StrategicRISK

GUIDE TO:

Technology risk

SUPPORTED BY AIG

95
Years helping insure brighter tomorrows
65,000
AIG employees worldwide
$1.5B
Global Property per risk capacity
AIG

100+
Countries and jurisdictions where we serve clients
90M
Clients served by the AIG companies
one
World Trade Center rebuilding as lead insurer

FOREWORD

Brave new world

The advent of technology has created amazing opportunities for businesses, that is if they are able to keep up

TECHNOLOGY IS CHANGING THE world at a pace faster than ever before.

The growth of computing power and the internet, combined with the spread of social media and the development of novel manufacturing techniques, has created extraordinary opportunities for business development, particularly in the past decade.

For all of the positive elements such changes have brought there are also some negatives and challenges, as large corporate businesses need to find flexibility in order to embrace some of these developments.

Even the smallest company can become a global player quickly, and crowd-funding can turn bedroom-based businesses into bona fide enterprises almost overnight

As such, competition is increasing and becoming less predictable as established market dominance is shifting as never before. Nowadays, even the smallest company can quickly become a global player quickly, and crowd-funding can turn bedroom-based businesses into bona fide enterprises almost overnight.

This guide aims to review some of the major current technological developments and assess how they might benefit, disrupt or threaten large corporate businesses around the world.

It also considers how companies can best embrace these changes or adapt to mitigate some of the inherent risks they create.

These are challenging and exciting times for businesses and the focus of this guide is firmly on the future, whatever it might bring.

Mike Jones,
editor, StrategicRISK

Editor Mike Jones
Deputy editor Kin Ly
Managing and legal editor
Hélène Préchac
Asia editor Jessica Reid
Executive editor, Asia-Pacific
Sean Mooney
Commercial director, Asia-Pacific
Adam Jordan
Senior production controller
Alec Linley
Senior data analyst
Fayez Shriwardhankar

Publishing manager Tom Byford
Publisher Jack Grocott
Executive publisher, Asia-Pacific
William Sanders
Managing director Tim Whitehouse

To email anyone at Newsquest Specialist Media, please use the following: firstname.surname@nqsm.com

SUPPORTED BY

AIG

Stay one step ahead of the hackers

As the sophistication of cyber criminals grows in leaps and bounds, the onus is on businesses to anticipate and block their attacks

CYBER RISKS ARE GROWING AND changing rapidly. No longer only an IT department or security issue, cyber risk is now an enterprise-wide risk management issue.

"The advent of the digital world and the inherent connectivity of people, devices and organisations open up a new playing field of vulnerabilities," says Mark Brown, executive director of cyber security and resilience at EY.

"Every day, hackers are working on new techniques to breach the security of organisations with the aim of causing damage, accessing sensitive data and stealing intellectual property. In an ongoing cycle, as old sources of cyber threat fade, new sources are increasingly emerging to take their place."

Anticipating and preparing for a cyber attack are imperative components for organisations to stay ahead of cyber criminals. "To get cyber security right, the first step is to activate available defences and get the foundations right," says Brown. "Such defences are not only technical software solutions but a mixture of governance, risk, compliance, people, process and technology, all of which should be aligned to business needs and strategies."

The next stage is to adapt cyber security to be more dynamic, better aligned, and integrated into key business processes, formally embedding itself within the business. "Once these two aspects have been delivered comes the real opportunity: the chance to anticipate and get ahead of cyber crime," says Brown.

"In the meantime, the threat landscape is rapidly expanding, the power of cyber criminals is growing and organisations are still struggling with a number of roadblocks." **SR**

Cyber security takes an enterprise-wide effort

Mark Camillo,
head of cyber, EMEA, at AIG

RECENT HISTORY IS LITTERED WITH examples of corporate titans humbled by cyber attacks, whether through the theft of customer credit card data, privacy exposures or the public humiliation of having their homepage or Twitter feed defaced. Some firms still feel their risk of falling victim to a cyber attack is low. However, in reality, all firms are now viable targets for cyber criminals, whether through the exposure of their corporate secrets or a privacy breach.

As the cyber threat has evolved, so has the corporate response: first came cyber security and antivirus, anti-malware software; later came the growth of cyber insurance as the scale of the problem grew and grew and firms began to look at risk transfer.

A point has now been reached where it is important to pan back and take a look again at the risk in its totality. These days, businesses are ready for a version 3.0 response to the risk. Cyber security risk is not only a technology issue. It takes an enterprise-wide effort to prevent attacks and to mitigate damage when they happen. The technology to prevent attacks is very effective, but the human factor or human error is a common thread.

Insurance carriers are beginning to partner with leading cyber security experts that specialise in the many components necessary to help clients monitor, mitigate, and manage the dynamic nature of cyber risk in addition to the financial protection and expert incident response needed after one occurs.

For example from a risk consultation and prevention perspective, AIG has recently partnered with K2 Intelligence, RiskAnalytics, BitSight Technologies, RSA (the security division of EMC), Axio Global, and IBM to offer insureds access to the pre-breach threat intelligence, governance tools and latest best practices to help gain a holistic understanding of their cyber security exposure.

Clients have access to a web-based training and compliance platform to help build a culture of security through strong company policy and employee awareness; customised intelligence on the deep web and dark net chatter about the organisation; insight into its cyber security posture ratings; identification of key functional areas of improvement to achieve an improved cyber security risk posture; security vulnerability scans; and more.

Risk managers need to work with other key stakeholders across their organisation and their broker to build an end-to-end risk management cyber security risk management solution and obtain the kind of cover that not only helps them after the event, but provides access to education and tools that enhance existing security practices already developed by the IT department.

However, a data breach not only causes damage that needs fixing, it can also cause network interruption. Thus, some firms are already looking to purchase extensions that cover the income loss stemming from systems failure caused by attacks or viruses, as well as those arising from internal failures, such as a patch that failed or an inability to access cloud services.

The threat of cyber attack continues to evolve and grow as do the protection and education provided by insurers, cyber security experts, and brokers. Risk managers need to constantly work with key internal stakeholders and their broker to craft a specialised enterprise-wide solution that prevents and mitigates damages of a cyber attack for the organisation.

The human factor

WHEN IT COMES TO CYBER risk, firms consistently overlook one critical vulnerability: their employees. Exploiting this weakness is key to a successful attack.

For example, hackers use clever tricks to convince staff to reveal key pieces of information they will be able to exploit to gain further access to the network.

This can be done by tricking people into either downloading some malware or giving information away on a website.

"The problem is that many businesses respond to this threat by saying, 'We must train employees better,' but the trouble is this is often not very realistic," says Professor M Angela Sasse, UCL's head of information security research and director of the Science of Cyber Security Research Institute.

"For example, how can you tell people not to click on embedded links when part of their job might entail clicking on those links for legitimate business? Also, how much time can you expect your employees to spend studying a URL before they click on it to make sure that it's OK? They have to get on with the job that they are paid for, right?

"So, when I go into businesses I ask: 'Are links important to your company? If they are, then you can't expect people not to click on them.'"

The problem with many cyber security policies is that they forget that businesses exist primarily to generate a

profit. This consideration has to be at the heart of any cyber security strategy.

> *'There is an unfortunate tendency among security specialists to think that humans are at fault for not spending all their time looking at security issues'*
>
> **Angela Sasse**, UCL

Busy staff

"It is impossible to expect people who are working hard – and most people have time constraints and too much to do – who are also not security experts, to disrupt their primary task and pay all their attention to these things," says Sasse. "That would ruin most businesses from a productivity point a view.

"Many businesses are currently not supporting their employees properly and they think that they can just dump this responsibility on them.

"There is an unfortunate tendency among security specialists to think that humans are at fault for not spending all their time looking at security issues. However, in reality, it is ridiculous to think that the average person has the time and capacity to do this.

