Risk Management

People

Monday November 21 2016

www.ft.com/reports | @ftreports

When the workforce is the weakest link

Staying alert to possible disaster should be a priority for employees, writes *Brian Groom*

A matter of life and death: firefighters and doctors attend a fatal train accident in Germany this year, which has been blamed on human error — AFP

The 21st century has so far been littered with corporate crises, from accounting frauds to fatal explosions, security breaches and mis-selling scandals. Companies are increasingly aware that the way they manage people is often at the root of these crises. To what extent they are learning lessons from them is a more open question.

Wells Fargo, the US bank, was fined $185m in September after thousands of staff, under pressure to hit sales targets, were found to have set up bogus bank accounts, in some cases faking customer details and signatures. The resulting furore prompted chairman and chief executive John Stumpf to resign.

"People risk" issues stretch far beyond banking. Samsung Electronics' exploding Galaxy Note 7 smartphone, for example, looks on the surface to have been caused by a technical fault — defective software or hardware. But critics accuse Samsung of not giving its engineers sufficient testing time or opportunities to provide feedback.

Other reminders of the human risk element include: Mitsubishi Motors' admission that employees inflated fuel efficiency data; Yahoo's two-year failure to spot that it had been subject to the biggest known data breach; and a fatal Bavarian rail crash in which the traffic controller was allegedly playing a game on his mobile phone.

People risk can range from sabotage or fraud to poor training, strategic miscalculations, lax safety rules or simple mistakes such as opening a virus-infected email. One of the biggest risks is a reckless boss who ignores warning voices: arguably, the decision by former UK prime minister David Cameron to call a referendum on EU membership because he was overconfident of winning fits that profile.

The problem multiplies as a business becomes bigger, more complex and more global. "When you have complexity, there is potential for things to spiral out of control in more varied and sometimes more dramatic ways," says Anthony Fitzsimmons, chairman of consultancy Reputability.

Many industries are trying to tackle the problem. The finance sector, for example, has made changes to how it recruits, trains, pays and monitors people. But overall, says Mr Fitzsimmons, "I don't think leaders realise that there are things they have to do and that only they can do in order to get people risk properly tackled."

Research by Cranfield School of Management for Airmic, a UK association of corporate risk managers, has identified five principles needed to achieve resilience: the ability to anticipate problems; adequate resources to respond to changing conditions; a free flow of information up to board level; the capacity to respond quickly to an incident; and willingness to learn from experience.

The airline industry is often cited for good practice in this regard. Although accidents happen, the industry has achieved an enviable safety record by encouraging pilots and others to confess to mistakes and allowing these to be publicised and studied worldwide.

Keith Blacker, consultant and co-author of *People Risk Management*, says that addressing the issue starts at the top — by "making sure you have got the right person leading the organisation and setting the values". He suggests companies could give staff a personalised code of conduct, against which they will be measured. "There's no reason why you can't train people about what the culture entails and what their role is and try to get everybody to maintain a sense of vulnerability . . . to assume that something might go wrong."

Boards often focus on corporate culture, although that can be a slippery concept and takes years to change. Pat McConnell, honorary fellow at Macquarie University's Applied Finance Centre in Australia, points to three levels identified by Edgar Schein, an expert on corporate culture: local, organisation-wide and industry-wide. "The payment protection insurance mis-selling scandal was the result of a culture that pervaded the retail banking environment in the UK," Mr McConnell says. "If it pervades the industry, then individual managers can do very little about it."

A survey by Australian insurer QBE found that only three in 10 businesses felt there was a shared understanding in their organisation of risk management's importance. Deborah O'Riordan, practice leader for risk solutions in QBE'S European operations, says companies need to focus on staff attitudes, using face-to-face meetings to make sure everyone understands they have responsibility for risk management.

She cites instances of law firms that have been subject to fraud in property transactions, in which criminals intercept emails between the firm and clients and insert their own bank details. Occasionally, staff fail to follow the rules on verifying bank details by phone, and so money is siphoned off to a fraudster's account. "The message isn't getting through because it just isn't taken seriously enough," she says.

