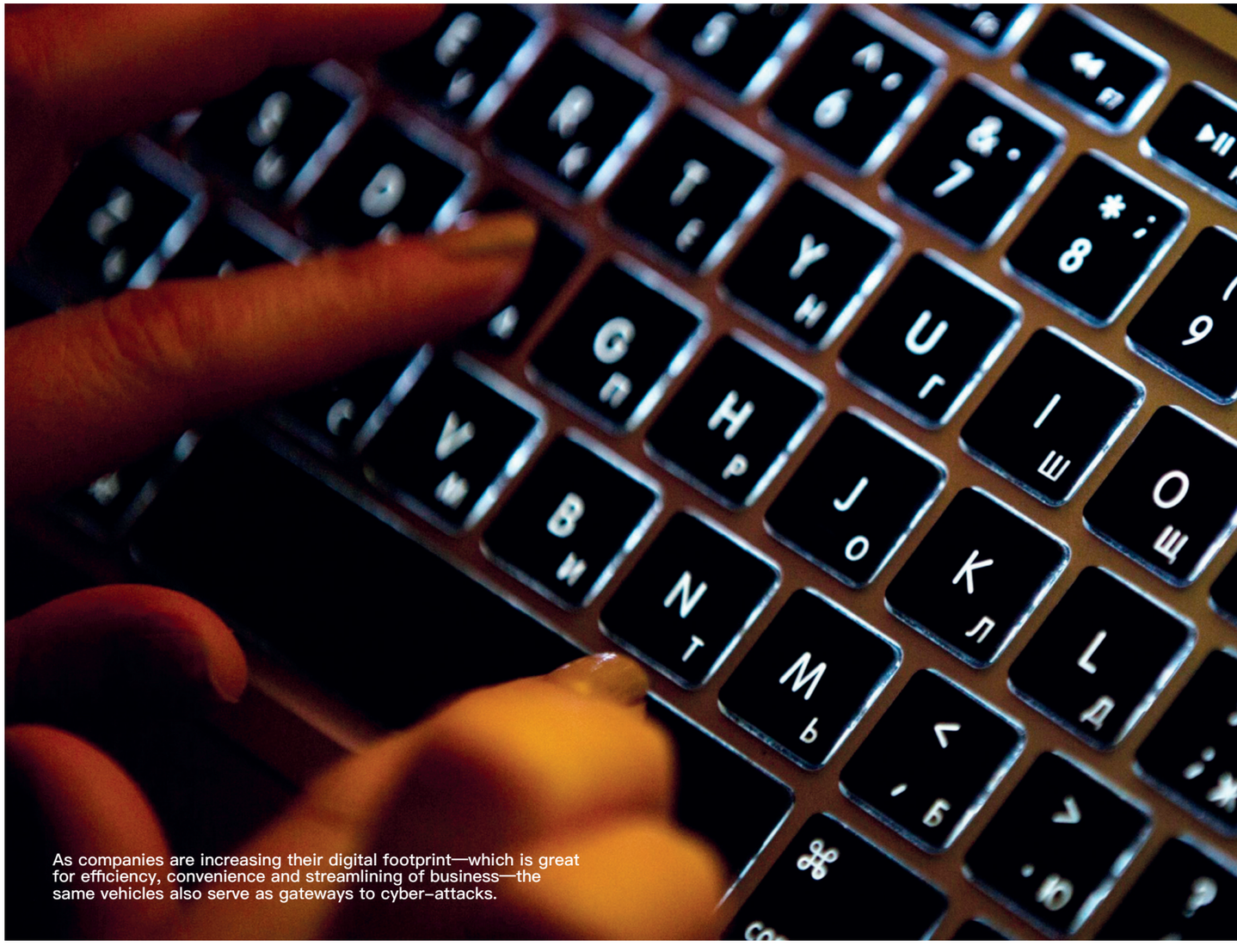
Mitigating the risks of innovation

Tracie Grella, the **Global Cyber Practice Leader** at **AIG**, highlights the importance of cyber insurance as well as the guidelines on how companies can mitigate cyber risks