"People are sensitive to their productivity being compromised." »

» Given this reality, the challenge is to design systems that can deal with risk and the need to be efficient while taking human fallibility into account.

"If firms expect their staff to make security decisions, then these have to be straightforward," says Sasse. "They have to have simple rules that can apply across the board. All too often, staff have to evaluate whether certain rules apply in certain situations and it's too much. If this approach was taken to health and safety, the health and safety officer would say that this was not acceptable."

Management trends

The situation is becoming more critical in part because of trends in management. For a long time, cyber security was seen as the preserve of the IT department, but in recent years this responsibility has shifted towards the entire enterprise. Although this approach can be effective, Sasse also warns of potential problems.

> *'Employers are accepting – perhaps without admitting it – that their employees will cut corners, because they can't afford to get an order out late or upset a key customer'*
>
> **Angela Sasse**, UCL

"With this approach, there can be a kind of tacit complicity by management in the tendency of employees to put their productivity ahead of complicated, long-winded security measures," she says.

"Whether for regulatory reasons, or whether it is the 'industry standard' to offer training for staff and place the responsibility on them, if it is taking too much time, employers are accepting – perhaps without admitting it out loud – that their employees will cut corners to get things done, because they can't afford to get an order out late or upset a key customer.

"Security rules must become an easy habit. If they don't become second nature, they won't work, and far too many policies are just not workable."

Sasse cites the example of a hospital where it might take 45 minutes for a caregiver to log on to the system in the morning. "That just won't happen," she says. "They don't have 45 minutes. Instead, the first person in will log on and everyone else will use their log in for the rest of the day – with all of the security problems that can cause, and the total loss of any hope of an audit trail."

Dialogue needed

Rather than take a top-down approach, Sasse argues that staff need to be involved in developing security measures – and listened to when they give feedback. "There needs to be a co-design process," she says. "There needs to be dialogue. All too often, measures are suggested and designed by security experts who do not look at how these will work out in practice.

"The business owners should also set performance goals for the security people, [such as] that a process doesn't take more than eight seconds or similar. Where this happened, the security people do respond to this."

Sasse advises is to ask employees what the biggest sources of friction are in respect of technology and working practices. Then, the findings should be taken to the security people and a demand be made to find a better way of handling the problem.

"Get the security people involved in the business," says Sasse. "The best security experts are already doing this; they understand their role is to be a business enabler, not merely thinking about risks but how to make things run better and increase productivity."

A well-designed security system can offer many business advantages. It may enable them to operate in more 'risky' environments because of improvements in the way their security is managing risk. It can also help in the way they interact with customers.

"Perhaps [customers] are not using services offered through a PC, because they find the security arrangements too complex," says Sasse. "By talking to them, it can become apparent that with a phone app, a greater degree of security and ease of use can be achieved, because the customer has more confidence there.

"Organisations may have been relying on a password for security. This can be a good system – if used frequently. However, if people don't access the product every day, they may find it hard to remember a password and frustrating as a result. Instead, perhaps something graphical, picture-based or biometric might be better. It is vital to think around the problem to get results.

"In the future, more situations will arise where the customer won't have to do anything and security will recognise them by their devices." **SR**

Pay up or we paralyse your business

By infecting a system with ransomware, criminal gangs can 'kidnap' a company's own data

RANSOMWARE IS AN INCREASINGLY common threat whereby hackers and criminals take possession of data through encryption and threaten to release or destroy it unless their demands for money are met. Although it originated in the 1980s, since 2012, the phenomenon has been amplified. "This is due in part to the increasing monetisation of cyber crime," says Gareth Evans, director at security consultancy KCS IS.

"Rather than thinking of cyber crime as hacking, as kids in their basement doing this for fun, [this should be recognised] as something undertaken by organised criminals to make money."

Companies spent an estimated $114bn (€102bn) dealing with malware-related cyber attacks in 2013, according to research by Microsoft and the IDC. The study states that losses caused by data breaches may be as high as $350bn.

Often, criminals exploit security loopholes with the aim initially of stealing intellectual property or data and selling that on. However once the information has been sold, the money pot has run out. Ransomware is another way of keeping the funds coming in.

"It takes some effort to get this kind of malware past corporate security and on to systems and so criminals want to maximise their profits," says Evans.

"Once they have sold what they have copied and stolen, they will somehow encrypt or put that data beyond use – effectively denying a company access to its own data – unless, of course, the board decides to pay.

"To accomplish this, criminals use highly sophisticated algorithms, which are very resistant to cracking."

As good as their word

The key to the continued success of these attacks, says Evans, is that when the ransom is paid, the criminals are as good as their word: the data is released and the company can carry on as normal.

"By doing this, they encourage people to pay," he adds. "When word gets around that if you pay, you will be all right and you will get the keys to the digital safe back, companies will hand over money more freely."

'Unless the company has a supercomputer, it has little chance of cracking the encryption'

Gareth Evans, KCS IS

Many companies do not appreciate just what a difficult position such an attack can put them in. They may have gone to great lengths to encrypt and protect data they see as valuable, such as credit card numbers. However other, more mundane aspects have been neglected, and when hackers take control of the day-to-day data that companies rely on – such as sales and purchasing data or email systems – it paralyses them.

Knocking out a global law firm's email system, for instance, could cost thousands of euros quickly. According to Solutionary's *Global Threat Intelligence Report*, it can typically cost firms $3,000 a day for up to 30 days to mitigate and recover from malware attacks – and that covers only consultants, PR crews, incident response teams, mitigation software and other immediate investments, not lost revenue from systems downtime or lost productivity.

"All organised criminals have to do is stop a business running to force it to meet their demands," says Evans. "There are even types of malware that will change only the way in which computers access the internet, meaning that the organisation will be bombarded with pop-ups or otherwise disrupted until it pays up."

The problem for corporate security and risk management is that the malware is encrypted and by the time it is on the corporate system, it is already too late. "Unless the company has a supercomputer in the basement, it has little chance of cracking the encryption," says Evans. "Even the National Security Agency would struggle.

"The only solution is to prevent the malware from infiltrating the IT system in the first place."

The criminals are winning

To do this, risk managers and IT staff must encourage an enterprise-wide approach to cyber security and make sure everyone knows what not to do. The key is to use secure devices and to be careful online and with email – but even this may not be sufficient.

"Malware will get through typical virus protection systems," says Evans. "It is important to rethink the way in which cyber crime is approached – Hollywood may have created a picture that hackers are young computer geniuses as portrayed in *The Matrix* or *Die Hard*. However, they are not; they are criminal gangs. and, at the moment, they are winning.

"To stop them, what firms need to remove the capacity for human error. In most walks of life, that cannot be achieved, but within IT, it can. Better security systems can be designed and this needs to happen now." **SR**

Getting entangled in the internet of things

ALTHOUGH IT IS EASY TO PREDICT some of the consequences of the growing popularity of connected devices, many will not be understood fully for some time. Insurers need to pay attention now, however.

Each of the two main concerns – security (cyber risks) and property liability (casualty) – has the potential to affect the other, and other lines of business can also be affected, as was exemplified, for example, in the 2014 attack on a German steel plant by hackers: see box right.

This demonstrated how, if connected devices are attacked or malfunction, people and businesses can be at risk, thus creating new product liabilities.

The question insurers need to be asking is who will identify and allocate fault and who will pay.

Under traditional principles of strict liability, fault flows up the chain of distribution from the retailer to the manufacturer through mid-channel distributors. However, in the case of connected devices, new complexities arise.

For example, will the software developer be liable if a connected device causes a loss? Who is responsible for its vulnerability to attack? Will the consumer become a target for fault apportionment if they failed to update security software, used easily hacked passwords or downloaded malware from insecure sites?

