FT SPECIAL REPORT

The Connected Business

Wednesday June 1 2016

www.ft.com/reports | @ftreports

Cyber villains pose greater risks to smaller companies

Experts say many businesses not properly insured against security breaches, writes *Oliver Ralph*

An attack can seem very innocent at first. It can look exactly like an email from the chief executive or a message from a supplier or a bank. But links in malicious messages can set off a devastating sequence of events that could lead to data loss, unwanted encryption of systems and ransom demands, or damage to property if connected infrastructure control systems are hijacked.

For large companies, cyber attacks can be an unwelcome distraction that takes a while to sort out. For small and medium-sized businesses, the impact can be far more serious. "Large companies appreciate the risks quicker but small companies face even more severe risks," says Stephen Ridley, head of UK cyber business at insurer Hiscox. "Even a small breach could be curtains for them. Something mundane could turn out to be incredibly problematic."

The problem for smaller companies is attacks are becoming more common. According to a UK government report published in May, a third of small businesses has had a cyber breach over the past 12 months. For medium-sized businesses, that figure rises to just over half.

It is no surprise, then, that the insurance industry sees cyber attacks as a business opportunity.

The cyber insurance market for large businesses is already well developed but providing cover for small businesses is currently much less widespread.

Mark Camillo, cyber leader at insurer AIG, estimates that less than 2 per cent of businesses in Europe have some sort of cyber insurance. "Small companies don't think they're going to be targeted with this sort of attack," he says, "so it is a surprise when they are hit." In the US, cyber insurance is well established. Laws require companies to report to both regulators and affected customers when information has been stolen, and insurance covers them for the costs of making these reports.

Illustration — Øivind Hovland

Jamie Bouloux, a cyber expert at insurer Ryan Specialty Group, says: "Notification charges can be huge in the US, and there is also the potential for class action lawsuits."

An EU data protection regulation, due to come into force in 2018, will impose similar requirements on European companies. This is expected to spur a much wider take up of cyber insurance.

"There are obligations to report data breaches to regulators and individuals in some circumstances and, where this needs to be done, the timescales are short," says John Benjamin, partner at law firm DWF.

'Small companies don't think they're going to be targeted, so it is a surprise when they are hit'

He says the EU regulation will result in a much higher standard of privacy protection than that provided by US legislation, where the rights of the individual are not as well protected.

Mr Benjamin adds: "Potential fines will be a lot higher than those provided under current law. They will be similar to antitrust-style penalties, which are based on global turnover."

Cyber insurance can cover business interruption, damage that hackers cause to IT systems, extortion (where a ransom is demanded, with payment often required in the digital currency bitcoin) and the costs of dealing with

Continued on page 2

Inside

Eric, Asimov and me: or how to stop worrying and love robots

OPINION

Adam Jezard

I first became aware of Eric about 20 years ago when my disabled uncle — seeking to divert himself from permanent discomfort — sent me an email with a picture of a metal man, something like a knight from the days of yore, with the letters R.U.R. on his chest. Uncle asked if I knew what it was.

While Eric was new to me, R.U.R. was not. As a student of early 20th-century drama, I had in my teens come across *R.U.R.* (Rossum's Universal Robots) — the play by Czech writer Karel Capek for which the word "robot" was coined to describe man-made, subservient artificially intelligent beings. What surprised me then — and ever since — is that most people, many of whom know far more than I about robots, have never heard of the play or realised that the word did not exist before 1920. In the play — spoiler alert — humanity is wiped out by robots who then seek to develop emotions and become the new humanity.

Eric, it seems, was nothing to do with *R.U.R.* but an automaton who could seemingly answer questions put by his creators. It was of course a stage trick rather than an early example of AI.

I always assumed Eric had been built by mountebanks trying to cash in on *R.U.R.*'s success, although it seems he was made to publicise a mechanical engineering show. He was an overnight hit and went on a world tour in 1928 but suddenly vanished. His metallic remains have never been found.

R.U.R. was also a worldwide success. It appeared on US radio in the 1930s and the BBC televised it in 1938, but like Eric it too has been largely forgotten.

My uncle died last year and, while clearing out his stuff, I came across a first US edition of Capek's play I had given him one birthday. This contained photos of a 1920s' stage production that reminded me of Eric, but otherwise I had forgotten the robot completely.

I, Eric: a rebuild of the robot is planned

So I was surprised while on my way home from work one night in May, to find a feature about Eric in London's Evening Standard newspaper. The London Science Museum is planning a big exhibition about robots in 2017 and has opened a Kickstarter crowdfunding campaign to raise £35,000 to rebuild Eric. As I write, it has had pledges of £13,000.

Science-fiction author Isaac Asimov, considered an authority on robots, began writing about them when *R.U.R.* was still well known. He said there were three kinds of robotic tale: robot as menace, robot as pathos and — his own take — tales of "industrial products built by matter-of-fact engineers". *R.U.R.*, the parent of all robotic fiction, is all three, and its prediction of mass-produced human-like machines that do our work seems stunningly prescient.

