equipment that consumes even more energy, such as lawn mowers, other power tools, and in the Nordic countries even rotary snowploughs, belong to households. Electric cars are coming rapidly into several international markets. Buses, ships, ferries, large trucks, and even aeroplanes are being developed for commercial purposes, all using Li-Ion technology as the power source. Large Li-Ion battery banks are used in power storage for optimising solar power technology.

"We are surounded by billions of devices."

Fire statistics trends

Is there an increased risk of fire in introducing all these devices into our homes and workplaces? Our statistics do not show any clear trends, considering the enormous number of units. We receive fire claims caused by batteries in or charging for flashlights, electric bikes, drones, radios, and even children's toys. But still the 'normal' root causes, such as electrical faults, not following safety manuals, oil fires, and hot work, are much more common sources of fire.

Looking across the Atlantic to the US, interesting stories unfold. During the past few years, up until 2017, more than 500.000 hoverboards were recalled after at least 99 reported events of smoking, fire, or explosions in devices, according to the Consumer Product Safety Commission. After introducing strict guidelines for approving batteries for hoverboards, the problem seems to have nearly disappeared in that market.

E-cigarettes

The US Navy banned the use of e-cigarettes after 15 incidents in less than a year caused injury to personnel or material damage. The statistics by the Federal Aviation Administration (FAA) build up for this concern. Looking all the way back to 1991, the authorities have registered all events of overheating, smoking, or fire in Li-Ion batteries in passenger and cargo aeroplanes or registered at airports. The curve grows steeper every year with the increasing number of devices in our society. There were 238 reported incidents over the whole period, of which 94 occurred just in 2017–2018. Of these 52% occurred either in battery packs or e-cigarettes, and 18 % started in mobile phones.

The list of recalls over the years is long. A quick Internet search shows HP and Dell laptops have experienced recalls, as well as the Samsung Galaxy Note 7 and even battery-powered radios.

Electric cars

Electric cars are seldom the centre of attention related to battery fires, but there have been some examples of wrecked cars with heavy damage to the battery pack causing thermal runaway and fire. Not only can the batteries form a fire risk. In the case of electric cars, even though they have several built-in safety barriers in their battery and charging systems, the use of so-called emergency chargers in regular sockets can lead to overvoltage and fire in electrical switchboards or in sockets. Remember the power needed to charge such large batteries might often create much larger resistance in the circuits than they were originally built for. Correctly dimensioned over-voltage protection must be fitted, alongside the use of fuses that are adequate for such charging.

If Insurance investigators in Finland decided to examine whether driving nails through the battery pack of an electric fat scooter would cause a fire.

High-energy fire

Taking a step back, given all the devices on the market, the number of fire incidents is not very high. The problem is the fierce fire experienced, just as in our client case mentioned above. A Li-Ion fire is difficult to fight due to the chemical reaction continuously creating oxygen.

Mitigating fire risk

There are several mitigating actions taken by battery suppliers to prevent fire from occurring. As Helge Weydal Larsen explains, there would normally be built-in surveillance of charging and battery status. An X-ray of all batteries, to ensure the electrolytes are not polluted, is a precaution used by serious battery producers. Power tools are often considerably better protected from external impact and damage than regular consumer goods.

Why is all this important information for industrial businesses?

During our client visits, we often come across private devices such as radios brought to the workplace, power banks, and e-cigarettes.

A common recommendation issued in loss prevention reports is that the employer must keep track of these devices. Private electric and chargeable devices should be inspected and approved before allowing employees to bring them to work, regardless of the power source.

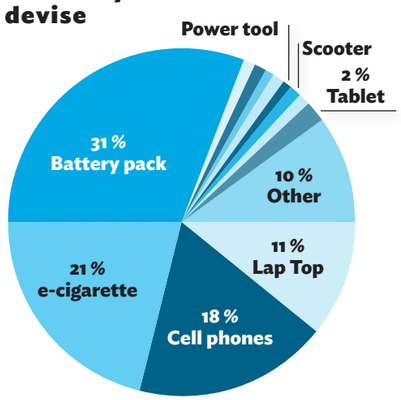
Means of getting around

In the larger industrial estates and warehouses, we can often find employees using kick-scooters to cover large distances rather than walking on foot. Introducing electric kick-scooters or fat scooters might be even more tempting. However, be aware that this might introduce a new fire hazard to the company. Tests done by our investigators clearly show that physical damage to battery packs might start a thermal runaway in the battery and consequently a fire. Rough handling of scooters at the workplace can therefore, in a worst-case scenario, cause injury to personnel or a fierce fire.

With the introduction of large battery banks storing power from PV panels for later use, a new fire risk can occur. These banks should be stored in separate fire compartments and protected with proper extinguishing systems, or preferably located an adequate distance from the production buildings. This could be the difference between an isolated battery fire and total damage of the location.

ANDERS RØRVIK ELLINGBØ
anders.ellingbo@if.no

Reported recalls by devise



Better battery safety

Make sure the batteries used in your business are of high quality and approved according to relevant standards.

- Inform all employees of the possible fire hazard. This is also good employee policy, caring for their safety.
- Do not allow employees to bring personal Li-Ion devices to the workplace without approval.
- Ensure charging is done in a safe manner, and ensure that electrical systems are properly dimensioned.
- We recommend that charging is only done on a non-combustible base, away from any storage, and in areas with properly fitted smoke detection.
- Make sure that devices exposed to rough handling and damage are inspected. Greater than usual heating of the device when charging or during use is a sign that something is wrong.
- Make sure connections are properly fitted and undamaged, to prevent electric arcs.
- Follow airline regulations for transporting and handling battery-powered devices when travelling.

ISTOCK

Safer and more secure travel

Travel safety and security are becoming increasingly important in all companies. Travel related risks need to be managed in a holistic way.

For business travellers there is often more urgency with these issues, as business interruption is an issue, along with greater concern about more severe incidents like kidnapping, terrorist attacks, and epidemics like Ebola and Zika. The increasing value of companies' data as intellectual property also brings concerns about IT security and cyber threats while travelling.

Duty of care

Nordic companies are becoming more and more international, resulting in more employees both travelling and working abroad. The employer needs to take the possible implications into consideration, from ethical and legal perspectives.

"Duty of care means the employer's comprehensive obligation to take care of its employees. It is both a legal and a moral obligation. Duty of care is emphasised when employees travel and work in foreign environments. It is about the employer ensuring that the employees are adequately protected while under employment, be it at home or abroad", If's EB (employee benefits) underwriter Hannele Sääksvuori says.

Duty of care consists of several different areas, and by considering and fulfilling these, the employer can ensure that the duty of care is carried out.

Careful planning and preparation

On a general level, planning can mean an up-to-date travel instruction, which is more in-depth than just the hotel category and reservation rules. The travel instruction creates the grounds for ensuring that nothing happens, as well as the framework for if something does. This means instructions to ensure that everyone knows who needs to act and how if something were to happen. These instructions should include crisis plans for more severe incidents.

Up-to-date information on the safety of the destination country, both gathered for the destinations and specifically for the trip, is another crucial part of preparing and planning. This should contain health safety information, such as possible epidemics and other health threats, and information on the political situation and other everyday safety concerns at the destination.

The state of the travelling employee's health also needs to be considered e.g what possible acute or chronic health issues might affect travel or increase the risks while abroad. This is, of course, an area to be sensitive about, remembering privacy as much as possible.

Furthermore, it's important that all planning, instructions etc. are documented as proof of duty of care.