Insurers need to decide now how to manage these claims and what kind of expertise they will require to do this – as well as what other lines may be affected by the internet of things, such as financial lines, property, marine/cargo and aviation. **SR**

WHEN HACKING GETS PHYSICAL

Discussions about cyber security usually focus on the risk of damage to brand and reputation caused by security breaches or compromised systems.

However, another, much more serious risk is emerging: that of actual physical damage.

In December 2014, hackers accessed networks at a German steel mill and disrupted control functions to the extent that a blast furnace could not be shut down properly, causing "massive" damage.

This type of attack first made the headlines in 2010 when the Stuxnet worm – widely thought to have been deployed by the US and Israel – disrupted Iranian nuclear facilities.

Both attacks highlighted the danger hackers pose to key infrastructure and their ability to cause real-world damage. It is feared incidents will only increase as industrial systems become more complex and interconnected.

PREPARING FOR THE INTERNET OF THINGS

Wearing clothes that can talk to the internet and update users on their health and wellbeing might grab the media's attention, but the implications of the internet of things (IoT) go way beyond enhancing consumers' experience.

There are already an estimated 10-20 billion devices connected to the internet and this figure is expected to reach 40-50 billion within five years. Smart businesses in all sectors will be able to use this major boom in connectivity to radically alter the way they work, creating greater efficiency, productivity, safety – and profits.

However, these new rewards bring with them new risks, from the increased opportunity for cyber breaches, to shifting questions of property and products liability.

Businesses cannot afford to enter this new technological world unprepared.

Fortunately, the insurance industry is already well positioned to help businesses navigate this new frontier and many of the elements of the IoT have long been used by insurers to better understand risk and improve safety.

In addition, just as insurers will be able to help their customers navigate a changing world, so they will be able to better adapt their own core services at the same time, and provide an ever-improving protection.

For more on the IoT, read AIG's white paper at www.aig.com/iot

DYRE WOLF: THE MECHANICS OF A CYBER ATTACK

Since 2014, the 'Dyre Wolf' attacks have used a variant of the so-called Dyre malware to steal between $500,000 (€445,000) and $1.5m from targeted organisations.

The attacks show just how sophisticated cyber criminals are. Combining fairly simple, freely available malware with some old-fashioned patter, the gang drilled through corporate security.

Organisations affected were those that frequently made wire transfers of large sums of money – although how they were identified is not yet known.

Most antivirus tools failed to detect the malware, which monitored operations the instant a victim at one of the organisations logged on to a banking website.

At that moment, it fired up a fake screen explaining that the site was having technical issues and that the victim should call a number to get help.

That number led to the criminals, who set about convincing the employee to reveal bank details.

Those who did were fooled into believing that they had made the correct transfer. In reality, the funds were bounced around a network of global banks until they reached the gang's account, beyond the reach of the victim, their bank and law enforcement.

Essential facts about digital due diligence

A Q&A with Hannah Fish and Oisin Fouere of K2 Intelligence, which is working in partnership with AIG

What is digital due diligence?

A digital due diligence is an examination of an organisation's IT systems and procedures to determine potential associated risk or even existing compromise to company assets. It includes a review of internal security technology and controls, processes and policies, as well as an external look at potential threat factors. A company might have a misconfigured firewall or may not enforce periodic password changes. It may be in an industry that has suffered few cyber attacks or in one that is frequently attacked by criminals or even competitors. All of these, and many more, affect the potential risk to company assets.

What makes a good score?

A good score provides a comparative analysis to industry averages. It also highlights deviations from current best practices. It needs to consider multiple facets of cyber security, not only IT security systems and controls but also risks that may arise from physical security or operational policies. This should be carried out with careful consideration of the external threats to the business. For example, if a hacker organisation declares that one company is a target for future attacks, this information needs to be included in the assessment. Lastly, a good score needs to be linked to the business value of

each asset at risk. High risk of breach to a low-value asset is not as troubling as a low risk of breach to a critical asset, or one that has cascading effect on the organisation.

How can risk managers get a better score?

Once valuable assets have been identified and major gaps have been mapped against these, closing down the biggest gaps will provide the most dramatic improvement to a company's risk score. Although it is tempting to consider the introduction of new security technologies and systems, an improvement in procedures and policies often have the biggest effect on an organisation's overall security posture. This activity should always be followed by a comprehensive monitoring and compliance programme to ensure that the risk manager can adequately measure the improvements to their risk posture. **SR**

INTEGRATING CYBER RISK MANAGEMENT WITH YOUR ERM: KEY QUESTIONS

- When and how should an organisation disclose to investors and shareholders that it has been the subject of a damaging cyber attack?
- Is the cyber security strategy aligned to the organisation's risk appetite and risk tolerance?
- Are the financial consequences of a cyber attack fully understood? Has the organisation looked beyond the immediate expenses such as direct loss and remediation expenses?
- Do the firm's technology officers understand how its cyber security approaches must flex in response to its strategic and operational policies?

Mark Brown is executive director of cyber security and resilience at EY

Inside a cyber intelligence service

K2 Intelligence's Hannah Fish and Oisin Fouere explain the security value of collating information

'In many cases, the intelligence indicates an attack that had not been identified'

Hannah Fish and Oisin Fouere, K2 Intelligence

What is cyber intelligence?

Cyber intelligence generally refers to the collection, analysis and dissemination of information relating to digital security threats. The collection of information is traditionally captured from a range of sources, including open sources, such as social media, closed sources, such as vendor vulnerability announcements, and human sources, such as cyber group infiltration. In many cases, each source allows for the enrichment of the intelligence product, enabling the affected organisation to ensure that it has the necessary defences in place prior to the execution of an attack. In particular instances, the intelligence may provide evidence of an existing security compromise that results in the organisation deploying an incident response team.

How does it help firms address their cyber risk?

Many firms rely on static information security controls that permit only the identification of an existing threat. Firms that employ managed intelligence services or, alternatively, develop internal intelligence functions, are provided with a much clearer picture of the threat vectors facing them, enabling them to put in place appropriate security controls and respond to potential security breaches in a more timely manner. In addition, having the appropriate dissemination process enables management to allocate and prioritise resources and budgets in a more targeted manner.

What business advantages does it offer?

In many cases, although it may not prevent the launch of an attack, it will enable the organisation to better identify and respond to potential and ongoing attacks. The intelligence collected from our analysts often indicates the presence of an attack that had not been identified by any of the firms' existing cyber security controls. This enables the firm to adequately deploy or engage incident response specialists to contain the attack and execute remediation measures. **SR**

Don't let complacency land you in court

Company directors, be warned. Leaving cyber security to the IT department alone is a gamble you cannot afford to take

BY NEGLECTING CYBER SECURITY and leaving their network to be looked after by the IT department, many company directors could be placing themselves in serious danger.

In the event of a major data breach, directors are likely to face legal action, having to prove they did everything they could to take cyber risk seriously and protect their company. For this reason, cyber is no longer an issue directors can delegate to someone else.

Of particular note is the risk of derivative shareholder lawsuits. These are already happening frequently in the US and there is a fear that many multinationals do not yet understand their exposure to this threat. The expectation is that they will emerge in Europe soon.

In June 2014, Dennis Palkon, a shareholder of Wyndham Worldwide Corporation, filed such an action against that company's board of directors in response to three data breaches between 2008 to 2010. Similar shareholder claims have been lodged against the retailers Target and TJX Companies (owner of brands such as TK Maxx).

These kinds of cases assert that directors are personally responsible for internal failures to prevent, respond to and report data breaches effectively.

Of course, in such circumstances, many board members may take some comfort from their directors' and officers' cover – but exactly how these policies will respond is unclear. Some may contain exclusions around privacy that may limit or deny cover.

In this environment, risk managers need to make sure that they are working with their brokers and insurance partners to constantly re-examine and interrogate their cover to identify gaps.