While one cannot use fiction to predict the future, I have been reading Asimov to try and gain some philosophical insight into how we might respond to robots: as a species, as individuals, as employees and workers. *R.U.R.* has merits but is a stilted, stiff drama by modern standards and its dystopian view has influenced other, better-remembered works, such as Fritz Lang's 1927 film *Metropolis*, that present a dim view of robots and AI.

Asimov's tales waver between menace and pathos perhaps more than he would have liked to admit. In the background there often is the US Robots and Mechanical Men, Inc, churning out machines to perform tasks from being companions to mining or visiting threatening aliens. This gives his stories a base in something like real capitalism, if you do not look closely.

As well as automated cars, Asimov, who died in 1992, predicted robots that could write and edit, and computers that get bored running big organisations and mess their human operators around for light relief (the daily computer crash explained). He also devised the three laws of robotics:

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2. A robot must obey orders given it by human beings except where such orders would conflict with the First Law.
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

The apparent common sense of having some laws governing our future AI-equipped helpmates gives one the hope that, at some point, global policymakers might consider what the dawn of the robots really means for us.

I do not get the feeling from Asimov's tales that robotics is good or bad. It just is. Some characters manipulate robots, others are afraid of them, some robots go wrong. But the future he envisages in the stories I have read so far seems more hopeful than the *crepuscule* of *R.U.R.* If a rebuilt Eric is ever able to answer for himself, I can only hope he will agree.

Olympic data help decide victors in race for 2020 funds

Sport Speedier decision making will boost the possibility of medal success, reports *Jane Bird*

The world-beating performance of medallists at the Rio Olympic Games this summer will probably be matched by the speed at which Team GB's performance levels will be displayed on computer screens at the UK's sport-funding body.

The data will help UK Sport determine the funding British athletes will be receive for Tokyo in 2020 — and possibly even for Olympic Games further in the future. The body hopes speedier decisions about funding will boost the possibility of athletes' success because training for the next games begins just a few days after they take the podium.

Time waits for no one in world-class competitions, says Simon Timson, director of performance at UK Sport. "The quicker and more accurately we can make our decisions and get the right support to the right athlete and the right sports, the greater our competitive advantage," he says.

UK Sport agrees individual medal targets with 38 Olympic and Paralympic sports plus an aggregate target with the government as the basis for investment.

"Three years ago, we'd often sit in reviews of sport and investment meetings and ask what potential a group of athletes really had," says Mr Timson. "We'd have to take the sport's word for it and we'd have some doubts. Track records would be patchy and often the likelihood of successful performances looked marginal, so we would have to err on the side of caution."

In 2014, UK Sport's intelligence team began working in partnership with Quebec-based CGI to create a portal to analyse and report on a wide range of data that can inform its decision making for the 2020 Tokyo Olympics.

The techniques that are being used include logistic regression — a method of predicting outcomes based on several variables — to analyse previous and current performance data of UK athletes. This is combined with data, such as the performances of other world-class competitors in big sporting events and the normal swing in the number of medals from event to event on a sport-by-sport basis for each nation.

The software lets UK Sport look at failure and success rates for athletes who are, or were, on its "podium programme" of potential medal winners. Mr Timson says: "It gives us a lens to look into how ambitious and realistic the proposed target range for Tokyo might be. So we can understand whether we should be investing in fewer or more athletes."

Previously, such calculations would have been too complex, says Mr Timson. "The analysts had to spend most of their time collecting, 'cleaning' and ordering the data. So they had less information and were able to perform fewer analyses.

"We now have a much clearer understanding of each athlete and each sport's medal potential, which is crucial when you're making four to eight-year investment decisions."

The software allows UK Sport to focus on potential implications of their decisions. "And it enables us to put the facts and evidence on the table for individual sports," Mr Timson says.

"A sport might claim a particular athlete could win a medal for a specific event in 2020, or even in 2024, and we can see from the analysis that to have a 40 per cent chance of achieving this the athlete would need to be 10th in the world," says Mr Timson.

"If the athlete is outside that range, it would take something pretty special to convince us that this is a worthwhile investment."

Data are also fed into a forecasting algorithm for the Rio games that simulates Team GB's performance 250,000 times to understand the range of potential outcomes and predict the most likely number of medals it will win — which currently is 53.

"It has changed the dynamic and the nature of conversations we have with sports," says Mr Timson. "We can be prudent, targeted and precise now in where we place our investments. It takes out much of the uncertainty and risk in our decision making, enabling us to make the most precise and best use of the £500m National Lottery and government funds we receive [for 2013-17]."

The first phase of the project, now complete, was the automation of data collection but high-volume analyses still takes two to three weeks.

Phase two will be live analysis of the Rio results as they come in for each event, plotting athletes' trajectories towards the podium in 2020.

Carl Statham, director of digital transformation at CGI, says other countries are investing in similar software, including the US, the Netherlands, Brazil, Australia and New Zealand and the winning nations will be those which use it most effectively. "Sport has been slower than sectors such as finance to deploy analysis, but the UK is ahead — other countries have not put so much thought into it," he says.