Work safety and safety while travelling

Work safety at the destination is also an important fact to consider: what kind of environment the employee will be placed in, what kind of safety measures are in place in case of accidents, and what kinds of risks are included in the commute, and so on.

Safety while travelling, meaning safe transport and accommodation, is also to be considered: what kind of transport is chosen for travel to/from the airport and at the destination, and how safe this is; and what kind of accommodation is available at the chosen destination and what possible safety concerns might be related to that. Travelling in known dangerous areas or destinations has to be considered in more detail, and more detailed instructions need to be given.

Adequate insurance

"Ensuring that the travelling employees are adequately insured is one of the key factors in duty of care. The employer needs to make sure that the insurance coverage is sufficient and relevant, and one needs to ensure that special circumstances are also covered, such as ambulance flights to the home country in case of emergencies", Hannele Sääksvuori says.

Another important thing to consider is a professional and capable partner in emergency services. Considering distance and time differences, this is often the first contact for the employee and an invaluable help in big and small emergencies.

"Cyber threats and the need to consider IT security are increasing fast. A company's value is more and more tied to intangibles like data, intellectual property, and technology. This also brings an increased risk of cyber threats and theft. These are issues that need to be considered in every aspect of the company's operation, but travel is an area where safety might be more easily compromised", If's chief information security officer, Peter Granlund, says.

There are a few easy areas to consider when trying to guard against cyber threats while travelling.

Device security

When it comes to keeping your devices secure, a simple rule goes a long way: don't let your devices out of your sight. When travelling, keep your electronic equipment in your carry-on luggage to avoid potential in-flight loss or damage. Remember, too, not to leave valuable or sensitive electronic equipment lying around in your hotel room. Always lock up electronic equipment when it is not in use.

Password protection does not keep your devices from being stolen but will protect intellectual property. Always use passwords on all devices, and ensure that device encryption is enabled on computers and Android devices (it is done automatically on iPhones and iPads).

Even with password protection and encryption, thieves might try to hack into stolen devices. Enabling settings that erase all data if the password is entered incorrectly ten times can help ensure that no data can be accessed if the device gets stolen.

To keep your data safe, also activate cloud backups of photos, emails, documents, and settings. Even if your device is stolen, if you have a backup then you don't lose valuable data.

A few more useful tips are to keep your computer updated, so that all operating systems and applications run smoothly and securely, and to write your name and local address on the screensaver with a reward, in case the device is lost, making it more likely to be returned to you if it is found by someone after a theft.

Wi-fi and mobile security

"In addition to the physical devices, the connections used are a major threat to the security of your data", Peter says.

"One of the clearest things is to stay away from unsecured networks. This includes public wi-fi at airports, railway stations, and cafes. This is especially important if you are accessing sensitive data such as internet bank or payment services", Peter continues.

The risk with open wireless networks is that you never know who is connected and, in the worst-case scenario, eavesdropping on your traffic. Most of the major services on the internet today use encryption to protect login and subsequent traffic, but if you log into a service that does not use it, someone who is eavesdropping may see sensitive data in plain text.

In addition, if someone were to set up a wireless router with the same name as a known network, such as "Airport Wi-Fi", your devices may automatically connect to that router if the signal is stronger. Then the person controlling the router can see the places you visit and can redirect your traffic to a page of their own, designed exactly like the original, but which actually steals your login details or gives the attacker access to your data. All of this can happen without you noticing it.

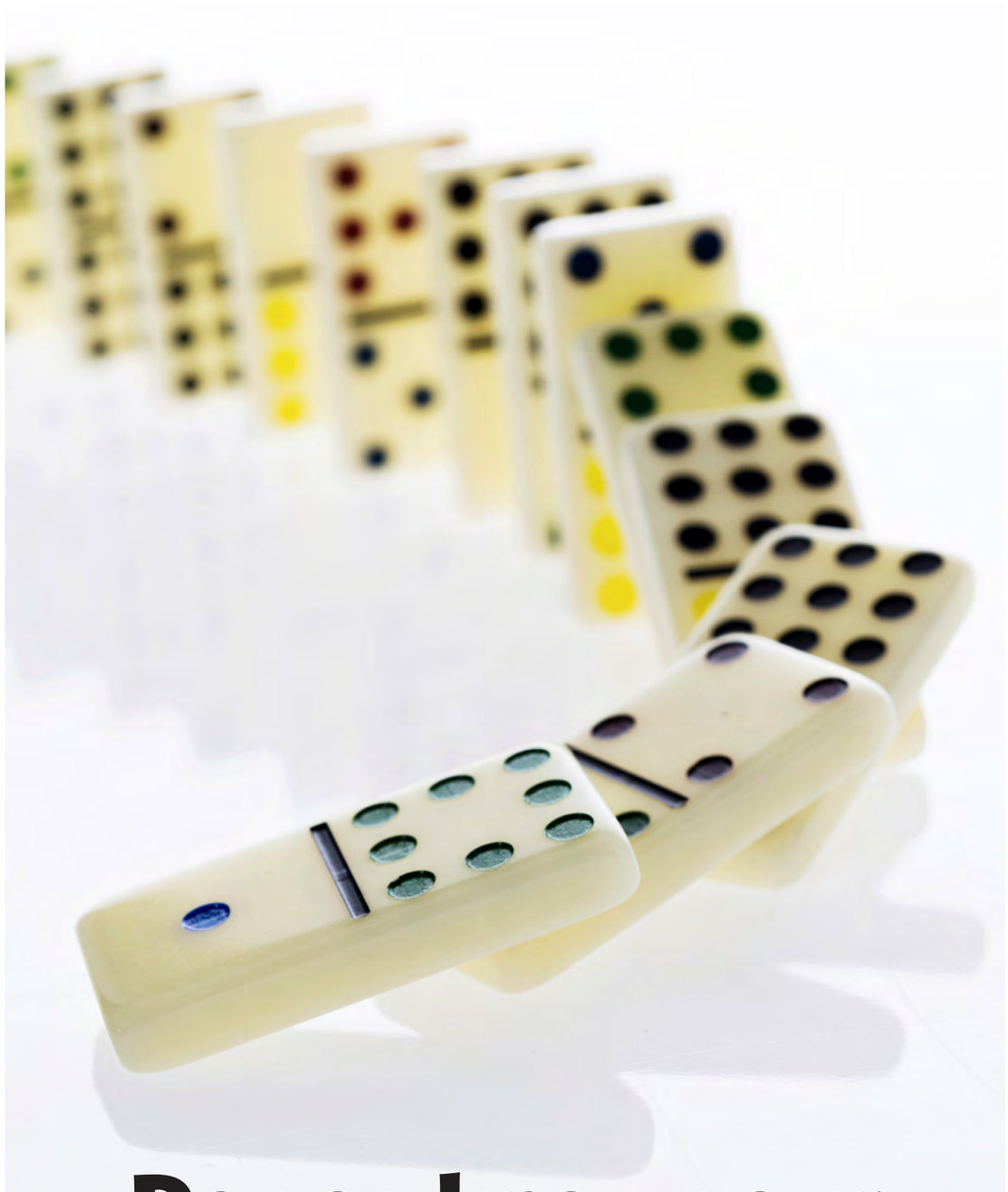
"Since June 15, 2017, the cost of so-called roaming, when traveling in other countries, has been removed within the EU, Norway, Iceland, and Liechtenstein. Since it is much harder to attack mobile networks than wi-fi networks, accessing data that is sensitive or has great personal or financial value should be done over 4G or 3G networks", Peter says.

One good security measure is to use a virtual private network, VPN.