Companies have put a lot of effort into processes to protect themselves, including enterprise risk management, or ERM, systems and there is a global standard for risk management, ISO 31000. These can give a false sense of security, however, because they do not take full account of the unpredictability of human behaviour. "The only way you are going to manage risk effectively is to use your eyes and ears and get round the organisation," says Mr Blacker.

Sayed Sadjady, who heads human resources consulting for EY in the Americas, has a more optimistic view than many people of the progress being made in tackling risk culture, even if it is still "embryonic": "Certain organisations are beginning to think more about leadership attributes, behaviours and how they translate culture into its various constituents." Risk management, he adds, must be carried out in a way that does not stifle innovation, "because innovation has become critical".

Mr Fitzsimmons, co-author of *Rethinking Reputational Risk*, says leaders must understand the psychological factors that blind people to risks — such as bias towards optimism and overconfidence in their own actions — and recognise that these apply to themselves too. They should set up a system that captures, analyses and widely shares lessons from mistakes, including those made by the most senior leaders. They also need to ensure that bringers of bad news, and those who report mistakes including their own, are welcomed.

He quotes Richard Feynman, the physics Nobel laureate who examined the root causes of Nasa's Challenger rocket disaster: "The first principle is that you must not fool yourself — and you are the easiest person to fool."

Inside

Age of authenticity redraws the rules on public gaffes

Reputation

The substance of what you say matters more than the style with which you say it, writes *Miranda Green*

When Gerald Ratner stood up to speak at an Institute of Directors event in 1991, he was probably anticipating indulgent laughter from his audience of fellow business leaders. Little did he realise that admitting — boasting — that the jewellery and homewares his chain of shops was selling at suspiciously low prices was "total crap" would make his name an eternal byword for commercially disastrous gaffes.

The original and best example of "doing a Ratner" is still jaw-dropping: Mr Ratner, chief executive at the time, went on to quip that earrings for sale at his eponymous stores were "cheaper than an M&S prawn sandwich but probably wouldn't last as long".

The joke was on him when £500m was wiped off the value of the company that his father had nurtured, £1bn was lost in sales and he was fired the next year by the company chairman.

Straining to avoid blunders that can destroy a company and a career, business leaders have relied to varying degrees on the advice of communications experts, who are often drawn from the ranks of former journalists.

Traditional advice is still valuable, say such experts — preparing for interviews, training to be at ease on live broadcasts or under tough questioning and honing the messages you want to project. But the problem for a business leader has changed in this more complex digital age, even if the idea of a figurehead communicating the values and delivering the messages for a company or organisation has survived.

"Audiences are looking for someone who is not papering over the cracks — you have to respect the audience's knowledge," warns George Pascoe-Watson. A former political editor of The Sun newspaper, he works at Portland Communications, a London-based agency.

In an era where trust is easily lost — companies' reputations are potentially undermined daily by disgruntled customers on Twitter, for instance — he argues that "what people want from a leader is authenticity. They need that leader to tell a story that makes sense and feels true."

Many would argue that Mr Ratner's mistake was to speak the truth — classic gaffes are moments when the mask slips. Communications advisers argue, however, that it would be far more difficult today to maintain the type of false personal and company image that he disastrously punctured with his speech.

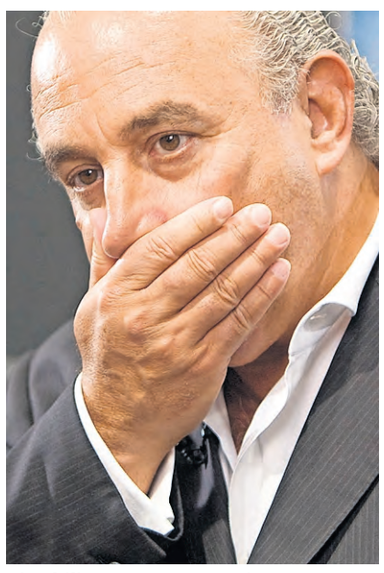
Alastair Campbell, strategy and communications chief to former UK prime minister Tony Blair, and now also working for Portland, alludes to the core of much contemporary advice to leaders on handling media, when he writes on its website: "It is no longer possible, if ever it was, to control what people say and think about you." Instead, he says, "recognise that you can only control what you say and do yourself". If your business or you are trying to hide something, then look out.