In addition, when a major cyber event occurs, the main risk is of brand damage and no insurance policy can cover for a damaged reputation. In addition, individuals who have been affected – namely shareholders – may see this as a third-party attack and take action. **SR**

WHAT IS BIG DATA?

Big data is commonly defined in terms of the 'three Vs' developed by the analyst Doug Laney in 2001

Volume

The amount of data being generated by business has increased significantly. There are many reasons for this. For example: it has become easier to store things such as transaction data; social media creates huge amounts of unstructured data; and machines and computers increasingly talk to one another while carrying out a range of functions that generate more data.

The challenge is what to do with this data and how to make it relevant.

Velocity

Not only is there more data, but it is arriving more quickly, placing firms in the increasingly difficult position of trying to collect it all and make sense of it. For example, a smart meter may provide a utility firm with some commercially useful information, but how can it be managed in real time and scaled up successfully as the technology becomes more popular?

Variety

In addition, the data arrives in many different formats, from the numeric data contained in database fields to free text documents, social media, audio and video media, email and more. Managing this, and sorting it to the extent that it can make useful comparisons, is a major challenge.

A matter of trust

Sources of data have never been more numerous, but firms should be wary about taking the information at face value

AS IBM'S STEVE MILLS SAYS: "When it comes to big data, clients need to apply the handbrake at times.

"Yes, it's a great opportunity and some aspects of business do get excited about the potential to do things in a new and more agile way using new forms of data, whether it's coming from social media or devices or elsewhere.

"However, there are real issues in respect of trust. For example, if gathering data from social media, how does one know it's real? In the case of a tweeted complaint, how does one know it hasn't been sent by a competitor?"

According to Mills – IBM's insurance big data analytics, digital and mobile consulting lead – being clear on the risk posed by external social media data is vital, as it remains almost impossible to verify with any certainty. Are all of the devices used to generate data secure at the point of use? Are they providing good data and, importantly, can they be hacked?

"Telematics is another interesting example," he says. "If an organisation is using phones to generate data, again trust issues arise. For example, with motor insurance, if I am sitting in a car with my mum, and she is a safer driver than me, and my insurer is gathering data from my phone about how the car is travelling, then it is getting it wrong."

When facing this risk, organisations need to assess not only the upside of big data, but also the risk. "This is complicated," says Mills. "Real issues need to be addressed in this space. People need to go into using big data with their eyes wide open; start with one device and see how it performs. An external agency should be employed to analyse and format data so it conforms to actuarial requirements."

Too much information

It is also important to ask how valuable the data being gathering is and whether the exercise is worthwhile. Accumulating information from someone's smart fridge might be of little use when compared to data on river levels that has a real potential to help reduce flood losses. "For a logistics company, being able to track where the cargo is will be useful," says Mills.

"Being able to monitor how a truck is being driven and whether fuel efficiency is being maximised will be useful. In banking, big data could have a real effect on the way credit risk is analysed before a loan is granted.

"However,e many sources of data are just not useful."

> *'How do you know if the social media data is real? In the case of a tweeted complaint, how does one know it hasn't been sent by a competitor?'*
>
> **Steve Mills**, IBM

The fact that new technology is rapidly increasing the scale and type of data can compound the problem.

"Quantity can certainly be a problem for some companies," says Mills. "Taking the telematics example again, this technology can generate a significant amount of data and some firms are not yet used to handling this.

"However, a smart solution is available. This is not personal injury data; it may link to a car, but it doesn't say who is driving, and so some clients are outsourcing this process. The real value of the data is in its aggregation and its ability to help with pricing.

"This kind of approach could become a trend with the growth of the internet of things, where companies want access to the data, perhaps not immediately, but certainly in the future when they become more mature in a market. However, they don't want to store the data themselves or keep it within the organisation." **SR**

DATA'S DRAWBACKS

An increasing reliance on data poses two major risks to business.

The first is reputational. "This will have indirect financial consequences as individuals lose confidence in the company," says Caroline Baylon, research associate, science, technology, and cyber security at Chatham House's International Security Department.

"Customers may be very hesitant to trust [an organisation] knowing that they have to provide their personal data.

"In the Blue Cross loss [a data breach at the US health provider Premera Blue Cross this year, thought to have affected up to 11 million customers], the loss of so many social security numbers means that millions of Americans need to monitor their credit ratings for life."

The second risk to business is directly financial. "For example, I've read a number of cases of banks refusing to reimburse their customers for losses on various grounds.

"It seems that banks are becoming increasingly affected as the size of the losses increase, because my impression is that in the past, they reimbursed much more automatically."

According to Baylon, firms need to make sure they are protecting their critical assets. "This needs to be on different levels, with the most critical information most heavily protected," she says.

Insurance is also critical, but it is important to make sure that a product is providing a real advantage and not merely helping with compliance or ticking boxes. **SR**

The year of living dangerously

Data vulnerability has become a major concern in the past 12 months, posing three distinct risks to organisations

DATA VULNERABILITY AND security is an issue for all organisations, regardless of their industry sector.

"The risks of unauthorised surveillance, fraud, theft and hacktivism have become particularly apparent in the past 12 months, with a number of high-profile data security incidents in Europe and the US," says Arthur Artinian, partner in law firm K&L Gates' London office and a member of its intellectual property group.

"The issue is not specific to data-intensive businesses. It applies to any organisation that holds or collects individuals' data, whether intentionally or inadvertently. Of course, the risk profile increases as businesses become more data-intensive, particularly for businesses that are built around big data – for example, the use of geolocational data of customers –and those that operate across borders."

Data security poses three key categories of risk to businesses. "Legal risk arises where a business does not meet regulatory compliance requirements or is exposed to contractual or civil liability when incidents occur," says Artinian. "Operational risk causes business disruption and interference with internal and external communications. Reputational risk arises owing to significant public awareness and scrutiny of the data security issues."

European overhaul

A survey commissioned by the UK Department for Business, Innovation and Skills in 2014 suggests more than half of UK businesses had already experienced a loss of data or leak of confidential information in the previous 12 months.

More than 75% said they had been subject to external data security attacks.

"The European data protection regime is currently the subject of an overhaul, due to be finalised in the next 12 months," says Artinian. "Once implemented, the new EU-wide regulation will impose additional regulatory burdens, including requiring businesses to obtain specific consent from data subjects and introducing significant fines for breaches.

"At the same time, European lawmakers are progressing a draft cyber security directive that will impose regulatory and best-practice obligations on business in key sectors, including those involved in the provision of essential infrastructure and services. Similar moves are under way in the US." **SR**

'The new EU-wide regulation will impose additional burdens'
Arthur Artinian, K&L Gates

Reach for the crisis plan

A data breach can significantly damage a company's reputation, which makes preparing for one all the more critical

DATA SECURITY IS NOT ONLY A legal issue. "It is a significant reputational issue that attracts media attention," says Arthur Artinian, partner in the London office of law firm K&L Gates and a member of its intellectual property group.

"A multi-stakeholder, enterprise-wide strategy is therefore essential. Every business should have in place some form of cross-functional cyber and data risk team that includes representatives from the IT, legal, operational, PR/corporate communications, risk management and senior management/board.

"That team should, if it hasn't already, develop a crisis plan for managing and responding to security incidents in the specific business context."

At an operational level, businesses should conduct a holistic audit and review of how they collect and use data, and test those findings against their legal and regulatory obligations.

"If third parties are involved in the use or collection of third-party data, contracts that are entered into with those parties should impose strict obligations to ensure that legal and regulatory obligations are complied with down the supply chain," says Artinian.

Of course, insurance also has an important role to play in the cyber risk management toolkit, because it facilitates the assessment and transfer of cyber risk.

Assessing coverage

Sarah Turpin, a partner in the litigation and dispute resolution and insurance coverage practice groups at K&L Gates' London office, says: "Some cover for cyber risk is likely to be provided by existing insurance policies, but such policies have not historically been designed to cover the risks arising from intangible assets and network-related risks.