On track: analytics allows study of athletes such as Sir Chris Hoy — Charlie Bibby

Cyber villains pose greater risk to small companies

Continued from page 1

any legal or regulatory investigations. It will not, however, cover the costs of fines and penalties. The EU rules allow fines of up to 4 per cent of global annual turnover in the event of a breach.

For the insurers, helping clients to deal with the practical consequences of a breach, rather than simply sending a cheque to pay a claim, is a big selling point. "The most important part of the cover is the claim response and the direct access to service providers. A big part of it is the crisis management piece," says Mr Ridley, of Hiscox. Services provided by insurers can include IT forensics specialists, who can work out exactly what has happened, legal advice and public relations consultants, who can help the company to send out the right message to its customers.

Some policies are also preventive. "A lot of cyber policies now include loss prevention to help a small business stop getting hacked in the first place," says Mr Camillo.

"That can include devices which are updated every 10 minutes with information on the latest hacking groups."

It can also include training to help businesses better understand the risks.

Prices, according to Mr Camillo, can start at about £50 for £25,000 of cover and then rise from there. He says that costs for bigger policies, which can provide £5m or more of cover, vary from 0.5 per cent of the sum insured to 2 per cent, depending on the exact type of insurance bought.

The price can also vary by industry. "A credit card processor or a health facility with access to sensitive medical data would pay more than a company without access to these records, such as a manufacturer," says Mr Camillo.

Nevertheless, a lot of small businesses choose to operate without standalone cyber insurance. That is partly because some elements of cover are already provided in existing policies. Property, professional indemnity or kidnap and ransom policies sometimes provide cyber cover, or at least do not specifically exclude cyber attacks in their policies.

Insurers believe there is plenty of potential to increase the take-up of cyber insurance policies. "The standalone cyber insurance market for SMEs hasn't quite picked up as we might have expected," says Mr Bouloux of Ryan Specialty. "Lots of companies aren't aware that the product exists or aren't aware that they could be a target. But awareness is growing.

"There is a lot more publicity around the fact that small companies can be a target due to a lack of training, a lack of security management, small IT budgets or the use of older operating systems."

Cyber insurance What to look for in a policy

The Association of British Insurers has produced a guide for SMEs thinking of buying cyber insurance. It highlights six things that SMEs should look out for in their cover:

1 Loss of income caused by a cyber attack.
2 Costs associated with privacy breaches. This can include the costs of notifying customers and any legal costs that arise.
3 Cyber extortion demands.
4 Protection against loss or damage to data.
5 Legal claims relating to the company's digital media presence.
6 Forensic support from IT specialists after a breach.

Contributors

Oliver Ralph
Insurance correspondent

Emma Dunkley
Retail banking Correspondent

Kana Inagaki
Tokyo correspondent

Maija Palmer
Social media editor, Special Reports

Robin Wigglesworth
US markets editor

Jane Bird
Sarah Murray
Jessica Twentyman
Freelance technology writers

Adam Jezard
Commissioning editor

All editorial content in this report is produced by the FT. Our advertisers have no influence over or prior sight of articles.

Follow us on Twitter @ftreports

Dash to turn alternative batteries into saleable goods

Power supplies

Kana Inagaki examines the technologies being developed into products that will cost less and last longer

The race is on to develop next-generation batteries. Since the 1990s, when Sony commercialised lithium-ion batteries, advances in energy storage technology have been incremental and the battery life of mobile devices and electric vehicles has been limited as a result.

Breakthroughs have been made in labs but concerns about durability, safety and costs have stopped companies using non-traditional batteries. Analysts say, however, that new batteries could enter the market by 2020, claims underscored with investments by companies such as Dyson and Bosch.

None of this is necessarily revolutionary, says Kiyoshi Kanamura, a batteries expert at Tokyo Metropolitan University, as it is mostly based on existing research. "But," he says, "advances in chemical technology and the emergence of new electrode materials have now brought these batteries within reach."

Franco Gonzalez, a senior technology analyst at research firm IDTechEx, says: "Start-ups in new battery technology need to diversify into emerging niche segments in addition to trying to penetrate the traditional segments such as consumer electronics and cars."

His company estimates that advanced and post-lithium-ion battery technologies will achieve a market value of $14bn in 2026, comprising about 10 per cent of the entire battery market.

There is a wide range of alternative technologies under consideration that aim to cut the cost of electric vehicles and make gadgets last longer. The winner of the race will probably be the company that can safely apply the new technology in products at attractive prices.

Solid-state batteries This technology replaces flammable liquid electrolytes used in most traditional lithium-ion batteries, making it safer in different environments. These batteries have greater energy density, so they last longer, are more compact and weigh less. They are easier to package in medical and consumer devices and vehicles.

Dyson, the vacuum cleaner maker, last year bought Sakti3, a solid-state battery business, for $90m, while Bosch of Germany acquired Seeo, a Californian developer of polymer solid-state batteries for electric vehicles and power grids.