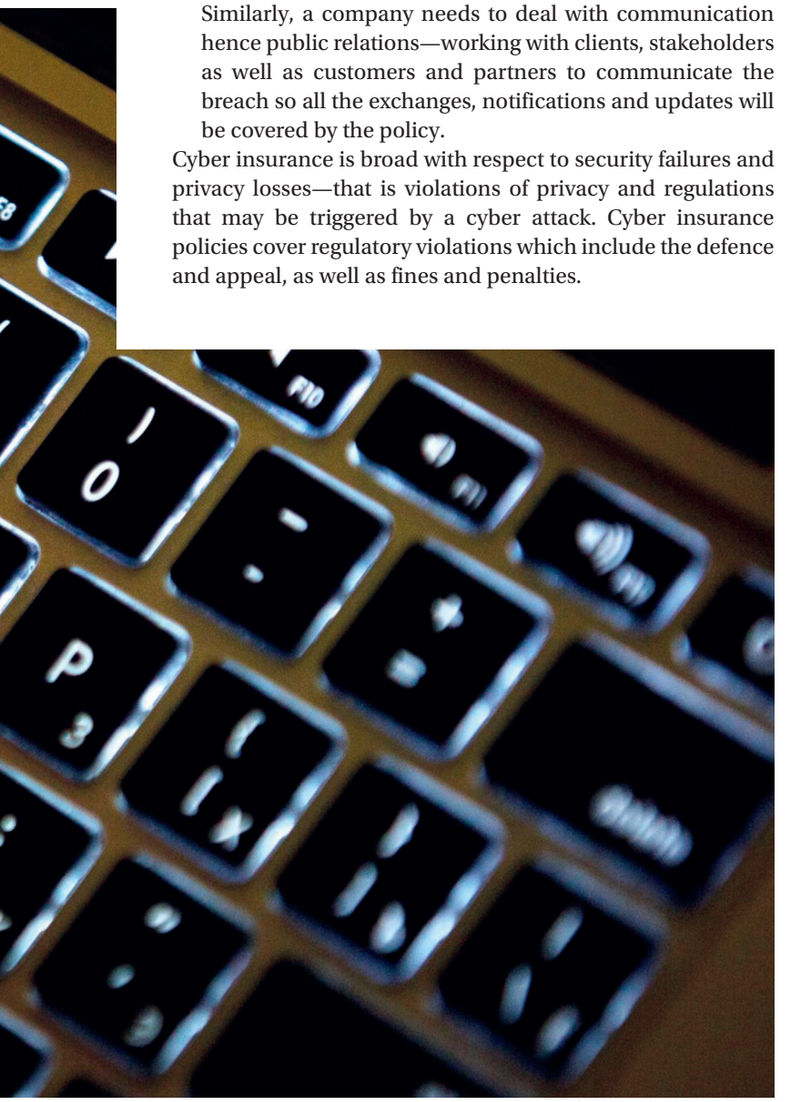
As companies are increasing their digital footprint—which is great for efficiency, convenience and streamlining of business—the same vehicles also serve as gateways to cyber-attacks.

Tell us more about cyber insurance. How does it work and how important is it?

Cyber insurance policy is designed to help an organisation mitigate risk exposure by offsetting costs involved with recovery after breaches and it has been around for 20 years but in different markets as well as times. There are four main coverages in cyber insurance:

- Security privacy and liability cover which insures against disclosure of data either through a cyber event or a privacy event. This coverage responds when confidential data is disclosed.
- Cyber insurance insures business interruption related losses—if a cyber event disrupts a business network, the loss of income and extra expenses as a result of network interruption will be addressed by the policy.
- Cyber insurance insures against cyber extortion, which pays the extortion payment where allowed by law. The decision to pay is made by the insured. Cyber extortion often results in business interruption as a result of the systems being down or data not being accessible, and the policy will respond to that as well.
- Additionally, cyber insurance insures crisis management expenses and data restoration. Cyber events involve many tasks which needs to be executed promptly, forensic experts need to investigate what happened as well as stop or mitigate the extent of the attack, get the intruders out of the network and make sure all the data is clean and restored. Similarly, a company needs to deal with communication hence public relations—working with clients, stakeholders as well as customers and partners to communicate the breach so all the exchanges, notifications and updates will be covered by the policy.

Cyber insurance is broad with respect to security failures and privacy losses—that is violations of privacy and regulations that may be triggered by a cyber attack. Cyber insurance policies cover regulatory violations which include the defence and appeal, as well as fines and penalties.



Similarly, cyber insurance insures against system failures and dependent business interruption. If systems are taken offline due to a programming or system upgrade resulting in loss of business income—the policy will address such unforeseen occurrences.

How does cyber insurance cover companies against data breaches?

The cyber insurance policy usually covers non-physical losses where a company is attacked and it results in the loss of corporate or personal confidential information. So, issues of companies losing confidential information that you see in the news will be addressed under the security and privacy section of cyber insurance. For data breaches, the event management coverage section is normally triggered first followed by the security and privacy liability coverage section.

What are the typical cyber risks for banks? And what are the less common ones that banks tend to overlook?

Banks have been dealing with the regulatory environment for a long time, so they are leading when it comes to prioritising cyber controls. Among industries, banks are more sophisticated in protecting against cyber attacks and have invested more money as well as talent to protect their networks.

However, banks are not immune to cyber events. Lenders are attacked on a daily basis with a number of incidents they are able to block but some cyber events are successful. By being a data-intensive industry and being on the lookout against disclosure of confidential information, banks are concerned about the loss of data.

A large-scale loss for banks may result in business interruption, resulting in loss of revenue as well as potentially damaging the bank's reputation and confidence from customers.