In a VPN, the data traffic from your device is sent via an encrypted connection to the VPN provider's internet connection, regardless of whether this is done over an unprotected wireless network or not. This makes it much more difficult for an attacker located close to you to eavesdrop on or redirect your data traffic.

Furthermore, should the VPN gateway that sends and receives your internet traffic be located in your home country, you may find it possible to access content that is not accessible outside your home country, such as streamed TV and radio channels. It is important to keep in mind that in some countries it is illegal to use VPN, so it is good to check in advance.

IDA TUONONEN



ISTOCK

Do you know your interdependencies?

A company can be dependent on parties outside the company, in the form of external dependencies such as suppliers and public utilities, as well as on parties within the Group.

In the effort always to improve and become even more competitive, one of the steps is to specialise: to do more of what you are really good at. In a company, this could have the effect that some steps in the process are done by one part of the Group while other production sites in the Group execute other parts of the production process before the end product reaches the final customer. This way of becoming even more competitive will affect the risk and also the cover in an insurance programme.

First of all, let's start with what we at If P&C mean by interdependencies. Looking at dependencies, a company can be dependent on parties outside the company, in the form of external dependencies such as suppliers and public utilities, as well as on parties within the Group.

We define the internal dependencies, called interdependencies, as the business interruption impact that a claim will have at another site within the Group, or the impact that will arise at another legal unit within the same Group, either at the same site where the claim occurred or elsewhere. To spot the interdependencies, we therefore have to look at both the process before the end product reaches the end customer and the business model applied within the Group. The impact on the process within the Group can be seen as the impact that a site will have both up-stream and down-stream within the Group, as the process flows towards the end customer. The business model often means that the ownership of a product changes within the Group, from one legal unit to another, so that different prices are set, creating margins in the process. The most common change might be the addition of some margin from a producing company within the Group, when the ownership is transferred to a selling company within the Group.

A Chain reaction started

The topic of interdependencies became really "hot" after the major international natural catastrophes starting with the Japanese earthquakes and the flooding in Thailand in 2011, when many insurers and companies were surprised by the huge and complicated chain reactions that came as a consequence of single factories getting hit. When an insurer tries to see what kinds of risks a company is asking to transfer to the insurer, a very important step is to estimate what the maximum impact of a claim could be at the sites belonging to the insured. This estimate is called EML at If, and similar names at other insurers. The effects of interdependency after the above-mentioned disasters were much higher than anticipated, which is why the insurance industry has focused on this issue ever since. Of course, triggers other than natural catastrophes such as fires could trigger this chain reaction of interdependencies within your Group.

"If you do not know your interdependencies, you cannot start your risk mitigation work."

If you do not know your interdependencies, you cannot start your risk mitigation work. We therefore recommend that you include this as a very important part of conducting Business Continuity Management (BCM) work. If has a competence centre working on business interruption, which has developed a quick guide on how to conduct BCM. Keep in mind, too, that your interdependencies will change continuously, which is why the map has to be rewritten on a regular basis.

Once you know what you face in terms of risks from interdependency losses, you can start to mitigate those risks. This can be done, for example, by getting alternative suppliers within the Group whenever that is suitable, having plans for external alternatives, improving the risk standard in critical processes, and so on. When that is done, there will most likely still be interdependency risks left, but you will have a grip on them and will know the approximate monetary effects that you would like to transfer to the insurer.

Business interruption

If is able to include interdependency effects in a business interruption solution for your company. The more we know about the interdependencies, the higher the limits are that we can provide. Having cover that is adapted to the actual risk will also affect the premium in a positive way. If you and If do not know what kinds of risks we mutually face, we will have to put a limit on this unknown parameter to cap it. We will be forced to suppose that the limit is always at stake if a very large claim occurs, which is why this unknown interdependency will have a negative impact both on the cover and on the premium.

To conclude, the more we know together about the interdependencies within your Group, and the more we can mitigate the risks, the better cover we can provide, and at an even more competitive premium.

Like to know more? Send the author an e-mail.

STAFFAN LJUNG
staffan.ljung@if.se

GETTY IMAGES

Flexible, high-quality international services

If's unique international network covers 170 countries globally, serving our clients on all the continents.

The wide and versatile network of 200 carefully chosen partners enables locally compliant service and readiness for If to go wherever the clients need us to. ll countries have their own, often widely different regulatory framework, as well as cultural issues affecting the business environment and operations. With an established partner network, If can offer specialised and in-depth knowledge and insight from each area and country, along with close connections everywhere we operate. Essential parts of the cooperation with our Network are mutual visits and knowledge-sharing activities.

If is a frontrunner compared to its Nordic competitors, both on the width of the network and on the different aspects of cooperation.

"We work differently in this field from our competitors. Instead of opening our own offices around the world, we have decided to seek the best expertise in each continent and country, so we are able to offer services more widely and in more detail", the head of International Services, Mia Himberg, says. "We know our partners, their operations and their expertise – and they again know their countries, the culture, regulations, and the insurance field. Through our partners, we have up-to-date business intelligence on 170 countries."

"No one has full knowledge or control of this field", Mia says. "It's kind of like surfing – you never know what kind of wave is coming, but you still have to make a decision to jump onto it and surf through it. When we are making the decision to jump in and create international insurance solutions for our clients, we want to know as much as possible about the wave – what's going on in each country we offer solutions in."

"With the intelligence we gain through our partner network, we have the ability to give true and versatile insight to our clients, and with that we have the ability and courage to surf the wave – which is so much better than staying on shore. We think this way of operating is the most efficient and productive - we develop and learn in both directions. In developing good and close relationships with our partners, they learn as much as possible and know what awaits our clients in different parts of the world", Mia concludes.

Knowledge-sharing to build commitment

If's operation with its partner network is a three-way relationship, beneficial both for If and the network partners, as well as for our clients.

Knowledge-sharing is one of the great benefits gained from this cooperation. Through its vast network of international partners, If gains not just the cultural and local knowledge crucial for successful insurance solutions, but also knowledge and insight into how the insurance market is developing and changing in each country of operation. Given that the width of our services covers 170 countries, deeper insights into specific countries through our partners is very valuable.

"There is a clear added value from meeting the local partners."

In addition to the day-to-day tight cooperation that If has with its partners, we also encourage our partners to visit If in the Nordic countries to increase our partners' understanding of If and our clients' operations, as well as to strengthen our relationship. These visits are made regularly by our different partners and often include corporate workshops to offer more opportunities for knowledge-sharing.

"The effort of these visits and workshops is very worthwhile to us, as by deepening the level of knowledge and the relationship, we can ensure an even smoother and higher quality operation", Mia Himberg says. "We want to learn from our partners and also willingly share our expertise with them. This is also a way to strengthen the commitment on both sides, which is a fundamental factor of the high-level services we offer to our clients", Mia continues. "Building strong commitment, we also support long-term relationships with our partners."

When visiting the If countries, whenever possible, the partners will also visit clients. If's client Wärtsilä and their corporate risk manager, Jan Virtavuori, have been involved in several partner meetings, and partners have visited Wärtsilä in Finland, as well.

"For us, there is a clear added value from meeting the local partners and having direct contact with them. We get immediate information if something changes in our country of operation. For example, if the insurance regulations in one of our African countries of business change, it is very valuable for us to know that as early as possible", Jan says.

Insights from Africa

If has clients, such as Wärtsilä, with vast operations in Africa, spreading across the different countries on the continent. Wärtsilä has been active in Africa for the past 40 years and has delivered power plants to 51 of the 54 countries. Part of the business is a continuing service agreement after the delivery, and in many countries, Wärtsilä remains to handle the operation of the power plant on behalf of the client.

