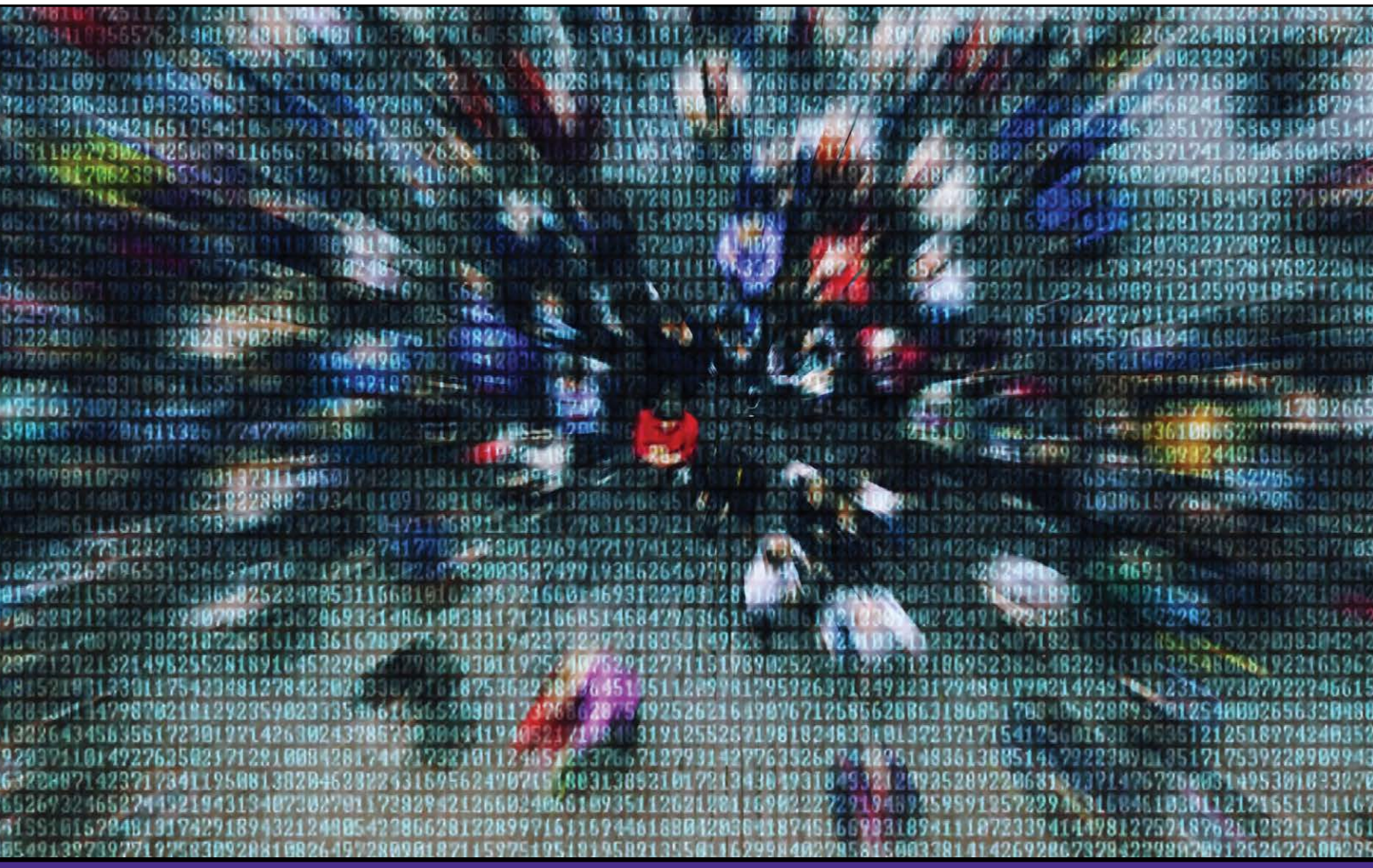
Sponsored by

FM Global

CIR

CONTINUITY INSURANCE & RISK



A world of complexity *Although navigating this complex world might be a challenge, the benefits for organisations that can build resilience by working closely with the risk management function could be significant and provide a major competitive advantage in the years to come. Adriano Lanzilotto explains Page 24*

Security in a complex world *The explosion of connected devices and mass digitalisation programmes creates multiple entry points for criminals and increasingly their targets are as much about physical property as intellectual. Tiago Dias explains Page 26*

Business Resilience Focus

FM Global

Sponsored by

A world of complexity

Although navigating this complex world might be a challenge, the benefits for organisations that can build resilience by working closely with the risk management function could be significant and provide a major competitive advantage in the years to come. Adriano Lanzilotto explains

It's already a year that we'll never ever forget, as the pandemic, social movements and political risk have changed our lives, society and the economy, disrupting organisations everywhere. Much of this disruption has been a direct result of risks that had not previously rated highly on many risk managers' lists of concerns. Coupled with more traditional hazards, which have not gone away, organisations are facing some serious challenges.