Researchers at Toyota and Tokyo Institute of Technology said in March they had developed solid-state batteries with more than three times the storage capacity of lithium-ion state batteries.

Hitachi Zosen of Japan says it plans to commercialise the technology by 2020, but acknowledges it has yet to work out the manufacturing process.

Sodium-ion batteries Since sodium is more widely available than lithium, the battery is less vulnerable to price volatility and to geopolitical tensions causing supply disruptions. It is also cheaper and thought to be safer.

Battery start-ups, including UK-based Faradion and BroadBit of Slovakia, claim to have developed sodium-ion batteries that match or exceed the energy density of lithium-ion batteries. Generally researchers say sodium-ion batteries still lag behind their lithium-based cousins in energy density and cycle life (how many times they can be recharged). Sodium is heavier than lithium, so is more suited to grid storage than consumer electronics.

"It is possible to commercialise sodium-ion batteries but whether it will become a profitable business that outperforms lithium-ion batteries is a different matter," says Shinichi Komaba, a professor at Tokyo University of Science working on the technology. "A battery without a track record always holds the risk of uncertainty in actual use."

Lithium-air batteries Many companies, including Toyota and BMW, are investing in lithium-air battery research because they have a potential for energy storage that could greatly extend the range of electric vehicles. They cost and weigh less than lithium-ion cells.

Researchers at Cambridge university last year said they had developed lithium-air batteries that pack five times more energy into a given space than today's best batteries and can be recharged 2,000 times. But the technology has practical drawbacks such as chemical instability that leads to a rapid fall in performance. While the scientists claim to have overcome some problems, they say it will take another decade before they can be used commercially in cars and grid storage. Researchers at Toyota have also said the technology will not be viable before the mid-2020s.

Sulphur-based batteries Lithium-sulphur is a closely watched technology that can also be used for military and aerospace applications. The batteries' energy density is at least twice that of current lithium-ion batteries.

Oxis Energy, an Oxfordshire-based company that has a patent for lithium-sulphur batteries, says it has achieved a theoretical energy density five times greater than lithium-ion. It is working with Seat, the Spanish car brand owned by Volkswagen. Nasa, the US space agency, has invested in lithium-sulphur batteries for exploration missions.

For the technology to move from experiment to commercial product it will need to achieve longer life cycles. Mr Gonzalez at IDTechEx adds that start-ups must be able to produce the same-quality batteries in large volumes.

Markets There are worries that increasing automation may simply replace human stupidity with robotic stupidity, reports *Robin Wigglesworth*

Algorithms bring benefits but fears of accidents grow

We are all 'algos' now: traders at work in the New York Stock Exchange in May
Michael Nagle/Bloomberg

When Bruce Bittles first started trading in the 1960s, the US stock market was a largely human affair. Exchange floors were the chaotic maelstrom of shouts, frantic phone calls and finger waving, later made famous by 1980s films such as *Wall Street* and *Trading Places*. But now the machines have taken over.

Nasdaq became the world's first electronic stock market when it opened its doors in 1971, but since then, the trading world has been revolutionised several times over. The old bourses and trading pits now are largely shuttered. Virtually all stock trades are done electronically in data centres.

The rise of modern electronic markets has also led to the birth of a new breed of traders: algorithms that either execute transactions on behalf of investors, scan markets for profitable opportunities or even buy and sell securities systematically — and largely autonomously from human control.

This is a development that has been under way for several decades but trading "algos" have grown increasingly complex, sophisticated and fast in recent years, sometimes even using artificial intelligence techniques to reach their decisions and help them adapt dynamically to shifting market conditions.

While this has hammered down trading costs to nearly zero, enabled the rise of popular vehicles such as exchange traded funds (ETFs) and allowed asset managers to deploy increasingly sophisticated strategies, it also means that markets can sometimes move in mysterious ways that can befuddle and frustrate human traders and investors.

"For much of my career, I had a pretty good idea of what would happen the next day. That's no longer true," laments Mr Bittles, now chief investment strategist at Baird, a wealth management firm.

Trading algorithms come in many shapes, from the deceptively simple to the staggeringly complex, and are used in many ways. But the advantages are clear. Trading has never been easier and costs never lower thanks to human intermediaries being rendered obsolete.

Algorithms have also nurtured developments such as exchange traded funds, which have revolutionised the industry and brought advantages to millions of ordinary investors.

In addition, the US stock market bid-ask spreads — the difference between the price for selling and buying a security and a handy gauge of transaction costs — have collapsed by 95 per cent since 1994, the Managed Funds Association noted in a report on algorithmic trading last year. "Over the last five decades, technology and automation have brought significant benefits to investors, including greater accessibility, lower transaction costs and fairer markets," the association argued.

These days, virtually every money manager, broker or day trader uses algorithms in some form. Most of the bond market remains the domain of human traders, but algorithmic trading has become increasingly important in the trading of US Treasuries, too. Indeed, algos have rendered human traders obsolete in many areas.