"Africa is a market with a lot of potential for us, especially in the renewable energy sector. Almost all African countries have inadequate supplies of energy or electricity", Jan Virtavuori says, with Wärtsilä having just delivered the first solar power plant to Burkina Faso at a 17 M€ value.

Conducting business in Africa is not without challenges, with the cultures and way of business being quite different. Government and safety can sometimes also bring their own issues, and on the insurance side, there are different regulations. French-speaking Africa, for example, has its own CIMA insurance regulation, requiring that 50% for Property and Liability and 100% for Cargo risk is invested in the local insurance market (except in cases where we have negotiated specific set-up with an admitted local reinsurer).

"For us as a client, the first thing is to ensure that we can be insured in a certain country, and to know what kind of setup is needed when the different regulations are taken into consideration", Jan contemplates.

If's partner in Africa is Globus Network. Globus is the first Pan-African, multi-lingual Insurance Network with members in 47 countries, covering almost the entire continent.

A cooperation agreement with Globus gives us one point of contact to most of Africa. The partnership with Globus →

From left: Mia Himberg/If, Sahar Mohsen/Orient Takaful Insurance in Egypt, Jan Virtavuori/Wärtsilä, Margaret Selasi Esi Ashiagbor from Activa in Ghana, Pekka Sarpila/If.

IF

opens up access to local insurance companies, brokers and market knowledge and importantly, to firsthand information of changes in local legislation. Cooperation with Globus gives us access to their Reinsurance captive, Globus Re, an admitted reinsurer in the CIMA region, enabling us to offer to our clients an additional option in terms of retrocession.

If's African portfolio has grown significantly during the last few years, and the same growth is expected to continue. Despite the challenging market, the solution that If has built up with Globus in Africa enables us to implement global insurance programmes that are in full compliance with the local regulations. Especially in Africa, cooperation with a professional network partner is utterly crucial for our global insurance offering.

As part of our knowledge-sharing principle, one of the most recent visits was from Africa. Two Globus risk engineers visited If in Finland and Denmark, as well as several clients in both countries, one of them being Wärtsilä in Finland. Margaret Selasi Esi ASHIAGBOR from Activa in Ghana and Sahar MOHSEN from Orient Takaful Insurance Company in Egypt shared knowledge and topical info on their respective countries, as well as insight into the way of working. In several training sessions, If again shared our risk management knowledge and operations in detail, among other things, and the client visits gave valuable on-hands insight to the visitors.

"We go where our clients go."

"These visits are very fruitful for both parties. We at If learn about the local conditions and can share knowledge on risks and risk management with our partners. It is a strength for both us and our clients to have local contacts in Africa and all over the world. These people are the true experts of the business, legislation and culture in their countries and that is a competitive edge for both If and its large corporate clients", says Pekka Sarpila, Head of Risk Management Finland, who was hosting the visit.

"It was a very useful visit. I like it that we work as a team, all working together towards a common goal for our clients", Margaret says. "I gained a lot of useful information and especially valued the insight into If's risk management system and operation, as well as the underwriting policy. I gained a lot to apply at home and something that goes a long way, benefitting both us and If – and the client of course", Margaret concludes.

"I was very impressed by the client visits and I feel both sides now know better how the other party is thinking and working", Sahar says. "When visiting Wärtsilä and meeting Jan, it helped us understand the risk and insurance needs so much better."

"We learned a lot about a variety of topics and have a lot to share in our companies when we go back home. This visit will undoubtedly make our cooperation more concrete and even closer and easier than before", both Sahar and Margaret conclude.

Flexibility and fast reactions

"We have a long and steady experience from operating in Africa and with our partners there", the head of If International Network, Mia Himberg, says. We have been doing concrete cooperation on the frontline and with our active risk engineers on the other side of the world. We have seen from experience in other countries that this sort of cooperation has a direct meaning and benefit for our clients, and we are happy to have reached this high structure and level in Africa as well", Mia continues.

"We believe that through sharing each other's missions, strategies, and way of working, we will increase understanding of the respective countries' and markets' business cultures and market environments. This understanding can be decisive when we have a challenging and/or urgent request", Mia says.

"Our cooperation with If and Globus has gone really well", Jan Virtavuori adds. "We have been positively surprised how well the model that If has with its partner network functions, not creating any of the bottlenecks that we have often seen in the more traditional insurer's own local office model."

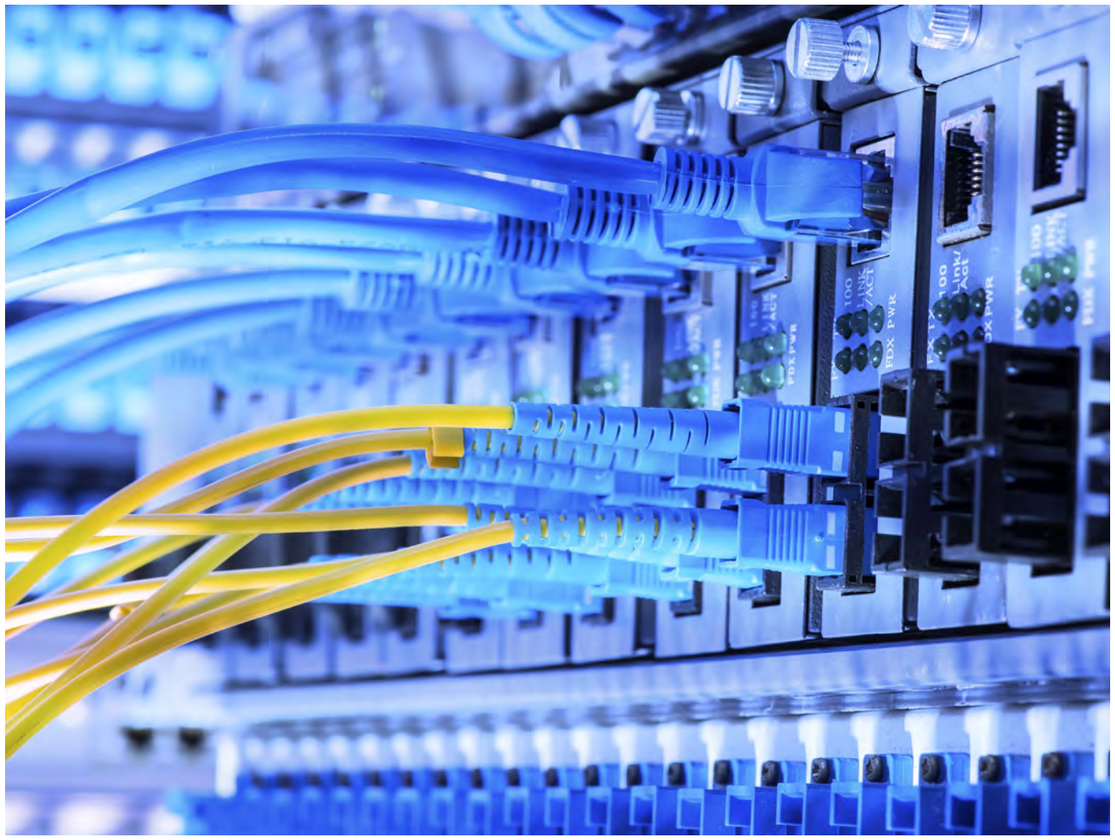
"We have also been very happy with the flexibility of the insurance solutions, as well as the response speed we have had from both If and Globus", Jan continues.

Regulation is increasing in Africa, and officials in all countries want to safeguard their own insurance markets. This means that insurance in Africa will definitely not get any easier.