Tari Lang, a reputation risk adviser with experience of how business leaders interact with the media in different regions of the world, agrees. In democracies in the late-1990s and early 2000s, she argues, business leaders seemed overconfident that the right advice and personnel could deliver ideal and idealising media coverage. They were taking their cue from the apogee of spin in the political world.

The new prizing of authenticity, however, makes the issue of substance as important to communication as a well-prepared performance on a high-profile television or radio show.

"First, look at the list of things you need to fix," Ms Lang advises. "Then, media strategy needs to be at the end of that process."

Business leaders' nervousness about being questioned by journalists, she believes, is explained by sheer unfamiliarity — with the media perceived as an alien world with different rules — or even an aversion to criticism by powerful individuals that verges on the narcissistic. Leaders should be given the same advice as budding actors, Ms Lang says: do not put too much store by either good or bad reviews.



Sir Philip Green: aggressive behaviour backfired

Mr Pascoe-Watson suggests that ego and force of character can be put to good use if things go wrong: "You can actually make use of a big personality to explain how the problem is going to be fixed."

The emphasis on "keeping it real" has its downsides, however, even without a Ratner-style bout of oversharing, Ms Lang argues.

A chief executive or senior business leader whose behaviour is naturally bullying, abrasive and macho is liable to discover that aggression towards reporters and interviewers that served their purposes on the way up becomes a way of ensuring terrible headlines on the way down. Think of a Sir Philip Green or a Dominic Chappell and the publicity for recent scandals relating to the collapse of BHS.

"They are so used to getting their way in business that they think 'why should I be nicer?'" says Ms Lang. "But the problem with that is that when you fall, people will dance on your grave."

Social media Plan for unexpected outcomes

Using a social media campaign to rehabilitate a corporate image is risky and unpredictable. Like others before it, SeaWorld discovered this to its cost last year when, beset by criticism for its treatment of killer whales, the theme park turned to social media.

The company had failed to think through the risks of not being in control of its #AskSeaWorld campaign, dubbed "You ask, we answer". It soon found itself in at the deep end as Twitter users flooded the hashtag with sarcastic questions and comments concerning animal welfare.

What can be done when a company's social media campaign veers off on an unplanned tack, or a thoughtless post goes viral?

"Social media is no longer 'the thing that the kids do' — it's the new communications medium and businesses need to take it seriously," says Phil Mennie, head of global social media risk and governance at PwC, the professional services firm.

Yet businesses are still mishandling their navigation of the evolving and unforgiving social media landscape.

Experts say the most successful social media plans include input from different areas of expertise such as risk and compliance, as well as marketing.

Companies' social media risks fall into two main categories, says Alexander Larsen, a fellow of the Institute of Risk Management, a global trade body: employees' use of social media and the organisation's own presence on social media.

The former may involve leaks of companies' intellectual property and data by revealing information, or loss of reputation by association if employees express unacceptable views. The latter ranges from unintended posts going viral or social media campaigns taking an unexpected turn, as was the case with SeaWorld.

Victoria Robinson, a chartered marketer and head of communications at the Institute of Risk Management, adds: "Consumers love nothing more than sharing cringeworthy examples of bad practice, making these cases go viral . . . educating staff is essential, from board member to junior staff." Preparing media-management plans in advance to deal with different outcomes will help organisations to avoid incidents and to respond effectively if one does occur, she says.