As companies are increasing their digital footprint—which is great for efficiency, convenience and streamlining of businesses—the same vehicles also serve as gateways to cyber attacks. Whether launched by run-of-the-mill hackers, criminals, insiders or even nation-states, cyber attacks are likely to occur and can cause moderate to severe losses for organisations large and small.

However, banks are prioritising security as they are embarking on digital transformation and planning about security should be a key component of that initiative. There are situations where companies in other industries are developing services and products without prioritising security. It is a good practise that when companies are developing new technologies, they also develop new security protections—this is a critical component of digital transformation within the banking sector.

What kind of trends do you see in the cyber insurance space in the EMEA region?

The cyber insurance policy covers non-physical disclosure were a company releases confidential data, as well as incidents, were businesses go offline but there is no physical damage to the network.

Financial institutions remain exposed to impactful cyber events, however, companies that rely on operational technology and industrial control systems have additional significant exposure to physical cyber events, for instance, where a valve can be adjusted resulting in a gas pipeline explosion.

Companies need to look beyond traditional kinds of cyber policies and consider the cyber risks the entire organisation is exposed to as well as how cyber events can be resolved in these kinds of physical losses. Insurance programs can be customized depending on your current business security posture and overall insurance program structure. ▸▸


Tracie Grella

"CYBER INSURANCE CAN BE A GREAT WAY TO MITIGATE THE DAMAGE CAUSED BY A BREACH, BUT IT SHOULD COMPLEMENT CYBERSECURITY TECHNOLOGY AS PART OF AN OVERALL CYBER RISK MANAGEMENT PLAN."

— Tracie Grella, the Global Head of Cyber Risk Insurance

Additionally, banks have been concerned about their exposure to potentially having cyber event triggred loss resulting in a physical exposure. It can cause a fire or explosion at a data center—causing physical loss and potentially taking the company offline thereby losing revenue.

Cyber insurance insures a broad range of cyber risk losses that may unexpectedly arise from cyber events and some policies can offer coverage for physical damage to hardware or coverage for business income loss.

The Middle East is the supplier of around 70 per cent of the world's oil and gas, and given this region's importance to the world, cyber events are a big threat which needs to be well addressed and managed for both nonphysical and physical losses.

How can companies manage data breaches and Distributed Denial of Service (DDoS)?

There are basic hygiene guidelines that are best practises on how companies can manage cyber risks. Developing a cybersecurity programme is a journey for organisations and they need to set targets. Cybersecurity management is limited by the company's resources as well as the available capital to invest in improving the cyber risk posture. Organisations need to decided where to a invest in order to get the best returns on reducing their risks.

Most financial instituation are implementing basic hygiene and the minimum standard includes two-step authentication, training employees as well as creating cybersecurity awareness within the organisation from top-down and avoiding using unsupported software.

Some of these precautionary measures might seem ordinary but they prevent around 98 per cent of data breaches. It is important that the cybersecurity controls a company invests in are implemented across the entire organisation.

A network does not have borders—it is important that companies invest across their entire network system because once the adversary attack part of the network they can move throughout the network system which may paralyse the organisation resulting in loss of income.

Do you find companies and individuals seeking insurance after they have been exposed to a cyber event?

Cyber insurance can be a great way to mitigate the damage caused by a breach, but it should complement cybersecurity technology as part of an overall cyber risk management plan. For a long time, there are several cybersecurity vendors trying to collectively sell their services, but companies have been reluctant to properly invest before a cyber event.

Some companies will only seek to implement the cyber controls after they have been breached which is more expensive because an organisation will be forced to implement protection immediately. The same applies to insurance, if companies are not investing in controls its value and why it is a good business decision for an organisation, they are often reluctant to buy insurance.

Cyber risks cannot be fully managed away, an organisation should do its best in implementing controls; but the threat is constantly changing and evolving. It is not possible to manage to zero risk. An organisation should reduce risk by implement strong controls that mitigate their threats, identify their remaining risk, determine how much risk they are willing to accept (their retention) and insure the remaining.

As Global Cyber Practice Leader at AIG, what is currently on top of your agenda?

Our top agenda is working with our clients to evaluate their overall insurance programme not just their cyber controls but their overall insurance portfolio, their crime property, casualty and other programmes they may purchase. AIG seeks to evaluate how our clients' insurance policies are responding to attempted breaches and cyber events and work with our clients to address this risk in the most holistic way.

Our clients should go through an assessment of their posture in developing scenarios of what could happen to them if they encounter a cyber events. Will it result in physical damage to their infrastructure, products, and services? Will it result in bodily harm or injury to employees and how will their policies respond?

This assessment is shared with our insureds to help them better understand their threat, control effectiveness and business impact. The assessment is provided in a boardroom ready document that can be shared with boards and C-suite executives. ■