With long experience, vast insight, and a well-established network of partners on the front-line in the changing market, If will seek to continue to provide the best possible insurance solutions to its clients in Africa.

"We go where our clients go", Mia says. "We have a large number of references from different countries, and we are proud that we never have to start from scratch. We have done this so many times that we know what to go for and where to look for the pitfalls", Mia ends. ■

IDA TUONONEN



ISTOCK

Don't touch this!

Physical security controls for IT and ICS

Examples of damage resulting from unauthorised physical access to data carriers and connected equipment reminds you of the physical security controls available to protect them.

If you can touch it, you can break it. Basically, that is what it is all about when considering physical security controls for IT and ICS systems. Protecting your IT and ICS systems against cyber-attacks using logical controls does not release you from the obligation to have physical controls in place as well.

Logical controls, such as two-factor authentication, firewalls, anti-malware, application whitelisting, vulnerability scanning, monitoring, and so on, leave your data and equipment vulnerable to the effects that physical access can generate. Being near your data carriers and equipment provides attackers with an opportunity to take, change, or destroy them. Like a cyber-attack, this may affect the confidentiality, integrity, and availability of your data and disrupt your business continuity.

According to Verizon's 2018 Data Breach Investigations Report (DBIR), about 11% of the breaches reported involved physical actions.

Examples of vulnerabilities

An example of a physical attack vector is theft of equipment containing data, such as laptops and mobile devices. If the screen lock is not activated, the attacker has immediate access to the data stored on the device and to the connected network. However, even with the screen lock activated, you will lose all the data on the device, and without a proper back-up in place you will never see it again.

Another well-known example of damage resulting from attackers having physical access to your equipment involves the installation of a key-logger between the keyboard and the computer. The key-logger collects the key-strokes comprising the username and password and sends them to the attackers. Using these credentials, the attackers can now log into the system and start finding their way around your systems. Furthermore, as the →

attackers receive all entries, they can also find out the sites you are visiting, the text you are writing, and so on.

Physical access often by-passes logic controls. If your data-at-rest is not encrypted, anyone accessing your servers can take a drive from the rack and read what is on it. The same goes for eavesdropping on your unencrypted data communications. Having access to your servers or routers would allow attackers to install listening devices.

If you believe this is far-fetched, you should take a peek into Verizon's DBIR or the annual report of your country's intelligence services, which rate industrial espionage as a top-tier risk year after year.

Physical access may also cause unwanted changes or damage to your (production) equipment's operating and safety systems. A contractor uploading an update to your machine without supervision from your staff could make a mistake, resulting in damage and business interruption.

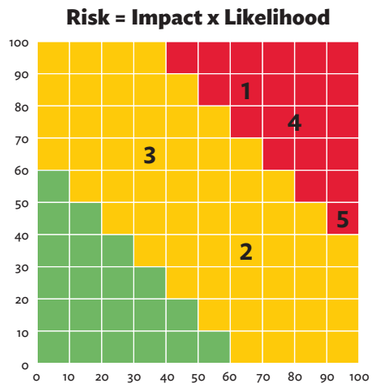
The above does not take into account disgruntled employees seeking revenge. Even though rare, they form a dangerous category of attackers, as causing havoc and mayhem is all they want, and setting a fire or destroying your property would fulfil their purpose just as well as launching a cyber-attack.

How to establish priorities

As we have seen, unauthorised physical access to data and equipment may jeopardise the confidentiality, integrity, and availability of your data. This is why we need to take a closer look at the security you need to have in place to reduce this risk. In 2016, the SANS[1)] Institute published a document named 'Physical Security and Why It Is Important'. We will introduce you to some of the strategies and tactics described in this document and provide you with references to European standards commonly used in the design of physical security controls and electronic alarms.

Without a security plan, no adequate security is possible. As in every risk management project, you will need to start with a risk assessment, taking into account the vulnerabilities of your staff, processes, data, and equipment. The next step will be to create a heat map by determining the potential impact on your business and the likelihood of its occurrence. When determining the impact, don't forget to take the potential period of business interruption into account.

1) www.sans.org SANS is a cooperative research and education organisation.



Risk scenarios could include:

1. Attackers having uncontrolled access to your industrial control systems.
2. Thieves taking a laptop containing personally identifiable information (PII).
3. Cleaning staff accidentally damaging the routers in a rack.
4. Thieves taking one or more hard drives from your data centre.
5. A contractor uploading a faulty update into your warehouse management system.

Each scenario is measured for impact (e.g. value of damage and time required for recovery) and likelihood (e.g. rate of occurrence in days), with the result plotted in a matrix. At a glance, you can now see that the risk of thieves taking one or more hard drives from your data centre (no. 4) is assessed as unlikely to happen but with a high impact.

As the subject of our plan is physical security for IT and ICS, the risks relate to locations. This enables you to translate the heat map into a site plan indicating vulnerable areas from an IT and ICS perspective.

In the site plan 1, we have marked the identified areas of risk, which could be classified as;

- **Red** Critical risk area
- **Yellow** Elevated risk area
- **Green** Normal risk area
- **Grey** Observation area

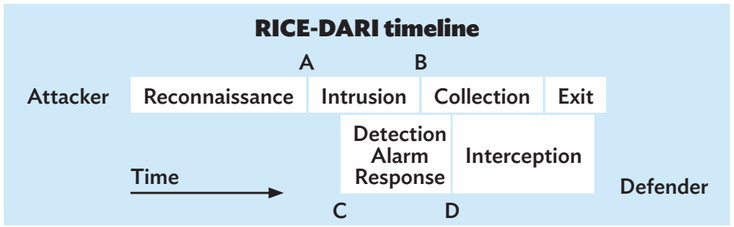
In this simplified example, we have identified the control cabinets for ICS, the server room for IT, and the server room for the WMS as critical risk areas. The offices have been identified as an elevated risk area because of the anticipated presence of devices containing important data. The warehouse and production areas are considered a normal risk as devices present in these areas are not considered to contain important data, and the area within the fence outdoors is considered the observation area.

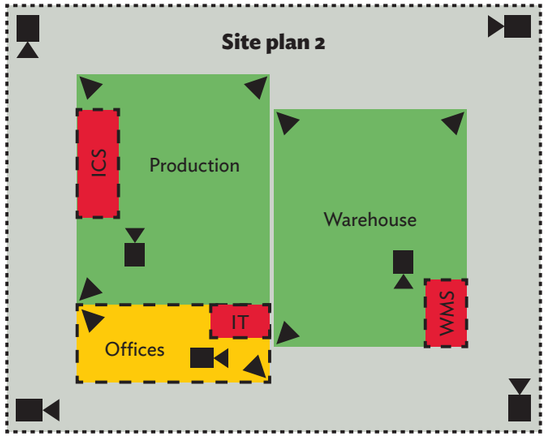
Designing physical security controls

To protect physical assets, the concept of choice is 'defence in depth'. This is a concept used to secure assets through multiple layers of security. If an attacker compromises one layer, they still have to penetrate the additional layers to obtain an asset. Adequate security can only be achieved by combining physical elements with technology in an administrative (response) framework.

Our RICE-DARI timeline is a visual aid. It shows the resistance time provided by structural security elements (e.g. wall, door, or window) counts only after the (attempted) intrusion is detected. This is because, if not detected, the attacker could remove the structural element altogether without triggering any response. When designing our 'defence in depth', the total resistance time provided by all elements between the entry point and the asset should be calculated and compared to the response time of the defenders.