Justin McCarthy, chairman of the Professional Risk Managers' International Association, adds that a company must be ready to act speedily and decisively after a mistake has occurred.

When KitchenAid's official account posted a tasteless tweet concerning US President Barack Obama's late grandmother in 2012 — meant for an employee's personal account — the brand responded quickly.

As well as deleting the message, which had been seen by many people, a senior executive took to Twitter to apologise and say the individual would no longer be tweeting on behalf of the company.

The KitchenAid incident holds two lessons: respond quickly and firmly to a gaffe; and insist employees keep work accounts away from their personal ones.

Mackenzie Weinger

Rise in threat levels impels need to protect staff

The extra mile: working in remote areas such as in Iraq requires additional attention
Reuters

Hostile regions Keeping safe involves regular contact and thinking ahead, writes *Rhymer Rigby*

Working in risky locations has been more different from working at home in the UK than he expected, says Alan Ryder, chief executive of environmental consultancy RSK. "The higher the perceived threat, the more preparation is required. In some situations, we work with specialist security teams, travel in armour-plated vehicles and wear body armour. In Iraq, we live in a secure camp and we only travel outside the camp accompanied by armed security."

Iraq presents more risk than most postings. But, at a time of increased instability, more organisations are considering threats faced by all employees travelling and working abroad, even in supposedly safe countries.

This year's Global Peace Index report, published by the Institute for Economics and Peace, said levels of peacefulness have continued to decline and that "the two indicators with the largest yearly deterioration were the impact of terrorism and political instability." The report ranks Iceland as the most peaceful and Syria the least. Countries that score "very low" for peace include South Sudan and Iraq; the US is categorised as "medium" and the UK as "high".

Nicholas Innell is a former head of security for the UN's war crimes tribunal in the former Yugoslavia and is now a senior manager in PWC's Enterprise Security team, which advises clients worldwide on safety. At a basic level, he says, companies should assess who is going, where they are going, and exactly what they will be doing. "If you are conducting investigations into fraudulent activity in a company in an unstable country, you are likely to face greater risks than you might if you were handing out food to refugees," he says.

Rob Walker, of consultancy International SOS, says: "The company needs to provide a framework which allows the individual to understand the preparations they should make and the responsibilities they have before going to work in these places." This could range from travel advice to providing a car and driver or close protection. In very high risk places, he notes, plans should include potential evacuation.

Sometimes, however, no more is required than a pragmatic assessment: "After[the shooting at Charlie Hebdo and the Bataclan massacre] in Paris, we reassured some clients that they didn't need to be escorted at great expense."

RSK follows certain protocols, says Mr Ryder. "Whenever we travel away from the office, we . . . let the folk 'back at base' know we have arrived safely. We try to avoid working alone and in remote locations, but if that is unavoidable we make sure we stay in contact with the office by mobile or satellite phone."

Although a violent attack is many people's worst fear, the risks faced by staff are usually more mundane, such as from traffic accidents. Thailand, for instance, while generally considered safe, has the second most dangerous roads in the world after Libya, according to the World Health Organisation.

Countries are not always homogeneously risky. A country may be more dangerous near its borders or during elections. "Some countries, or areas within countries, present unusual or particularly difficult circumstances, which require special planning and procedures by RSK," notes Mr Ryder.

People change too: long-stay staff who experience no problems may become complacent. In fact, says Mr Innell, an employee based in one place for a long time may be more at risk of kidnap because their presence is well known.

Another factor is the psychological toll of working in a higher-risk environment while far from family and friends.

Perhaps predictably, social media has added a layer of risk. A significant online presence could make staff more likely to be targeted by kidnappers by increasing both their visibility and the details of where they are. Or, if someone moves to a country with a different culture, social media posts from years ago could come back to haunt them.

> 'We make sure we stay in contact with the office by mobile or satellite phone'

If a member of staff is involved in an incident — being mugged at a cashpoint, having a hotel room turned over, or a terrorist attack — the company should deal with the after-effects. For the employee this might mean advice or counselling, while the organisation can also learn lessons. "Follow-up can be of huge importance," says Mr Innell.