On the upside, business leaders everywhere are now giving much more attention to their companies' exposure to risk. This provides a real opportunity for the risk management function to come to the fore and build long-lasting beneficial relationships with the C-suite.

One of the first conversations that must take place at a high level relates to economic conditions.

The pandemic has shown how quickly economic conditions can change along with market demand for products and services. Demand for certain products – sanitiser, PPE and bicycles – skyrocketed during the pandemic whilst demand for other goods such as cars, clothing and airplanes waned. With potential second waves of the pandemic on the way and increased political and trade tensions, organisations must be more prepared for economies and markets to quickly stop and start.

The push to respond to a sudden increase in demand may tempt some companies to push their machines harder, with less downtime for maintenance, to maximise production. While completely understandable given the situation and the desire to capitalise on heightened demand, a lack of maintenance for machinery or overuse could pose a significant risk of a disastrous failure, and potentially even a major fire.

Given equipment in many manufacturing facilities can be difficult, expensive, and slow to replace, it's clear that a focus on protecting machinery is another item that organisations and risk managers need to consider in today's changing risk landscape.

Similarly, the economic fallout from COVID-19 could create further issues for equipment as well as a company's facilities. We don't yet know how deep or long lasting the economic impact of COVID-19 will be, but with the possibility of a global recession looming, many businesses around the world will potentially be forced to take decisions that could create or magnify risks.

One of the challenges that an organisation will face in this situation will be deciding where to allocate capital, in the face of budgetary restraints. These restraints could create a clear issue that risk management professionals need to be aware of; that essential maintenance or risk improvement investments might be discarded or delayed to save money. However, moves to delay maintenance of machinery or equipment are likely to store up problems for the long-term, with a failure of machinery likely to cause significantly more damage than a loss of production time for maintenance ever could.

Additionally, many organisations have been idling facilities, stopping production either as restrictions on movement were applied or as demand for their products plummeted. Idle facilities can be more at-risk from various hazards, such as extreme weather events, fires, or even criminal damage such as arson, as employees who would usually be on-site are unable to respond and manage any of these risks.

Keeping appropriate maintenance schedules for key equipment, and ensuring that an appropriate pool of skilled employees are available to respond to any hazards that might affect an idle facility, should therefore be a priority for risk managers, and something they need to try to keep top of the decision makers' agenda in the coming months.

Climate change and natural hazards

Although COVID-19 has understandably captured the attention of so many businesses, it's vital that lessons learned in recent years, concerning different, traditional risks are not forgotten. Hazards such as hurricanes, storms, flooding and wildfires can all cause significant damage, and disrupt operations. Think back to major hurricanes of recent years such as Harvey, Irma, and Maria in 2017 which caused total economic damage of US$337 billion. Or alternatively, look at the damage that wildfires have caused

in California in recent weeks – it's clear that natural hazard exposures should still feature prominently in an organisation's understanding of their risk landscape.

All these risks are likely to be exacerbated by climate change. A warming world and an unpredictable climate is already causing significant disruption, with some of the most visible instances being natural hazards. While it's not always possible to definitively say whether an individual event has been caused directly by climate change, the science is clear; a warming world will result in natural hazards becoming more frequent and extreme. The challenge for risk managers will be in ensuring that their organisation builds resilience. This could consist of physical protections at facilities, a greater focus on business continuity plans, and potentially a revaluation and possible relocation of facilities which are deemed to be particularly at-risk from natural hazards. Tools such as the FM Global Resilience Index or the Natural Hazard Maps can be useful when evaluating facilities for their natural hazard exposures.

Cyber risk

Although the immediate, short-term, effects of COVID-19 – social distancing restrictions, lack of face-to-face contact – may all create challenges, in many ways it is the longer term effects and changes to how businesses operate that pose the most serious threats. Many of these changes, such as a significant shift to working from home practices, have not come out of the blue. In many cases they were expected to take place within the 2020s as technology advanced and made them possible, but the concentration of these changes in the first six months of the decade creates vulnerabilities.