In the RICE-DARI timeline below, it is shown that reconnaissance can be done by the attacker without triggering a response if no surveillance is present. The resistance time provided by the elements is represented by the distance AB. The attack is first detected at point C after a large part of the resistance time of the elements has been taken away. While detection and alarming take only seconds when using electronic sensors and signalling, the response will take much more time to organise. Before private security or police are on site, it may take as much as 15 minutes. This is represented by the distance CD.





Selecting physical security controls

Assuming that we want to prevent an attacker from entering the ICS cabinets or the IT and WMS server rooms, the values CD and AB are the ones we need to consider when deciding on the number and resistance time of the structural security elements.

In the site plan 2, we have now entered physical and technical security controls as follows:

- fences around the yard
- reinforced walls, doors, and windows around the offices
- reinforced walls, doors, and windows around the ICS, IT, and WMS
- cameras in the yard
- cameras near the ICS, IT, and WMS
- passive infra-red detectors inside the buildings

Taking the IT room as an example, the resistance time is now defined as the resistance time of the wall around the offices plus that of the wall around the IT room. The shortest line from outside the yard to inside the IT room appears to go through the yard, passing the wall (or door) around the offices, and passing the wall (or door) around the IT room. Assuming that the cameras in the yard have built-in video content analysis, the attacker will be discovered after crossing the fence. The resistance time will therefore be the total resistance time available for both walls surrounding the IT room. Without the outside cameras, this would be limited to just the wall surrounding the IT room, as the wall around the offices could be passed without being detected.

"The concept of choice for physical protection is 'defence in depth'."

European standards that can be used to select and describe physical security controls can, among others, be found in the series EN 1627 to EN 1630. Resistance classes relating to tool sets used by attackers provide the resistance time in minutes. For technical (electronic) controls such as sensors and signalling equipment, the EN 50131 and 50136 series provide advice along the same lines. Using these standards together requires a careful approach, as the definitions used in the standards do not always match.

Hidden 'defects' in the defence-in-depth model.

This article is only a summary of the considerations to be made and the tools available to physically secure your assets. It is possible to mix and match physical, technical, and administrative controls, but this should be done very carefully. One should especially take care not to include common vulnerabilities in the defences. Examples of such common vulnerabilities include using a single key for all doors, or having only a single transmission path for the signalling of alarms. Physical controls can, of course, be combined with logical controls. Again, however, one should take great care not to create single points of failure in the defences, such as using a default password or providing access to persons who do not have a direct need to access those systems. A major pitfall for all security systems is the 'manager dilemma'. Often, managers believe they should be able to access all rooms and systems by themselves. However, it is strongly recommended to apply the 'least privilege' and 'four eyes principle' for all employees, including managers. Do bear in mind that people with access to all and everything are the preferred targets for social engineering and/or coercion.

Summary

If you can touch it, you can break it. Access to IT and ICS assets can bypass the best logical controls, such as two-factor authentication and firewalls. According to Verizon's 2018 Data Breach Investigations Report (DBIR), about 11% of the breaches reported involved physical actions. Physical actions could include adding spyware to your systems or simply taking data carriers from your server rooms.

Designing physical security measures requires the application of a risk management process. The heat map from your risk assessment can be transferred to the site plan to indicate where physical protection is most needed.

The concept of choice for physical protection is 'defence in depth'. As the resistance time of the structural security elements is only valuable when detection and alarming are in place, you can use the RICE-DARI timeline to visualise the minimum requirements for your physical, technical, and administrative security elements.

In the specifications, you can use European standards to assist you in selecting the correct quality for your security elements. Of course, you can (and should) combine your physical security with logical security. ■

ERIK VAN DER HEIJDEN
erik.van.der.heijden@if.se

ISTOCK

Minimizing a company's legal exposure when entering the U.S. marketplace

When entering the U.S. market, foreign companies should be familiar with the U.S. legal system and more importantly, strategies to prevent unnecessary litigation.

"The first thing we do, let's kill all the lawyers." ~ William Shakespeare, Henry VI, Part 2

Well…not so fast!

In litigation loving America, economic globalization has naturally led to increased legal disputes against foreign companies doing business in the United States. When entering the U.S. market, foreign companies should be familiar with the U.S. legal system and more importantly, strategies to prevent unnecessary litigation.

Clients doing business in the U.S. should be advised that the most effective way to resolve disputes is to avoid them in the first place. This article will discuss potential causes of action and serve as a guide on how to minimize legal exposure and risk for product manufacturers and distributors doing business in the U.S. through quality control, meticulous drafting of warranties, contractual agreements, product manuals, warnings and insurance coverage.

The U.S. Legal System

The types of lawsuits that may be filed in a U.S. court are far reaching in both subject matter and dollar amount. Foreign companies doing business in the U.S. should be mindful that seemingly frivolous claims that challenge the most basic principles of common sense may withstand initial judicial scrutiny and immediate dismissal. As both winning and losing parties are usually responsible for their own legal fees and costs, all claims, regardless of legal merit, can become costly.

Going further, the far-reaching scope of discovery allows for virtually unfettered discretion to seek documents, identification of witnesses and other information from parties to a lawsuit. The obligation to comply with broad discovery requests is often costly, time-consuming and may require disclosure of documentation within the company's "possession custody and control." This legal requirement may directly conflict with the European Union's General Data Protection Regulation (GDPR), a data privacy regulation which went into effect in May 2018 and limits the transfer of personal data to countries outside the E.U. A foreign based company may face conflicting legal obligations if a subpoena for documents served in a U.S. lawsuit requires the company to produce documents that may constitute protected personal data under GDPR.

Product Liability Claims

Product liability claims may be made against the designer and manufacturer in addition to any distributor, importer or seller in the chain of distribution who may be liable for injuries resulting from a defective product. The three most common product liability claims involve defective design, manufacturing defects or failure to warn/improper labeling. A defective design claim focuses on the danger of a product based on the design as opposed to the manufacturing process whereas a claim alleging a manufacturing defect asserts the product was unsafe because it did not conform to its intended design. Failure to warn claims allege that a manufacturer failed to warn of an inherent danger in the product.

Quality Control

Before entering the U.S. market, a product manufacturer or distributor is advised to seek assistance to confirm compliance with federal regulations for certain products in addition to industry standards and the required product safety testing and certifications. In an effort to avoid legal action or provide a strong defense against claims or lawsuits, product manufacturers should ensure they have produced a safe product for which there is no safer alternative design. Manufacturers should also perform regular, documented visits to the facilities where the products and/or all component parts are made and develop a protocol for the inspection of all components and finished products.

The most effective way to resolve disputes is to avoid them in the first place.

Warranties

Warranties in the U.S. may be used as a shield against potential product liability claims. A carefully crafted express warranty is crucial for minimizing liability exposure for damages caused by an allegedly defective product. To be upheld in the U.S., warranty language must be clear and straightforward. Some warranty requirements regarding clarity and damage limitations vary by state.

An express warranty is a promise made about the quality and features of a product being sold (e.g. a watch is waterproof, or a washing machine will not fail during the first 3 years). An express warranty should clearly describe the manufacturer's product and the specific length of time the company guarantees the product will be free from defects. A manufacturer's express warranty should only offer to repair or replace a product after the company is given ample time to provide an analysis to confirm the product is in fact defective.

A warranty should also purport to limit damages resulting from any defect to repair or replacement of the defective product and further disclaim recovery for consequential or indirect damages. Be advised that damage limitations must often be conspicuous and appear in capital letters or a specific font size. Further, a damage limitation for personal injuries arising from consumer goods is considered unacceptable. Thus, foreign product manufacturers should consult with a U.S. attorney to ensure that warranty language associated with their products complies with federal and state law.