"A careful assessment of the coverage provided by existing policies is essential, as there are likely to be potential gaps in cover, which can be filled either by enhancements to existing policies – where available – or through the new cyber insurance products being offered by insurers."

Although the cyber insurance market has developed rapidly in recent years, the scope of cover provided still varies significantly. Some policies still impose very onerous terms and conditions that may enable the insurer to deny or limit the cover provided.

"A careful assessment of the policy terms, conditions and exclusions is essential to ensure that the policy is fit for purpose and there are no exclusions or limitations that could prevent payout in the event of a significant claim," says Turpin. "Some insurers are now providing access to their own panel law firms and cyber security specialists to assist insureds in the event of a cyber crime incident or data breach.

"This may prove beneficial in certain jurisdictions, but some insureds may prefer to use advisers they are already familiar with in what can be a crisis situation. Either way, it is worth considering these issues up front and attempting to reach agreement with insurers over who should be appointed.

"The purchase of insurance should be used as part of the risk management process and most insurers are likely to expect insureds to have appropriate incident response plans in place." **SR**

ALL AT SEA: TACKLING THE CYBER RISK TO SHIPPING

The sea has always been a dangerous place to do business and the shipping industry's increasing reliance on computerised systems in all areas of operations brings with it new vulnerabilities.

For example, in July 2013, researchers from the University of Texas demonstrated that hackers can change a vessel's direction by interfering with its GPS signal, which could cause the onboard navigation systems to pick up a false position and heading.

A hacker also forced a floating oil-platform off the coast of Africa to shut down by tilting it to one side, and evidence shows that Somali pirates have employed hackers to access shipping companies systems to identify vessels passing through the Gulf of Aden with cargoes and light security; something that led to the hijacking of at least one vessel.

Unfortunately, awareness of this threat is still too low. Marine operators need to improve their risk management by adopting the same rigorous systems and protocols as forward-thinking firms operating on land.

However, because shipping is, by nature, open and companies rely on interaction with a wide range of partner organisations, more needs to be done to establish global standards.

The International Chamber of Shipping, the Baltic and International Maritime Council, INTERTANKO, and INTERCARGO are developing guidelines and best practices, which it is hoped will be presented to the International Maritime Organization for approval in 2016.

In addition, underwriters need to look at the risks that they are writing, in particular, the way in which these can be aggregated on larger ships running more complex operations.

Everyone involved needs to read the weather well: a storm is brewing on the horizon and the time to start plotting a safe passage is now.

Smarter than the average software

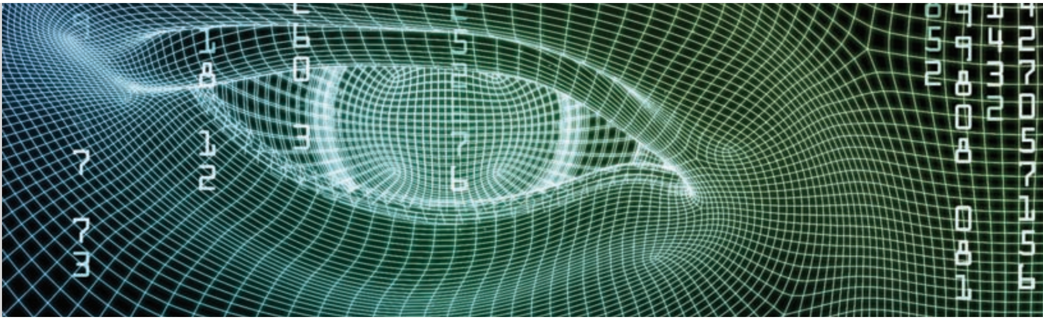
With its breadth of knowledge and ability to understand human languages, cognitive computing is the next line of defence in the fight against cyber crime

IN AN ATTEMPT TO TACKLE SOME of the major cyber risks of our time, IBM is developing 'cognitive computing' technology. "We focus on what I call 'security intelligence' – the process of getting useful information from all the data that we are gathering by pulling it all together and analysing it visually, in such a way that it is really possible learn about what's going on," says Martin Borrett, director of the IBM Institute for Advanced Security, Europe.

"In this realm, there is already machine learning – or cognitive computing – involved, and this technology is becoming important to tackle the challenges posed by the volume, veracity and sophistication of the attacks everyone is facing."

As criminal gangs are increasingly using the 'dark web' or the 'deep web' to share information, their attacks, such as Dyre Wolf (see box, p11), are becoming far more sophisticated and precise.

"The question is whether the resources – and, more importantly, the expertise – are available to avoid or



mitigate these attacks?" says Borrett. "This is where our security intelligence comes in, because it enables us to keep experimenting and look to the art of the possible.

"This is concerned with trying to [establish] the potential in technology and then applying it to problems where it can really add value. Its ability to view language in natural form, to score and give weighting to data – these give it real potential in the security space.

"You load a corpus of knowledge, you teach and train it. It ingests data from a whole load of IBM sources and other, external sources to build up this huge breadth of knowledge and you teach it about key relationships. Then you can test it, ask it questions and really get to grips with the problems you face."

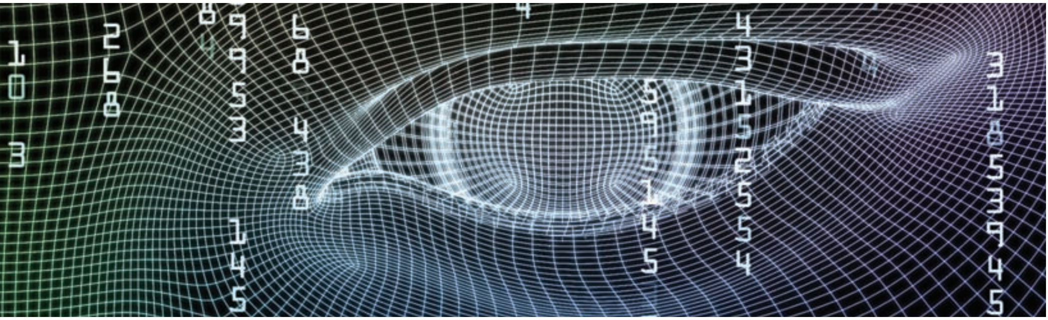
Future potential

This is potentially a powerful tool in a fast-moving security environment. "Cognitive computing will have the potential in the future to augment what we are doing today," says Borrett. "People often describe security as a game of cat and mouse, and it is. It never stands still. Things are always changing. Security intelligence has the power to offer a different perspective.

> *'It can look far and wide, explore multiple hypotheses, come to a judgement on them and come back with a series of proposals'*
>
> **Martin Borrett**, IBM Institute for Advanced Security, Europe

"A lot of what IBM does at the moment is analytic: bits and bytes and very numerical. The power of cognitive computing is in its capacity to use natural language to bring a whole new range of data to us. It can look far and wide, explore multiple hypotheses, come to a judgement on them and then come back with a series of suggestions and proposals. It can help establish what is behind an attack and even when another attack will be likely to happen.

"It won't replace what we do now, but it may well make it a lot better." **SR**



Social network

What doesn't kill you makes you stronger

Digital disruption, namely using new technology to compete with corporate dinosaurs, wiped out the likes of Blockbuster Video. Digital transformation provides a practical alternative

DIGITAL TECHNOLOGY IS transforming approaches to business. Irrespective of the sector, when it comes to staying ahead through innovation, the message is 'be quick or be dead'.

"In the list of Fortune 500 companies in 2000, 52% have either gone bankrupt, been acquired or ceased to exist," says Neil Sholay, senior director of products and industries, EMEA at Oracle. "In most cases, this has happened owing to digital disruption of their existing business model. It might have been not called that then, but that's what it was."

Digital disruption is the use of new technology – or a business model based on new technology – to significantly affect an existing value proposition.