As working from home has demonstrated to many businesses the benefits of virtual, online communication, it has simultaneously heightened the cyber risk faced by organisations as employees in some cases move away from a company's cyber security protections. This of course is also exacerbated by trends we've seen across industries in recent years – digitalisation and the rise of automation systems, which have also contributed to an increase in cyber exposures.

"We don't yet know how deep or long lasting the economic impacts of COVID-19 will be, but with the possibility of a global recession looming, many businesses will potentially be impacted – forced to take decisions that could create or magnify risks"

All of these trends and changes are constantly altering cyber exposures, muddying the waters for risk managers and business leaders. Fortunately, this is an area where insurers or cyber specialists could help. At FM Global, our clients can conduct unique cyber risk assessments to help understand their cyber exposures by assessing three critical areas – physical security, information security, and industrial control systems. By building a clear picture of a client's exposure appropriate risk mitigation can follow, and allow a business to reduce their exposure to this complex and ever-changing component of the risk landscape.

Supply chain risk

Finally, one more area that is threatening major changes within the broader risk landscape is supply chains. Even before COVID-19, political decisions and trade wars were threatening a backlash on globalisation. The pandemic has of course magnified these trends, with lockdowns, restrictions on movement, and in some cases government embargoes, disrupting the flow of goods.

For organisations, all this disruption – both threatened and real – should highlight the importance of building resilience into their supply chains. Auditing suppliers to gain insight into the risks they face across their locations can be an incredibly useful first step and can immediately highlight some urgent issues. But by identifying back-up suppliers (ideally in separate locations with a different risk profile) which can step in if a first-choice supplier fails to provide, organisations can build resilience. This diversification and auditing of suppliers is one of the most fundamental steps to building supply chain resilience, and ideally this takes place across multiple layers of the supply chains (to suppliers' suppliers for instance) rather than just the first tier of the chain.

Although today's risk landscape is consistently changing, the key principles of risk management are just as valid as they have always been. Making decisions based on proven science and data, investing in protection appropriate to the business or facility, and taking care and maintaining equipment are all vital for building resilience – a trait which will help protect a business from disruption and loss during these difficult times.

Adriano Lanzilotto is vice-president, client service manager, London Operations at FM Global

Security in a complex world

The explosion of connected devices and mass digitalisation programmes creates multiple entry points for criminals and increasingly their targets are as much about physical property as intellectual. Tiago Dias explains

In the last week of August 2020, the New Zealand stock exchange was taken offline by a series of cyber attacks, causing tremendous disruption for four days of trading. The attackers looked to crash the New Zealand stock exchange's digital system by overwhelming it with a flood of internet traffic, from users located offshore. The motives of the attackers are still shrouded in mystery. Why New Zealand? Why then? The incident serves to highlight how modern cyber attacks are never as simple as we might hope.

Not only have the motives behind cyber attacks become more opaque, but so have the targets and ways-in. Traditionally, attacks targeted an organisation's main operating system, with the aim of extracting data or financial information. Now, with the explosion of connected devices and digitalisation there are multiple entry points for criminals and increasingly their targets are as much about physical property as intellectual.

When you look at a modern commercial facility it may have multiple networks and routers. For example, networks for machinery and equipment, air conditioning or a security system. These industrial control systems all act as potential entry routes for a cyber criminal. As well as increasing the possibility for damage from a cyber attack, these systems can offer a back-door for criminals.

The risks created by ICS are heightened by the fact that many of these systems are legacy systems, designed primarily to enhance efficiency and rarely with resilience in mind. Many ICS may be functioning on older operating systems, constructed without a key focus on how connectivity creates risk and a security weak spot. For example, a remote connection to an air conditioning unit may look innocuous, but it has the potential to give a criminal a route into a business' main IT systems.

Adding a global pandemic to the mix has further complicated the situation. One of the most obvious changes caused by the COVID-19 pandemic, which has significant ramifications for cyber risk, has been the exponential growth of remote working. This phenomenon will likely be with us long after the pandemic is over.

While this is great news for those looking to achieve a healthier work-life balance, it's not such great news for those responsible for cyber resilience, as the move creates and exacerbates certain threats. Many businesses are arguably more exposed than ever before, as they need to manage a digital workforce now working away from on-site security systems. Cyber risk professionals must understand how remote working affects their exposure to cyber risk and build resilience to it.