"I think the most obvious advantage of algorithmic trading is the reduced cost and scalability," says Christina Qi, who works at Domeyard, a high-frequency trader.

"Some people think that your execution costs will magically go down if you are faster," she adds. "What I mean is that hiring a trader costs a lot and, more importantly, adds very little value. You can back this up with data. We've seen many companies replace traditional traders with computers."

'Hiring a trader costs a lot and, more importantly, adds very little value'

But as a result, the stock market has grown increasingly complex and often confusing, with millions of algos sparring for advantages in the electronic markets of today. This may be leading to negative side effects.

For example, to counter HFT firms that have largely supplanted the old "market makers" of Nasdaq and the New York Stock Exchange's "specialists" — dedicated intermediaries that facilitate trading — and to avoid moving markets too severely, many asset managers splice and dice big buy and sell orders into smaller bites and drip them into markets at random intervals.

"In the old days we could do 'big tickets', but we have to be much more careful these days," says Patrik Safvenblad, chief investment officer at Harmonic Capital Partners, a hedge fund.

"Technology is both helping and hurting us. It means we can seep out orders more gradually, but because everyone does it the liquidity suffers."

Despite assiduous risk management controls, things can go wrong. Most memorably, a poorly executed automated sell order by a big US asset manager triggered the 2010 "flash crash", and in 2012, Knight Capital, a high-frequency trading firm, imploded after an errant algo lost it about $440m in a 30-45-minute trading frenzy.

"Sometimes all computers do is replace human stupidity with machine stupidity. And, thanks to speed and pre-programmed conviction, machine stupidity can devour markets far faster than any human panic can achieve," Gavekal, a brokerage, noted at the time.

The market ripples and waves caused by automated investment flows can also frustrate investors. Nevsky Capital, a London-based hedge fund, earlier this year closed down in part because the "current algorithmically-driven market environment is one which is increasingly incompatible with our fundamental, research-oriented investment process".

In its final letter to investors, Nevsky wrote: "Butterflies flapping their wings now regularly create hurricanes that [hurt] fundamentally driven investors who cannot remain solvent longer than the market can remain irrational."

Even some of the proselytes of the revolutionary benefits of technology fret that this complexity makes modern markets vulnerable to glitches that can have devastating impacts at high speed.

The benefits are real, but so too are the risks.

Banks turn to software to ease regulatory stress

Financial services

Panama Papers highlight need for companies to hold and retrieve accurate data, reports *Emma Dunkley*

Revelations about offshore accounts around the world, designed to shelter billions of dollars from tax, have thrust financial regulation into the spotlight.

At the heart of the Panama Papers were banks and financial services firms that had hatched thousands of shell companies in murky territories for clients, as revealed in files leaked from law firm Mossack Fonseca.

The debacle exposed how legal corporate structures were abused to enable money laundering and tax evasion in some instances. It highlighted a big challenge for banks: the need to tighten checks, controls and more effectively police customer data.

Experts believe banks will increasingly turn to external technology providers to help them comply with a mounting regulatory burden.

Financial services providers are under pressure to stop abuse and comply with a stream of regulations that vary across jurisdictions. These range from anti-money laundering rules to country-specific regulation such as ringfencing in the UK, which requires banking groups to hive off their retail arms from riskier divisions by 2019.

Most recent reforms have come in response to the 2008 financial crisis. In the UK, the bank levy was created in 2011 to make banks contribute to economic recovery. The Dodd-Frank act in the US aimed to lower risk in the financial system with measures including a requirement for banks to have contingency plans for a quick and orderly closure.

"There are huge regulatory costs and overheads, which are something of an issue for banks," says Cliff Moyce, global head of finance practice at technology consultancy DataArt. "Banks are using screening software, plugging in extra IT tools to core systems to pick up any activity that might not be compliant . . . you don't want to screen everything but you don't want to miss anything."

In the UK, more than 80 per cent of banks' technology budgets for the past five years have been spent on addressing regulatory requirements, mitigating litigation and streamlining, according to estimates from consultants KPMG.

In 2013, the Basel Committee released its principles for risk-data aggregation and reporting after it found banks had been unable to efficiently quantify their exposure to the collapsed Lehman Brothers. In the US, the Office of the Comptroller of the Currency issued "heightened expectations" to enhance the risk management practices of large national banks — including a focus on data and reporting.

The Panama Papers leaks highlighted the need for banks to have strong "know your customer" checks in place and the ability to find information quickly for regulators. The UK's Financial Conduct Authority gave banks about a week for urgent reviews looking into whether they were linked to Mossack Fonseca.

'Banks don't want to have 10 different sets of regulation technology'

Plugging in third-party technology requires banks and financial services companies to have sufficient customer data, without which the software cannot screen for anomalies or areas that do not comply with regulations. Any instances of insufficient data would require reinputting client information, wasting time and resources, says Joe Cassidy, partner at KPMG. For example, documents such as passports must be scanned, kept in a database and be easily retrievable. But third-party software adds to costs for banks already suffering from lower profits and fines for behaviour such as mis-selling mortgage-backed securities and rate rigging. And their systems can be old and complex.