Overall, Mr Walker says, with the right preparation, staff can be sent to most locations, except de facto or de jure war zones. "There are very few places we say 'Just don't go'."

Vital advice
'Run away — fast'

Somewhere in the rural Herefordshire hills, the man who blindfolded me is now forcing me up from a kneeling position and into an orange jumpsuit.

I have been warned this might happen and I know it is just a training exercise. Nevertheless it is a gut-wrenching moment — a fleeting realisation of just a fraction of the terror that must be felt by those who undergo this in real life.

This is the final day of my hostile environment training. It is a rite of passage for foreign correspondents; one that most accept with a shrug and muttered queries about how much use it is ever going to be.

Those doubts are enhanced following the kidnap exercise: the climax of the five-day course, which gives training in basic first aid, avoiding danger and the importance, above all else, of running away.

What good is it to have been put through this, I ask, if the lesson to take is not to get into such a situation in the first place?

The answer is threefold, and has stuck with me:

First, tiny actions can save lives. If you are taken captive, for example, try not to be carrying a notebook containing the details, phone numbers and locations of all your sources.

Second, do not panic. One of the main reasons for undergoing scenario training like this, the instructor explains, is that the shock is marginally less if it ever happens in real life, allowing you to think and plan more clearly.

Third, and most important, run away. If there is any chance of escape, take it early, before you are exhausted and while your kidnappers are not yet in control.

Kidnap awareness is just one part of the course. Of more immediate practical use is several hours' worth of medical training, which could turn out to be useful at any time, even in otherwise benign situations.

Kiran Stacey

The writer is South Asia correspondent for the FT

Wearable technology Gathering data from tooth to toe

From fitness trackers to sleep monitors, ever more gadgets are on the market to log our waking or slumbering hours. This is the era of the "quantified self", in which the path to self-knowledge comes through wearable technology and the health metrics it can generate.

But the tech is not merely solipsistic: employers, workplace health schemes, and insurance companies have spotted opportunities for gathering more information about our "wellness", too.

They may be taking a cautious approach for now, says Ramon Llamas, analyst at research firm IDC, but they are "trying to figure out how they incorporate these wearables into their strategy".

Fitbit, a market leader in fitness trackers, has partnerships with a number of US health insurers, as well as a "corporate wellness" business that it folded into FitBit Group Health in June.

Chicago-based Vitality Group has teamed up with some big health and insurance industry partners. One scheme, developed with John Hancock Insurance, rewards consumers for using an Apple Watch that sends data to the insurer.

Tal Gilbert, Vitality's US chief executive, says insurance companies will need to take a long view of the benefits and risk reductions that come from having access to customer health data through such devices. "We talk about it as a shared-value model of insurance," he says. Small improvements in health now will have an impact over many years on the policy and on the employee.

Minnesota-based insurer UnitedHealthcare has developed a programme that offers financial incentives to customers who meet specified walking goals, measured by a custom-designed wearable.

Craig Hankins, vice-president of digital products, says the initiative assesses three types of walking: "Employees can earn credits of up to $4 per day based on the frequency, the intensity and the tenacity."

Ohio-based Beam Dental has developed a dental health insurance plan in which clients use a Bluetooth-connected toothbrush. Chief executive Alex Frommeyer says the start-up intended to sell an internet-connected toothbrush as a consumer health product, but soon realised it could marry tech to insurance.