Contractual Agreements

Careful drafting and review of contractual agreements can further assist in limiting exposure to damage claims. A well-written contract between a foreign manufacturer and a U.S. based distributor will include a limitation consistent with those in the governing manufacturer's warranty. Any contractual indemnity provisions will further attempt to exculpate a product →

manufacturer from defects arising from an installation error or another manufacturer's product or component part. Alternatively, a foreign based distributor should insist on a contractual provision that indemnifies it from any damage claims arising from a defective product. Importantly, all insurance requirements set forth in a contract should be carefully reviewed by the company's insurance carrier and attorney.

Product Manuals and Warnings

A manual for products sold in the U.S. should carefully set forth a description of the product and any installation instructions. As failure to warn and failure to instruct are common, but different, tort claims in the U.S., a manufacturer must provide adequate instructions about a product's proper use and product warnings should detail risks that cannot be eliminated through reasonable design. Even if adequate instructions are provided, a product manufacturer must provide warnings that inform users about potential dangers related to the nature and use of the product. Be mindful that even the most obvious dangers to a pragmatic individual may not be considered "obvious" to a litigious American end user! Foreign product manufacturers should also refer to U.S. standards setting forth requirements for the content, location and appearance (e.g. font size, symbols) for specific product warnings.

Insurance

Importantly, foreign companies should also ensure that they have obtained adequate insurance to protect themselves in the event of a lawsuit in the U.S. As some European based policies exclude U.S. based claims and lawsuits, company representatives will want to evaluate their potential exposure and speak with their insurer or insurance broker to discuss adequate coverage.

In the US a commercial general liability policy will typically cover claims for negligence, personal injury, property damage, medical expenses, slander, libel and the cost to defend your company against these types of claims. Foreign manufacturers and distributors should be advised that a general liability policy may exclude claims involving the product itself. Alternatively, product liability insurance protects against loss resulting from a defective product that causes injury or bodily harm, but not the product itself. A company should ensure it has both general liability and products liability insurance cover with sufficient limits to cover general and product liability claims. In the Nordic market these covers are often sold under one GLPL insurance policy.


ISTOCK

Foreign manufacturers should also inquire about a vendor's endorsement, product recall coverage and directors and officers (D&O) insurance. A vendor's endorsement provides a manufacturer's vendor with an "additional insured" status on the manufacturer's policy and gives the vendor added confidence to sell and distribute a manufacturer's product without fear of having a claim affect their general liability coverage or premiums. It is further advisable for manufacturers to require that their distributors maintain a commercial general liability policy with adequate coverage to protect the manufacturer from the distributor's negligence. Product recall insurance provides coverage benefits for a recall which go beyond the scope of the standard commercial general liability policy. Lastly, directors & officers insurance provides valuable defense coverage for claims which are asserted directly against the directors and officers of the defendant company.

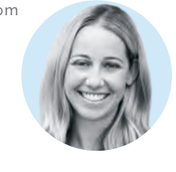
"Foreign companies should also ensure they have obtained adequate insurance."

Conclusion

Conducting business in the United States can be an exciting, yet sometimes daunting endeavor. However, taking in to consideration the points addressed in this article can facilitate success in the U.S. market. Fortunately, Shakespeare did not actually intend or desire to kill all the lawyers. Keeping this in mind, foreign companies entering and operating in the U.S. market are advised to consult with their insurer, or insurance broker and attorney experienced in U.S. risk mitigation to assist in killing the danger of unnecessary and costly litigation brought by adversarial American consumers. ■

GROTEFELD HOFFMANN,
Chicago, Illinois, USA

LINDSAY E. DANSDILL
ldansdill@ghlaw-llp.com




ISTOCK

Sustainability
in Claims and Loss Prevention

Sustainability is high on the agenda in Nordic companies, as many begin to 'walk the talk' and take action to support their environmental targets.

"People in the Nordic countries understand the risks caused by climate change. Still, we see a lot of claims that could have been avoided rather easily. When Copenhagen suffered from a cloudburst, a lot of vital equipment, such as IT systems, were destroyed, since these were kept in the basement,' says Anne Nielsen Sønderskov.

Anne Nielsen Sønderskov, is one of If's risk engineers, helping corporations in the Nordic area with loss prevention daily. She specialises in building materials and conducts analyses on building construction and materials, evaluating fire and smoke contamination hazards.

"We see new solutions and materials invented all the time, and one needs to be 'up to date' on all potential dangers connected to them. It is still common for corporations not to completely understand the risk, for example, that new insulation could lead to more damage in the case of a fire. These situations are possible to tackle, but you need to know about them," says Anne Nielsen Sønderskov.

Sustainable and resilient businesses can maintain their activities even when problems or accidents occur. This requires prevention and recovery planning, that deals with potential threats. By working together with our clients, If provides expert support through risk engineering to help limit damages, while enabling business continuity.

When a claim happens

If handled 596.000 cases of car damage and 432.000 cases of property damage during 2018. In almost every claim, lies the possibility to make more sustainable decisions.

"We take our sustainability responsibility seriously and require that the suppliers comply with strict environmental and health-related requirements", says Gunnar Ingelsrud, Head of Claims Purchasing, Nordic.

If's goal is to increase recycling and to reuse undamaged parts instead of disposing of them. By cooperating with leading suppliers covering the Nordic market, we enable stringent follow-up and efficient communications. This way, we minimise the negative environmental impact from repairs, while giving our customers the best possible support. A contractor with If needs to meet certain standards to be part of our supply chain.

'We appreciate that If challenges us when it comes to material use. We want to keep improving, and I also think the workshop has gained financially by working in a more environmentally friendly way,' says Dan Andersson, foreman at the Volkswagen workshop in Kista.

Digitalisation enables sustainable operations

With 450 building contractors and some 3000 vehicle repair suppliers working closely with If, it is important to deliver an efficient and streamlined process for property and vehicle damage claims handling, as well as ensure compliance with If's process requirements. When an accident is reported to If, a contractor conducts the first inspection using digital tools such as In4Mo, Meps, Cabas, and DBS (to mention just a few). Besides speeding up the handling time of a claim, digital tools minimise travel and paper consumption. Furthermore, through integrated reporting, we are able to measure how much waste has been sorted from damaged sites, for example.

Digitalisation enables improved processes and increases efficiency, while providing opportunities for more sustainable operations. This not only benefits our clients and If, but helps to mitigate the impact on the environment as well. ■

TERJE BRØNSTAD
terje.bronstad@if.no

GETTY IMAGES

New modern legal framework for conduct of reinsurance

If P&C has been actively involved in a global project to create a new private codification of reinsurance law. This set of rules of conduct for reinsurance effectively modernizes the old reinsurance law and enables uniform and transparent rules across the globe.

Reinsurance is a globally important financial services sector that enables insurance companies to provide efficient solutions to the largest and most complex risks.Reinsurance is sometimes utilized as a risk transfer mechanism in insurance solutions for corporate clients, especially with companies who have captive insurers but also when risk sharing within a panel of insurers includes reinsurance elements.

For nearly three years, work has been ongoing to create a single set of rules and principles for the conduct of the reinsurance business – the principles of reinsurance contract law project (PRICL). The idea of PRICL is to create a modern codification of reinsurance law, which would both provide a uniform frame of reference on a global basis and modernise the old (and often very harsh) rules regulating the conduct of the reinsurance business.

The principles of reinsurance law project is led by universities in Zurich, Frankfurt and Vienna, with the responsibility for the eventual published principles resting on the drafting committee. To ensure sufficient feedback from the market, participants' advisory panels from reinsurance company representatives and direct insurance company representatives were also established.