"Probably the most famous examples are when Netflix entered the video streaming market and destroyed Blockbuster in the process, or when Uber entered the taxi market globally and severely affected local providers," says Sholay. "A similar effect may well happen with Amazon Dash.

"This hasn't yet launched, but it looks as though it could be huge. The technology resembles a little microphone, and it enables users to scan a grocery item in their home – say a can of beans needs replacing – or even talk to it and order whatever is missing immediately. It's turning the entire model of grocery shopping on its head because instead of getting a big shop in, products are delivered as and when required, all the time."

Of course, this kind of development is not happening in all businesses all the time. If it were, the market would be in chaos. "Most of the conversations I have tend to start with digital disruption and move on fairly quickly to digital transformation," says Sholay. "What is happening in 99% of the organisations

I work with is that they are looking at the potential disruption posed by new technology and changing the way they work. They are certainly moving faster than they would have done otherwise, but this deals with transformation, not destruction."

Everyday business

Innovations might, for instance, involve the use of data, drones, robotics or identity management. "Organisations are giving digital some kind of leadership role, and about 30% of the companies I deal with now have a chief digital officer," says Sholay. "It varies from industry to industry and territory to territory, but it is happening.

"The best examples are incorporating digital into their everyday businesses. In some companies, the board is handing down tasks to their digital innovation groups, giving them areas to innovate around and tasking them to produce results. They may even be asking them to compete with each other in doing so. This is a totally different way of doing business."

These changes are not only limited to the kind of consumer-focused brands usually associated with new technology.

"Siemens, Bosch and many other manufacturers have invested heavily in big data, robotics and technology in general because they have seen that not only can new technology make their businesses run better, it can also really compress the amount of time it takes them to get a product to market."

For example, robotics firm ABB recently launched YuMi (you and me), the world's first dual-arm robot that can work safely with people without having to be separated from them by a safety cage. It is hoped YuMi will revolutionise monotonous tasks such as small-parts assembly, which is hard to repeat with consistent quality and precision.

Some of the anything-is-possible attitude of start-ups is trickling up to the

'Time and again, the big barriers are culture and behaviour. How does Bank of Scotland get 5,000 tellers to start thinking digitally?'

Neil Sholay, Oracle

large multinationals. "They are looking at what is happening and asking: 'How can we be more like a start-up?' However, the real problem they have in doing that is the sheer scale of their operations.

"Time and time again, the big barriers are culture and behaviour. How does Bank of Scotland get 5,000 tellers to start thinking digitally?

"Large companies are beginning to understand and this is why HR are coming to the workshops I run, because they are realising that they need to make changes to the way they recruit and train staff.

"It's no good launching an amazing app if the staff in the call centre just don't understand how it works when someone calls to ask for help."

Transforming customer experience

According to new research by MIT and CAT, about 44% of businesses are using digital to transform their customer experience offering, about 30% are using it for operations and 26% for short order innovation, which is genuine 'disruption'.

"We are at the stage where every business is now being affected by technology," says Sholay.

"If an organisation is not looking at what digital can do for it in all areas of its operations, whether it is B-C, B-B or even a government department, then it is putting at risk its very livelihood". **SR**

The future's driverless, or is it?

To their champions, autonomous vehicles herald a revolution on the roads – but safety and security worries are mounting

FOR MANY, IT STILL SEEMS A step too far. However, manufacturers are convinced that once we all get used to the idea of driverless vehicles, they will become commonplace and that reconfiguring our relationship with cars – moving us from driver to passenger – will make our roads safer, more efficient and more relaxing.

Intelligent automobiles also offer innovative comforts, enabling passengers to synch their smartphones and enable various useful features, from traffic alerts to media streaming.

For manufacturers, the possibility of live data from the vehicles offers significant advantages in terms of monitoring performance and maintenance issues.

However, nothing comes free and concerns are already mounting. For example, what happens to all the data being generated? Users might consent to their insurer having access, but what about the risk of being hacked? Could this compromise security or privacy?

Many in the industry are convinced that these issues can be addressed, citing the successes autonomous vehicles (AVs) are already having in industry.

Dr Peter Harrop, chairman of market research and business intelligence firm IDTechEx, says: "Autonomous vehicles that are well established in relatively controlled environments – such as under water, in the upper atmosphere and in nuclear power stations – offer well-understood parameters and history.

"At the other extreme, the intended autonomous cars weaving between driven vehicles, pedestrians and police on foot directing traffic have many unknowns and unquantifiable hazards.

"In between come multicopters following sportsmen to video them and similar applications and search-and-rescue robots in disaster scenes that can cause accidents."

> *'Autonomous cars weaving between driven vehicles, pedestrians and police directing traffic have many unquantifiable hazards'*
>
> **Peter Harrop**, IDTechEx

Pace of change

In response, the automobile industry must do all it can to mitigate such threats during design and manufacture – and then communicate that to customers. Security and, in particular, digital security, has to be a top priority, forming an integral part of the design, production, supply chain, sales, warranty and maintenance process.

Manufacturers face real challenges in doing this, not least the rapid pace of change. Functionality and affordability will no doubt improve through experience, but the speed at which developments occur works against the constraints imposed by proper testing and pre-release checks and balances.

"What use is a five-year test on a radar when a lidar replaces it?" asks Christopher Poulin, a research strategist with IBM's X-Force security research group. "What to do with long-term tests on a battery when it is replaced by one of the new lithium-ion capacitors? All this vast number of new innovations can bring initial lack of reliability and predictability with them, yet if anything has to be superlatively reliable

> *'Vehicles are no longer islands of electromechanical engineering – they are components of a larger system of systems'*
> **Christopher Poulin**, IBM

and predictable, it is the autonomous vehicle operating near people."

As these vehicles become more popular, transport networks will become more crowded, adding to safety and security challenges.

"AVs are particularly lethal if flying over a crowd of people or navigating a crowded road with pedestrians crossing," says Poulin.

"Connected vehicles are intended to be designed and built with security as a foundational requirement. However, vehicles are no longer islands of electromechanical engineering; rather, they are components of a larger system of systems, which integrates the vehicle, roads, manufacturer and consumer to provide a safe, secure transportation experience.

"Much as they expect anti-lock brakes, airbags and seatbelts as standard features rather than aftermarket or retrofitted options, today's consumers demand digital security that is delivered unobtrusively with the vehicle. This realisation will drive new revenues for forward-looking suppliers and manufacturers, as well as decreased costs for consumers and original equipment manufacturers.

"Those that can deliver the safety and convenience features consumers desire while also assuring their safety and security stand to leverage the true power of the connected vehicle."

Networks

However, getting to grips fully with emerging risk demands looking beyond the car to its interactions with the surrounding world.

"The connected car ecosystem should be viewed as a 'network of networks' or a 'system of systems'," says Mark Brown, executive director of cyber

security and resilience at EY. "It is only one more link in a much wider and complex network.

"When taking this point of view, we see the need to shift the emphasis from the connected car as a clearly defined system [to] the network itself… Security then defends those interactions and is no longer limited to the car as a thing."

In addition, because the connected car 'lives' in the network, security extends beyond closing doors and encrypting data. "Security means managing shared data and a more complex network of participants," says Brown. "Opening the onboard network to the internet means that legacy networks and applications become exposed and the 'attack surface' increases as the business model expands to new areas, partners and user types.