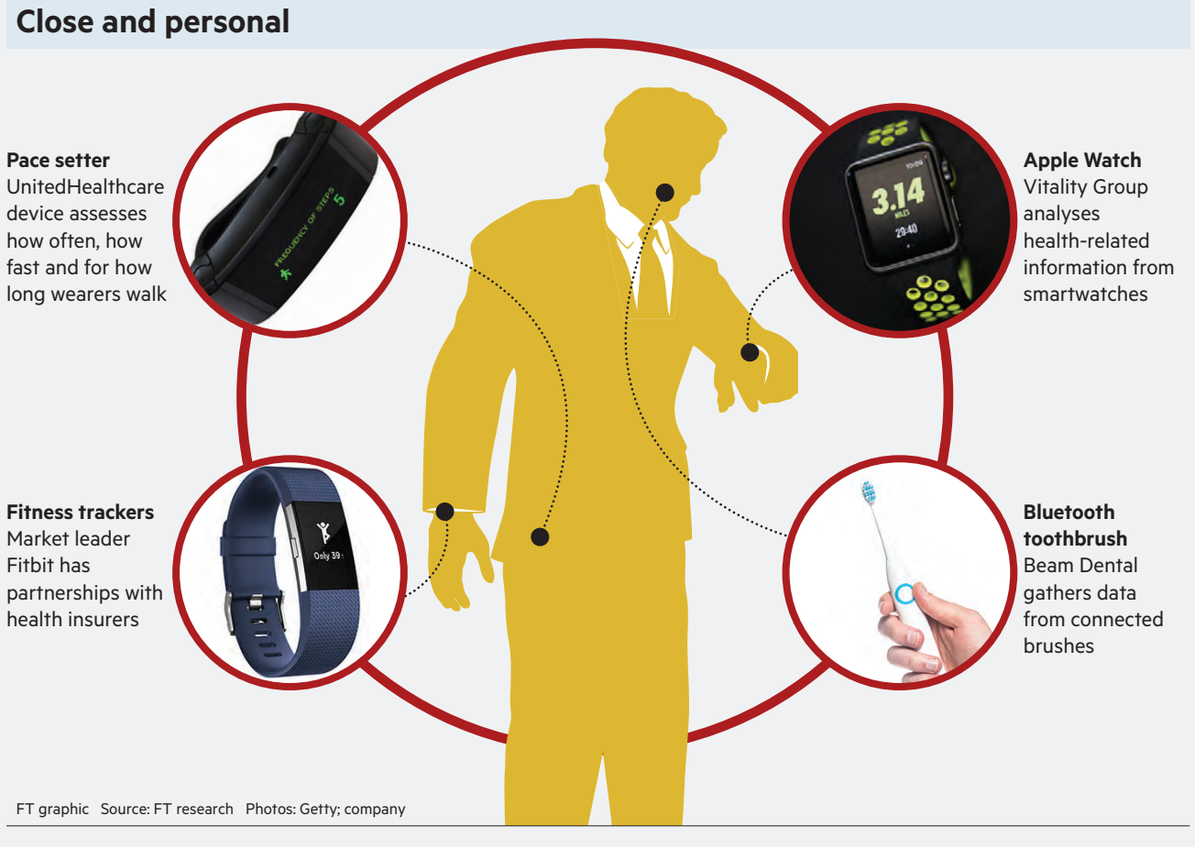
He says Beam is learning how to mitigate its risks and improve dental health for its clients, by using data from the toothbrushes, which are given to people who sign up for the plan.

Some experts predict that workers in critical occupations, such as airline pilots or firefighters, may ultimately be required to allow their employers to monitor their general health and stress levels via wearable technology.

Not everyone will welcome sharing intimate personal information with the boss, however, says Daniel Cooper, privacy partner at London law firm Covington & Burling. "Wearable devices could be a good way for insurers to get the data . . . but it's essential to address wearers' privacy and fair treatment concerns and the risk of discrimination against those who opt out."

Geof Wheelwright

Close and personal



FT graphic Source: FT research Photos: Getty; company

Hackers know to prey on our curiosity, naivety and greed

Cyber security

Digital tricksters understand the psychological traits that make employees their dupes, writes *Hannah Kuchler*

Wendy Tran discovered this year that hackers had filed fraudulent tax returns on her behalf, hoping to pocket a refund.