Voice alert: software can monitor conversations in trading rooms

Bruce Laing, partner at consultancy Deloitte, says: "There are lots of regulations in many different jurisdictions, but a lot of the technology only focuses on one problem. Banks don't want to have 10 different sets of regulation technology." He says some technology vendors are writing artificial intelligence programs that aim to create a single compliance software.

Increasingly sophisticated programmes are being developed. One type used by various banks, especially those with trading divisions, is voice surveillance. Some consultancies have developed a technology that can capture voices across the trading floor, take recordings and match conversations against lexicons to highlight anomalous words or patterns. This can send an alert to prompt human intervention. This process means that someone is not burdened with listening to all conversations.

Scott Weber, managing director of cyber-risk specialist Stroz Friedberg, says: "Communications can show increased levels of stress and disgruntlement and could highlight the potential for someone to do something risky."

As the Panama Papers affair has shown, businesses need strong customer checks and clear processes for using data. Technological developments offer banks and finance companies more tools to comply with an increasing number of rules.

Lords of WiFi hotspots beware: you may be leaking valuable data

ON TECH

Maija Palmer

I recently noticed a bunch of *The Lord of the Rings* buffs. They were not dressed in wizard cloaks or sporting fan T-shirts. There was nothing obvious, outwardly, to identify them, but I knew I was in the company of Middle Earth aficionados because of the names that popped up on my laptop's list of nearby mobile WiFi "hotspot" connections, which you can switch on and off in your smartphone settings. Gandalf, Frodo, Legolas, Boromir . . . and someone in that airport lounge even had a phone whose WiFi was renamed as "Treebeard".

It is one of the geekier forms of modern communication — playing with the name of your wireless internet connection. Most people call their phone WiFi hotspot something mundane like "my iPhone". A few use it to make a statement.

The BBC identified this as a trend among home WiFi users. People were changing the names of their home internet routers to send passive-aggressive messages to their neighbours: "Go away and don't steal my broadband" or "Stop slamming the door!". It is the electronic equivalent of leaving an anonymous sticky note.

Pranksters can use it to give their hotspots names like "FBI Surveillance Van" or "NSA Mobile Wiretap Unit 034" to make people nearby jump. A Qantas flight was grounded earlier this year when a passenger noticed that one of the WiFi networks available on the aircraft was named "Mobile detonation device". Frightened, she showed the message to the crew. Around 40 passengers were so unsettled that they had to be let off the flight with their luggage, leading to a two-hour delay.

It was a poor joke to make at an airport. But there is a serious side to this. The people who play with WiFi names are at least aware their phones are broadcasting information in a multitude of ways. Most people are not. Most mornings on the train, my tablet picks up WiFi networks displaying several people's full names. I could virtually take a roll-call in the carriage based on these. Are they aware they are wearing invisible, electronic name tags? Probably not. I am thinking about you, Sam Piggott in carriage four.

And this is just the tip of the iceberg as far as the information your mobile phone gives out. Phones are packed with accelerometers, gyroscopes and sensors to detect speech, light levels and whether the phone is on your desk or in your pocket. People will routinely give apps permission to gather data from these without too many checks on how the data might be used, stored or protected. Even if you are vigilant and switch off all tracking permissions, there are many different ways a phone can be traced.

Karsten Nohl, a German security researcher, recently demonstrated on CBS's 60 Minutes TV show that he could hack a helpful US congressman's phone, track his movements, listen to calls and read his texts, simply by knowing his mobile phone number.

Researchers at Stanford University and an Israeli defence research company last year showed that it is possible to map a mobile phone user's movements simply by tracking the handset's power consumption. The technique uses the fact that a cell phone uses more or less power for transmissions depending on how far it is from a base station and whether there are obstacles such as mountains or buildings in the way.

The UK government's Communications-Electronics Security Group gives sobering advice to British officials about phones:

- "Even when turned off, mobile devices are never truly off. It is possible for attackers to remotely turn on the microphone and record conversations. Consider not taking your device into buildings or rooms where sensitive discussions are being held."
- "In high threat countries, we recommend 'single use' mobiles for personal use to contact family whilst you're overseas. These should not be used to contact associates or colleagues, or be used for personal communication in the UK. These mobiles will not be any less vulnerable to intercept, but will not contain stored personal or business information which might be exploited by a foreign intelligence service."

Many people might shrug at this. Most of us are not spies or negotiating top-secret deals. We have come to expect nothing to be secure and feel there is little we can do about it.

But could things be different? Should we be asking device manufacturers to do more to protect our privacy? Apple was prepared to defy the FBI in court over an order to unlock the San Bernardino gunman's iPhone. Silicon Valley companies have made a great show of protecting their customers against intrusion. But the same companies are designing products that let users unwittingly haemorrhage personal data right from the outset. They could do better. Consumers should demand better.