Risk professionals must be aware of how there is now far less

standardisation amongst the computer systems and wifi networks employees are using to accomplish their roles. This change makes it more difficult for information security teams and risk managers to assess exposure and adopt mitigation strategies, since an organisation's digital footprint is now much larger than before.

Another issue, created by home working, is the fact that many internal systems and VPNs may become swamped by users connecting from external sources. This strain on existing digital infrastructure can trigger considerable weaknesses for an organisation, whilst also impacting productivity. Systems that were designed to be accessed by a limited amount of people now, and going forward, will need to be accessed by a lot more users. In this instance, not only does the bandwidth need to be bigger but security tools, like firewalls, need to be properly reviewed to see if they are fit for purpose. There may also be integration issues caused by employees using a wide variety of different devices and technologies.

Cyber risk professionals must also be aware of how criminal targets are changing. Cyber attacks are no longer just about data, as we know. Criminals are now using cyber attacks to cause damage in the physical world, to machinery and facilities.

For instance, in 2014 hackers unleashed havoc at a German steel mill with a targeted attack on an ICS, which caused part of the mill's system to be completely shut down. You may be wondering how these hackers gained access – phishing emails. One of the simplest methods of cyber attack brought down a highly sophisticated facility, bringing disruption and millions of dollars of damage to the mill's blast furnace. Examples like this are numerous, and risk professionals need to learn from past cases, drawing out key lessons to drive resilience.

For those organisations looking to build resilience, one simple step would be to initiate more security checks within IT systems. Businesses could follow a defence-in-depth approach, adding extra layers of security, with multiple defensive mechanisms put in place to thwart potential attacks and increase the security of the whole system. Digital checkpoints can be used to authorise the right people and prevent cyber criminals from accessing sensitive systems. This can be achieved with, for example, corporate laptops using specific controls like endpoint protection or multi-factor authentication not only for remote VPN enabled access. Each method adds a defensive layer to make sure the people with appropriate access can connect securely but also for privilege escalation, internet, and mobile applications and more so for business partners connecting remotely. When everyone was working internally this was simpler to control, but the model changes when people are connected from the outside world.

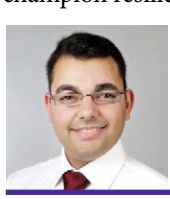
"We most likely haven't seen the full impact that a cyber attack can inflict"

Another method which promotes resilience specifically for issues linked to ICS, would be the FM Global Industrial Control Systems enhancement to our award-winning Cyber Risk Assessment Tool. This allows organisations to understand the best ways to drive continuity regarding their ICS, by identifying risks and providing practical recommendations to address those risks.

The ICS evaluation utilises proven loss prevention concepts to understand loss control management programmes, allowing clients to properly safeguard the vulnerabilities associated with their ICS. This is vital, as comprehending the risk a company is exposed to is often the first step to neutralising the dangers linked to its specific operations.

An additional area that organisations will need to consider when it comes to cyber resilience is the importance of having an up-to-date crisis response plan. The pandemic has highlighted how unpredictable events, seemingly separate from cyber security, need to be properly accounted for going forward. As a baseline, organisations need to understand their exposure to cyber risk and which areas may need more attention. For example, does the organisation have the right policies and procedures in place? Is the crisis plan regularly updated to account for any new potential scenarios? These questions need to be answered with an understanding of the business' critical processes, and how to properly protect them.

Even with all these sophisticated solutions modern cyber security is incredibly complex and will become more so. We most likely haven't seen the full impact that a cyber attack can inflict. It falls on risk professionals to keep ahead of cyber criminals, regularly reviewing entry points, mitigating risks, and identifying vulnerabilities. Clearly this is no small task, but it is one that risk professionals must adapt to, being ready to adopt the most up-to-date and innovative solutions to champion resilience.



Tiago Dias is cyber security consultant at FM Global

RESILIENCE MEANS NOT WORRYING ABOUT "WHAT NOW?" AND INSTEAD, FOCUSING ON "WHAT'S NEXT?"

The choice to be resilient has never been more important for a business to make. Today, resilience means choosing a different approach to insuring your commercial property. Above all, it's choosing to navigate the business, personal and risk complexities you face to ensure you move your business forward. Which is why at FM Global, we believe Resilience is a Choice.

RESILIENCE IS A CHOICE.

FM Global®