Her tax data and that of her colleagues at Seagate, the California-based hard drive maker, had been sent to cyber criminals by an HR employee. The HR member of staff, seeing an email request that purported to be from someone authorised to view the data, attached the US W-2 tax forms and sent them off by email.

The device maker's chief financial officer wrote to workers: "This mistake was caused by human error and lack of vigilance, and could have been prevented."

Ms Tran and a number of other colleagues have filed a lawsuit which details their case against Seagate. The company did not respond to a request for comment.

Seagate is one of a growing number of organisations where hackers have launched so-called phishing attacks that trick staff with fake emails, with results that include loss of sensitive data, locking down of computers with malicious software that demands a ransom and even the transfer of funds to criminals' bank accounts.

Many boards are allocating extra funds for cyber security technology but experts warn that humans are the weak point when protecting companies from attack.

Rod Rasmussen, vice-president of cyber security at Infoblox, a US network security company, says there has been a rise in these kinds of attacks — particularly against smaller businesses — because the hackers find that they work.

"Phishing is an online manifestation of an age-old problem. Confidence schemes and other kinds of fraud have been around for centuries — like the Spanish Prisoner," Mr Rasmussen says. He is referring to a 16th century trick to persuade people to send funds, in the hope of a reward, to have a wealthy person released from jail.

> 'You can now literally blast out emails to millions of potential victims'

"With the internet, instead of having to case the victim directly, to physically research them and then send the request by post, you can now literally blast out emails to millions of potential victims," says Mr Rasmussen.

Hackers understand human psychology and play on greed, fear and curiosity. They usually use a company's own website, or recruitment sites such as LinkedIn or Glassdoor, to discover who a target's manager is and send them an email pretending to be from that person.

"It can be something like 'we've seen there's this upcoming conference you might want to check out,' 'this invoice doesn't look right, can you take a look?' or 'can you see what's going on with this bill?'" says Mr Rasmussen, who is a member the Anti-Phishing Working Group, an industry trade group.

The recipient clicks on a link or downloads an attachment and their computer is infected. If the tricksters fool a privileged user, such as an account administrator, they can suddenly speed around the network. Or they may target an accountant with a request that is apparently from a harried chief executive with no time to speak. Eager to please a boss, the employee sends money to an account they think belongs to a supplier.

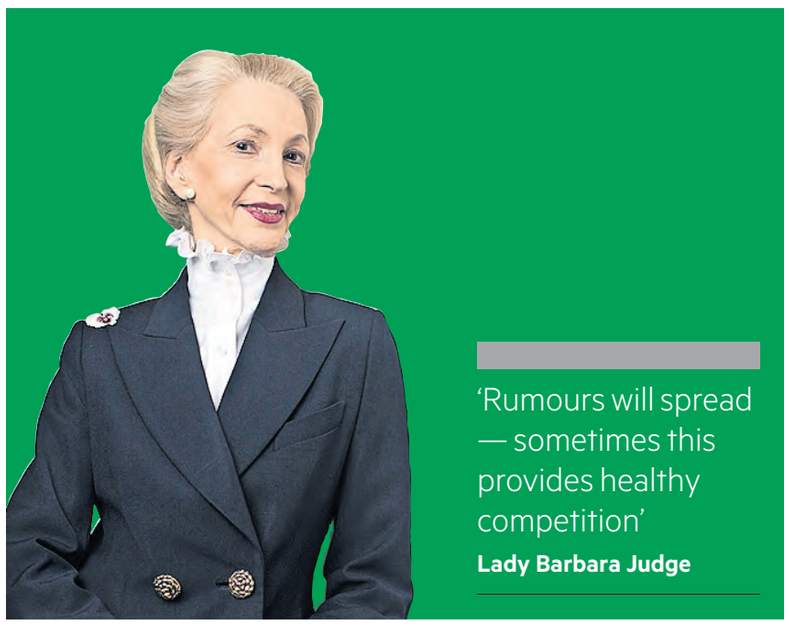
Phishing is the first entry point into a network for many serious cyber attacks, with one in 10 leading to a data breach, according to Verizon's latest annual report on such break-ins. The median time for recipients to open an attachment is less than five minutes after it is sent, says the report.