@maijapalmer

One web to rule them all: renaming your phone's hotspot is a geek thing

Wearables aim to reduce workplace accidents

Ones to watch The use of devices to safeguard staff is gaining in appeal, says *Jessica Twentyman*

Every day, 6,300 people die around the world in occupational accidents or from work-related disease — more than 2.3m deaths per year, according to the International Labour Organisation. "The human cost of this daily adversity is vast and the economic burden of poor occupational safety and health practices is estimated at 4 per cent of global gross domestic product each year," say ILO researchers.

But for those toiling in hazardous environments — mines, wind turbines or oil rigs, for example — wearable devices could make work safer. Helmets, watches and visors, bristling with sensors and connected via mobile or satellite transmission to supervisors and control centres, can help alert employees to hazards while keeping them focused on the job at hand.

Yet most of the buzz around wearable technologies has been about consumer devices, such as the Apple Watch, Google Glass or Fitbit's wristbands.

"For many of us, when we think of wearable technology, we think in terms of gadgets aimed at the fitness market or techies who want to view text messages and weather forecasts on their watch," says Mark Homer, a vice-president at ServiceMax, a provider of cloud-based apps for technicians and engineers working in outdoor, hazardous environments.

The desire to monitor "field service" staff working in remote and possibly dangerous locations is seen by many as a key driver in the creation of the elusive "killer app" that wearables will require for industries to adopt them.

Take, for example, the UK oil and gas industry. "With a decline in production rates, increasing production costs, a retiring skilled workforce leaving a void of knowledge and expertise among younger colleagues, not to mention a whole host of remote and dangerous working environments, this industry is an ideal candidate for wearable tech," says Mr Homer. Others exploring this potential include utilities and miners, he adds. Although still in its early stages, he says the idea of wearables is gaining ground within companies.

"Wearables in hazardous environments are actually quite real today," says Annette Zimmermann, an analyst with tech research company Gartner. "We're nowhere near blanket adoption yet, but we're seeing cases that go far beyond pilots in several regions."

One device that has caught her eye is the SmartCap, developed by an Australian company of the same name. This looks like a baseball cap, but it contains technology that measures brain activity. Information about how tired workers are can be seen by them on screens and is transmitted to their supervisors. Companies that already use SmartCap include miner Rio Tinto, which aims to prevent accidents by measuring truck drivers' fatigue levels.

Barriers still hinder the wider adoption of health and safety-related wearables. Brent Blum, an expert in wearable technology at consultants Accenture, says device battery life is an issue, as is screen size: "Some tasks are better suited for desktops with large screens, others for wearables with tiny screens."

Businesses will need to expand wireless networks to ensure WiFi connectivity for remote workers, he says, and address employee privacy concerns. "Companies should expand corporate security measures to cover wearables, which can be thought of as mobile devices at the edge, so that they're protected against data leaks," he adds.

Businesses also need to invest in back-end infrastructures capable of processing the information sent by "chatty" wearables for analysis. Wearables themselves are just the "things" in the so-called "internet of things", which connects previously unlinked objects.

Fujitsu, for example, is testing a wearables range including head-mounted displays, wristbands and badges that can detect falls, measure levels of drowsiness and heat exhaustion or simply pinpoint the wearer's location. These use the company's Ubiquitousware package, which converts transmitted data into useful information, according to James Maynard, a director for global internet of things at Fujitsu.

Wearables can keep people safe at work and help them return to their families when their shift ends

Meanwhile, US insurer AIG this year invested an undisclosed sum in Human Condition Safety (HCS), a maker of wearable devices that monitor employees in factories, construction sites and other high-risk workplaces. The company is running a pilot project at Citi Field, the home of the New York Mets baseball team, to simulate conditions at construction sites and large venues and test the wearables it is developing.

Companies and insurers have a hard-nosed commercial interest in adopting technology that reduces the risk of injuries in hazardous locations. But there is also a moral purpose too, argues HCS chief executive Peter Raymond. Wearables, he says, can keep people safe at work "and help them get home safe to their families when their shift ends".

Smartwatch

In May, the Tata Group announced it had doubled its number of published patents over two years, from about 3,500 at the end of 2013 to 7,000 at the end of 2015. Some of these relate to wearables and, in particular, a smartwatch for factory workers. This has a two-way alarm so the wearer can notify or be warned of dangerous situations at the push of a button. It has sensors that monitor health and environmental risks, such as heart rate and the presence of noxious gases. The watches are being piloted by crane operators at Tata Steel in Jamshedpur, India, and the company has identified several thousand of its workers who could benefit from the wearable in future.

Connected Worker

Honeywell Industrial Safety is working with semiconductor producer Intel to make wearables and has demonstrated its Connected Worker product range. Data from a self-contained breathing apparatus, a clip-on heart rate monitor and wrist-worn gesture devices, among others, are displayed remotely on a cloud-based dashboard, so that fire chiefs, for example, can anticipate risky situations and prevent "man down" scenarios among firefighters inside burning buildings.
The relationship with Intel has advanced thinking on internet of things connectivity, device design and data integration, according to Carl Johnson, Honeywell Industrial Safety's president.