Sharing experience

The project has participants from all major legal traditions around the world, with representation from the large European countries, but also from the US, China, Japan, South Africa, and Latin America, facilitating the creation of a truly global, uniformly applicable model principles. Reflecting the high quality of work and ambition within the PRICL project, UNIDROIT, the International Institute for the Unification of Private Law, adopted PRICL within its work programme for 2017–2019.

Many of the major reinsurance companies, such as Munich Re, Swiss Re, Hannover Re, and Lloyd's, are involved in the project. If P&C, together with companies like Zurich, Axa XL, AIG, and Generali, is representing the view of the direct insurers in the project.

"During the long history of If (and its predecessor companies), we have seen the benefits of efficient and secure reinsurance solutions, which help to provide competitive insurance solutions to many clients with diverse risks and needs. At the same time, we have seen the problems that can arise when the scope and function of reinsurance cover are compromised or misunderstood. Even through just the increased clarity of duties that it will bring, PRICL holds enormous promise", Lari Kuitunen, reinsurance manager at If says.

"We feel it is important to be part of the PRICL project, as we are contributing to building a clearer and more secure risk transfer framework for the global insurance and reinsurance industry. If has put a lot of effort into giving our input and sharing our expertise to ensure that the new private codification of reinsurance law will have the best possible chance to succeed in the market", Lari continues.

The co-ordinator of the project, Professor Helmut Heiss of the University of Zurich, appreciates the contribution of practitioners in general and of If in particular: "Drafting rules of reinsurance contract law requires in-depth information on current practices in the market. The PRICL project provides a unique framework for a joint venture of academics and leading players in the market in developing a systematic body of rules. The engagement of If and its reinsurance manager, Lari Kuitunen, was of the utmost importance to the successful outcome of the project. He acted as the voice of direct insurers in the project."

Three years of work

The PRICL framework is scheduled to be published soon, and it will become publicly available and ready to be adopted by the industry. PRICL represents a modern codification of the current reinsurance practice, with improvements in key areas where disputes have often arisen (such as aggregation of losses).

LARI KUITUNEN,
Reinsurance manager, If

Notably, for failure of duty as a reinsured party, PRICL adopts proportional remedies with quite a similar ruleset to that found in the UK insurance act of 2015. This means easy access to a fairer and less severe punishment for failure to completely fulfil the disclosure duty of the reinsured, or for other unintentional contractual breaches. This can be achieved without having to choose UK law to govern the contract, which may bring undesirable complications and cost.

Current reinsurance practice in this respect is lot harsher: for material non-disclosure or misrepresentation, the reinsurance contract can be deemed completely void. Under PRICL, the penalty more closely fits the crime, and complete loss of coverage would be expected only in exceptional cases.

Further "the new law includes not only the rules, but also commentary on interpretation and usage, providing far better clarity of duties and obligations of the parties to a reinsurance contract, allowing for ease of use and an almost textbook-like manual for conducting reinsurance, without having to collect years of reinsurance market expertise", Lari says.

PRICL can be easily adopted in a reinsurance contract through the choice of a legal clause or incorporation, and partial adoption is also possible with fully flexible contract design, selecting only individual articles of PRICL. These features should be especially interesting to entities who do not practise reinsurance on a large scale on a day-to-day basis, and they will be an especially useful contractual framework for captive insurers and major corporations that choose to structure part of their insurance protection in such a way that it contains reinsurance elements. ■

IDA TUONONEN


ISTOCK

Track your claims

A large company can have many hundreds of claims a year.

Until now, it has been a challenge to keep track of the claims process, including important process steps such as: what loss was reported and when, what was said to the claims handler, how far has the insurer got in processing a specific claim, and so on.

If has been analysing the registration process from the client's point of view. The outcome is a new way of using the client portal If Login to let the client control the entire process for all their company's claims.

The claim registration starts with easy-to-fill forms in which all known data about the client and the policy is prefilled. "Draft" and "share" functions let the user co-work with colleagues, if many people's input is needed to describe the claim correctly.

A registration can also be made very easily from a smartphone, with which the user can take pictures directly with the camera and attach them to the registration.

Once posted to the claims handler, all activities can be followed in real time via an activity log.

So far so good, but the unique thing is the communication part, in which a dialogue can take place between the client and the claims handler. Files such as policy reports, PDFs, or pictures can be sent back and forth, all tracked in the activity log. Several persons at the client company can participate in the dialogue if necessary, and they can also receive notifications by email when something changes in the process or when more info is needed. A daily summary mail on all claims activity is also sent, so no one involved will miss any detail.

"This is excellent and just what we need. We used to send emails to the claims handlers, but we never really knew what was happening and if someone really was working on our claim. This solution solves that issue", says one large client with subsidiaries in several European countries.

Once the claim is closed, communication and activities remain accessible, so follow-up is easy, if needed. All in a safe, secure, and compliant way. ■

KRISTOFER PALM
kristofer.palm@if.se


ISTOCK

What happens to product liability in the age of digitalisation?

Have liability regimes ever remained stable? Absolutely not. The legal rules about the responsibility to pay damages to a person who has suffered an injury or property damage are constantly evolving in one way or another.

Product Liability Directive 85/374/EEC, the cornerstone defining liability for damage and injuries caused by defective products in Europe, is over 30 years old. It created a common basis for all member states and adopted the concept of strict liability and the claimant's direct right to claim damages from the producer. Products are tangible objects but not, for example, data or software. The directive has been a success story, making the Single Market operate in quite a uniform manner and simultaneously promoting fair competition.

During the decades since the directive, the EU Commission has published several reports on the functioning of the directive and legislation based on it in the member states. These reports have not brought up problems calling for amendments. The set-up has endured enormous changes in production and new products. However, things may change soon. Two years ago, the EC launched a public consultation on the directive, particularly on the following themes:

- **whether and to what extent the directive meets its objectives of guaranteeing, at EU level, the liability, without fault, of the producer for damage caused by a defective product**
- **whether it still corresponds to stakeholders' needs**
- **whether the directive is fit for purpose where new technological developments, such as the Internet of Things and autonomous systems, are concerned**

The replies have been published. The opinions varied, for example, between consumers and industries, but the survey revealed plenty of interesting areas needing further analysis.

Last year, the EC continued by setting up an Expert Group on Liability and New Technologies. The group consists of members from academia, law firms, stakeholders such as industry and consumers, and authorities and public entities.

The work has progressed with drafts of the documents, and some results should be ready next summer. The aim is to study even the most fundamental concepts like "product" and "producer" or "defect" and "damage". One deliverable will be a non-binding guidance for courts and practitioners on product liability, which is intended to lead to more uniform outcomes in liability.

The work will also study the role of new technologies such as software, IoT, AI, 3D printing, and service platforms. Who should, in the end, be liable for injuries and damage? It must be relatively simple to find out who is liable. Otherwise, handling and legal costs may blow up.

We in the liability insurance business, as well as our clients in the manufacturing or service industries, are keenly following the work. Can product liability be developed in an orderly fashion to represent better the influence of different factors and operators that lead to damage or injury? ■

MATTI SJÖGREN
matti.sjogren@if.fi

HANNU HIRVONEN
Head of Property UW, FIN

PASI PURSIAINEN
Account Executive, FIN

KRISTOFER GIMLEGÅRD
Risk Engineer, SWE

SARA MOBERG
Risk Engineer, SWE

KRISTIAN EHLERN
Account Executive, DEN

MIRAN MARUSIC
Marine UW, SWE

"Technology is changing the way we work."