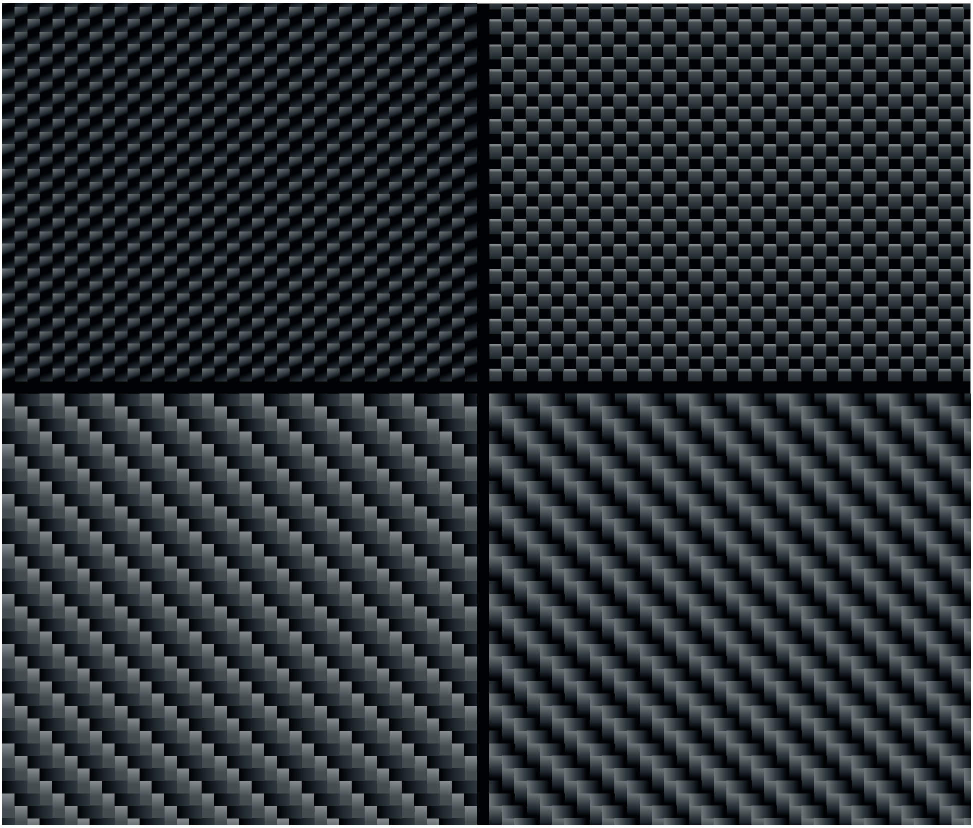
The target of protection, the object of security, becomes the network of networks, not the individual car. "All cyber security measures and technologies need to be aligned with this goal in mind," says Brown. "Security requirements must be addressed at the application or channel level.

"When considering connected car initiatives, businesses need to establish a solid legal understanding of data ownership and data protection policies. Only on that basis will it be possible to design agile and secure services that will enhance business operations.

"Connecting to multiple trusted and untrusted networks requires a new trust model, but closing the trust gap between the manufacturer and the car owner and between the manufacturer and commercial partners means balancing risk and trust considerations to create a win-win situation for everyone." **SR**

Handle with care

The fiercely competitive aviation industry has turned to lightweight composite materials, but are they safe?



AVIATION IS A TOUGH BUSINESS. Attracting customers is not necessarily that hard – more and more people fly every year. By 2034, it is estimated that passenger numbers will reach 7.3 billion, which represents annual growth of 4.1% or a doubling of the 3.3 billion passengers who flew in 2014, according to research by the International Air Transport Association (IATA).

The problem is that competition is intense, capital investment costs are high, cash flow is challenging and changes in the cost of fuel can mean the difference between success and failure. In these circumstances, any savings that can be made on fuel can make a major difference.

Attention has therefore turned to new, versatile, composite materials – primarily carbon fibre, glass fibre and aramid-reinforced epoxy – which offer an opportunity to reduce weight during the manufacturing stage.

They can be used both structurally and in components to create complete aeroplanes, helicopter rotor blades, propellers and even seats and instrument enclosures. However, these materials also bring with them new risks in terms of ongoing use and maintenance.

"Where traditionally a frame might have been made out of steel – which is strong but heavy – composite material offers similar strength but at far, far less weight," says AIG aerospace specialist Stuart Boyd. "Holes can be drilled in them, they can be painted and they can take on almost any part of the manufacturing process. They are lighter, meaning aircrafts burn less fuel. They can be more flexible.

"Where the risk element comes in is when the material breaks in use. For materials such as metal, they can be subjected to a lot of traditional metallurgical testing processes to establish when they might fail.

"It's not so easy to do this with composite materials. I have seen examples of where helicopter blades made of composite materials have failed catastrophically. When you look at what's been going on, you can see that in a very few instances they just haven't had the same degree of quality control and

'These things are like Airfix kits – if they are bent or heated or otherwise over-stressed, entire sections have to be written off'
Stuart Boyd, AIG

non-destructive testing as their metallic counterparts."

Damage perspective

Also, from a damage perspective, there are risks. "Where metal can be patched, riveted and welded, composites can't," says Boyd. "These things are like Airfix kits – if they are bent or heated or otherwise over-stressed, entire sections have to be written off. Traditionally manufactured aircraft structures could be repaired fairly quickly. Nowadays, unless an entire structural component is ready to go, [the aircraft] is potentially out of action for a greater period of time."

Finally, composite materials are toxic when burning and can potentially make a crash site challenging to manage from a rescue position and an environmental position.

"With composites, continuing airworthiness needs to be given good consideration. What is an approved repairs process for an alloy-based aircraft is not directly read across to composite-based aircraft," says Boyd.

It is acknowledged that industry and academia are forming strong partnerships to rapidly resolve these issues".

He has similar observations about the use of lithium polymer batteries in aerospace. "These are very small in terms of bulk size and weight when compared to normal batteries, and so they offer similar advantages in terms of weight and consequent fuel use," he says.

"However, they also contain highly reactive chemicals and are made up of a series of cells that have to be charged in a 'balanced' way.

"If they're not, the battery can malfunction and potentially catch fire. New and pioneering technology brings challenges as well as clear benefits for customers but, above all, the manufacturers' focus is making certain that the engineering will remain safe throughout its lifetime." **SR**

> *'Where traditionally a frame might have been made out of steel – which is strong but heavy – composite material offers similar strength but at far, far less weight'*
>
> **Stuart Boyd**, AIG

A global issue with no borders

Anthony Baldwin,
AIG managing director and
head of distribution, EMEA

CYBER IS A SHORT WORD FOR A BIG RISK and as this report illustrates, new technology is creating perils that increasingly cross across all areas of operations.

However, although there is an overall sense that these risks are ever-evolving and growing fast – seemingly not a day goes by without a new virus or hack attack hitting the headlines – many firms are not fully aware of this developing situation.

Certainly, companies now place cyber higher on their risk register. However, there is still a lack of understanding about what is at stake and what the threat is.

In this environment, it is critical to engage an insurance partner that has a deep knowledge of the risk. AIG has been in the cyber market for 16 years and insures more than 20,000 clients.

We have seen the peril evolve and change and understand why your response needs to involve much more than only risk transfer: firms need to make sure they engage help with risk management and mitigation as well.

Our approach is to work with clients from the off to help them prepare themselves and become more resilient.

When we first analyse their operations to assess and understand their risk we do not merely see this as means to help us provide cover, we actively use the results to provide our clients with advice and insight.

By identifying weak points we can better help our insured prepare for risk events.

For example, through partner companies such as K2, we can help clients better understand cyber risks at the time of important M&A transactions.

We can also offer help with vulnerabilities that can arise via their staff by providing ongoing employee awareness training and we are constantly evolving our cyber product to reflect our changing world.

If a crisis does happen, it is important to make sure in advance that your insurer can provide access to the kind of 24/7 support and dedicated professional advice that you will need to navigate through the difficult and stressful times ahead as successfully as possible, whether you need help with PR or technical damage limitation.

Above all, remember that this is a global issue and cyber risk has no respect for borders.

Companies need to choose a global insurer that understands the implications this has and that can help firms stay secure in all markets where they operate.