Smart Helmet

General Electric's Smart Helmets tackle two problems facing the oil and gas industry: an ageing workforce and customers who demand power outages are fixed faster. The Smart Helmets directly connect field engineers to more experienced colleagues at headquarters, allowing the former to be guided through complex tasks by audio and video. Engineers are equipped with two small monitors on the helmet and an iPad. These enable two-way communications, so HQ can see exactly what the engineer in the field is seeing and share information. GE is developing Smart Helmets with the University of Pisa and prototypes have been tested with staff engineers.

SafeScan

Why ask a novice engineer to practice an unfamiliar task in a hazardous location when you could use virtual reality simulations to train them to deal with its challenges in a comfortable environment? That is the thinking behind Human Condition Safety's SafeScan, described as a fully immersive virtual reality platform. It uses phonemaker HTC's Vive headset as the basis for safety training for high-risk workers in fields such as construction and manufacturing.

The technology was on display during May's Exponential Manufacturing conference, run by Singularity University, the think-tank based in Silicon Valley.

Calamity warning over systems that make the world go round

Risk management

Vital services that rely on the internet could become targets for criminal groups, writes *Sarah Murray*

High tension: risks to technology that controls infrastructure grow — Dreamstime

As far back as the 1897 publication of HG Wells' *The War of the Worlds*, strategic planners, policymakers, and science-fiction writers have tried to predict what might cause a global catastrophe. While epidemics, hunger and nuclear conflict have all been cited, today's interconnected world is now seen by many as posing the biggest risk to our world.

As critical infrastructure — such as power grids, water supplies and transportation systems — is increasingly controlled by digital and web-based technology, could terrorism or natural disasters could disrupt services controlled over the internet on an international scale?

The good news is that destruction of the internet at a global level is highly unlikely. "The internet was built to be incredibly resilient," says Caleb Barlow, a vice-president at IBM Security. He cites the 9/11 attacks in 2001 as an example of the system's strength. Hijacked planes not only destroyed New York's World Trade Center, they also wrecked one of the world's largest switching networks.

"Almost all of it was destroyed, and on a day when internet traffic was at an all-time high," he says. "There were problems but they were very quickly resolved." The reason for this resilience, adds Mr Barlow, is that while individual parts of the system are vulnerable to unexpected events, the way in which internet services are spread between different suppliers, providers and operating systems makes it hard to destroy.

Despite this, risks to the technology controlling individual parts of our connected infrastructure are growing. For example, security experts worry about the damage an electromagnetic pulse (EMP) could cause. This is a short burst of electromagnetic energy that, whether of human origin such as a nuclear explosion, or caused by natural phenomena such as lightning strikes or solar flares, could shut down critical infrastructure and damage electronic equipment.

"Not only does an EMP take out the electrical grid but it also fries the chips in all our devices," warns Marc Goodman, a global security adviser.

Services that rely on the internet are also vulnerable. Take food supply chains, for example. Suppliers, retailers and farmers are increasingly reliant on web-based information systems to manage production, procurement, transportation, delivery and sales. Any online disruption could cause chaos.

"We live in a just-in-time world. It provides a greater degree of efficiency in logistical activity, but if the whole thing falls over, it goes bad very quickly," says Richard Seymour, co-founder of Seymourpowell, a design and innovation company.

In addition to network-wide attacks, cyber criminals could also attempt to exploit vulnerabilities in devices that are wirelessly connected — the so-called internet of things.

John Villasenor, a UCLA professor and an affiliate of Stanford University's Center for International Security and Co-operation, cites the ability of researchers to remotely hack into the controls of a Jeep Cherokee via the vehicle's entertainment system as an example of how cyber crime can affect ordinary people.

'We live in a just-in-time world . . . If it falls over, it goes bad quickly'

"No one intentionally created that vulnerability [in the Jeep]," says Prof Villasenor. "But this is a perfect example of where, in the interest of creating connectivity, people create too much," he says.

Given the commercial opportunities seen in the internet of things — in everything from remotely controlled heating systems to printers that order their own ink — the risks are increasing at a faster rate than policymakers or security companies can keep up with, according to Alan Brill, a senior managing director at Kroll, a security company.

"Cyber technology seems to be advancing at the speed of light but the laws and regulations covering it tend to move at the speed of congress and parliament," he says. "That gap represents a risk factor."

For Mr Seymour, the fact that physical objects are being connected so quickly and without agreed safety standards could lead to unintended consequences, "some of which could be annoying and some catastrophic".

One only has to substitute the example of the car — hacked though its entertainment system — with that of an aircraft to understand the magnitude of the risks created when previously unconnected systems become linked.

Technology may provide some answers, as data analytics and machine learning could eventually provide better security based on the recognition of individuals' behaviour patterns, so helping to prevent terrorist attacks, for example.

However, Mr Barlow argues that a shift from secrecy to transparency will be needed and companies, intelligence services and governments must start to share information about threats far more openly. "We have to completely change the mentality," he says.