New developments such as the internet of things and autonomous vehicles are blurring the lines and creating new, complex liabilities all the time.

Having access to the right intelligence and advice tailored to your requirements is now not only essential to maintain security, it is a strategically vital force multiplier, a way to differentiate your brands and help drive growth.

A new class of technology

Advances in artificial intelligence, synthetic biology, nanotechnology and robotics promise a new start for the human race – if it learns to understand the risks, that is

IF AN OPEN LETTER BEARING HIS name is anything to go by, Professor Stephen Hawking has mixed views on artificial intelligence (AI).

"The potential benefits are huge," suggested the letter, signed by 150 luminaries and released in January by the Future of Life Institute (which works "to mitigate existential risks facing humanity").

"Everything that civilisation has to offer is a product of human intelligence; we cannot predict what we might achieve when this intelligence is magnified by the tools that AI may provide, but the eradication of war, disease and poverty would be high on anyone's list. Success in creating AI would be the biggest event in human history.

"Unfortunately," added the letter (endorsed by entrepreneur Elon Musk, among others), "it might also be the last, unless we learn how to avoid the risks".

It is human nature to focus on the positive aspects of new technology, but we avoid the potential – perhaps catastrophic – downsides at our peril.

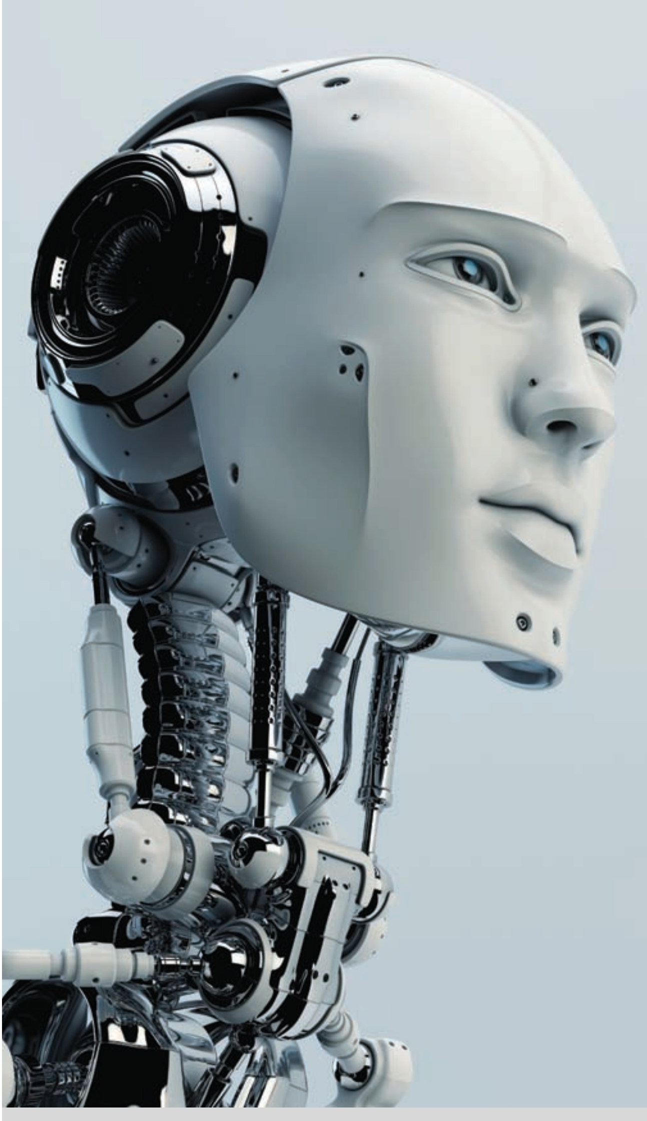
"People should be scared," says Professor Huw Price of Cambridge University's Faculty of Philosophy, one of the three founders of the Centre for the Study of Existential Risk. "As all risk managers know, the allocation of resources into what gets studied is not always logical. As far as we know, these events are not so unlikely to dismiss, and they are not called 'catastrophic' for no reason."

Advanced AI is not the only potential threat on the horizon, as advanced forms of synthetic biology, nanotechnology weaponry, robot warriors and machine superintelligence are all on the verge of becoming a potential reality.

"The great bulk of existential risk in the foreseeable future is anthropogenic – that is, arising from human activity," explains Professor Nick Bostrom, a philosopher at Oxford University's St Cross College and editor of the book *Global Catastrophic Risks*. "In particular, most of the biggest existential risks seem to be linked to potential future technological breakthroughs that may radically expand our ability to manipulate the external world or our own biology. As our powers expand, so will the scale of their potential consequences – intended and unintended, positive and negative."

As an example, Bostrom cites the advanced forms of synthetic biology, nanotechnology weaponry and machine superintelligence that might be developed this century.

"This new class of technology is greatly reducing the number of people it would take to wipe out our species," says Price. "However, because nanotechnology is perhaps not as dramatic as nuclear war, it has not yet received the attention it deserves. Yet, this will be the situation for



a long time; our technology is not going to get less powerful."

However, existential risks have so far barely been studied, perhaps because they are so vast and hard to grasp.

"We therefore know little about how big various risks are, what factors influence the level of risk, how different risks affect one another, how we could most cost-effectively reduce risk or what are the best methodologies for researching existential risk," says Bostrom.

> *'This new class of technology is greatly reducing the number of people it would take to wipe out our species'*
> **Huw Price**, Cambridge University

"We need to be investigating, mitigating and managing these risks," says Price. "We should be developing a serious plan. So far, many of the people concerned about these risks have come from outside science, or from Hollywood, and this has contributed to the sense that the risks are flaky. However, they are a real danger. We need to bring study into the realm of serious analysis. We all live in an environment with long-tail risks, and we all know that sooner or later a long-tail risk will get us. What about when that risk could wipe us all out? That is the reality we face."

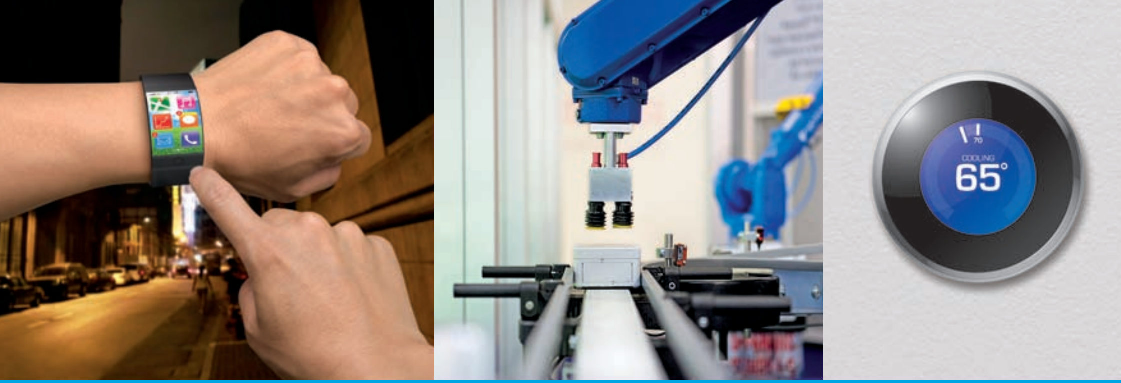
Cause of concern

Risk managers should be concerned about existential risk because they are human begins with moral responsibilities, agrees Bostrom.

"They might have the greatest opportunities to do something helpful with regard to existential risks outside their practice," he says.

For example, risks from future technologies might be studied by means of theoretical modelling to determine their capabilities, what kinds of safeguards are needed and the strategic context in which they might be used.

"We are not trying to say that we can change the world," says Price. "However, what we can do is shift the problem from a predominantly bad to predominantly good outcome. In many ways, this is akin to putting on a seatbelt. It might not be the whole answer, but it is definitely making things better." **SR**


COOLING
65°