There are other ways, known as "social engineering", that hackers play on human weakness to gain access to networks. Karl Sigler, threat intelligence manager at cyber security specialist Trustwave, says many people are tempted out of curiosity to plug in USB sticks left lying around in the workplace or even devices that appear to have been sent as presents. "Social engineering is basically when criminals are using psychological tricks to force behaviour on another human being," he says.

Trustwave's penetration testers, who act like hackers to show companies where their vulnerabilities lie, shipped modified keyboards to employees in an organisation, pretending they were rewards. "They are these huge, really decked out keyboards, all back lit, they stand out," he says. Five computers were compromised by three keyboards, suggesting one or two people were "stealing" them from their colleagues, he says, implying that envy or greed as well as pride were at play.

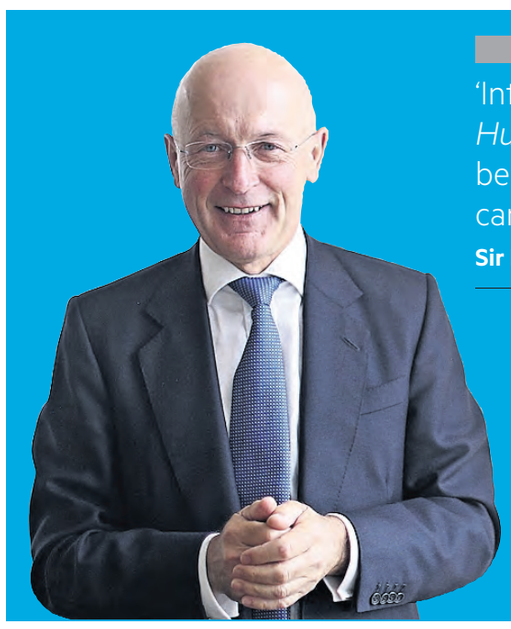
Stu Sjouwerman founded a company, KnowBe4, that trains employees to be more wary of potential cyber crime. One test is to send fake phishing emails to an entire workforce to see how many fall for them. Employees then take an online course to learn what to watch out for, knowing they will be tested with spoof emails in the future.

"The old style security awareness training where once a year you herd everyone in the break room and keep them awake with caffeine and sugar through death by PowerPoint doesn't hack it any more," he says. "Employees need to be trained within an inch of their lives to truly look again before they click."



'Rumours will spread — sometimes this provides healthy competition'

Lady Barbara Judge



'Internal options risk *Hunger Games* behaviour among candidates'

Sir Philip Hampton

'Some talented disappointed candidates will be tempted to leave'

Sir Win Bischoff

Prepare your understudies: views from the top

Key person risk

The stinging effects of a senior departure can be mitigated, business leaders inform *Patrick Jenkins*

Recent speculation over whether Mark Carney's tenure as Bank of England governor would be cut short highlighted the importance of "key person risk", often exemplified at companies where unexpected chief executive departures leave dangerous vacuums.

How should boards prepare for leadership change and balance thoroughness of succession planning with the danger of lining up too many squabbling heirs apparent?

Below is the edited transcript of a debate conducted among the FT City Network, a panel of chairmen and chief executives who are among London's top financiers and business leaders.

Among them is Sir Win Bischoff, the former chairman of Lloyds Bank, who in 2011 had to make an unexpected succession plan, barely six months after his newly appointed chief executive had begun in the job. In the event, António Horta-Osório took two months' medical leave on the grounds of exhaustion and returned to work. Lloyds shareholders again expressed concern about "key man risk" this summer, after tabloid reports of his extramarital affair.

At Royal Bank of Scotland, Sir Philip Hampton oversaw the 2013 ousting of former investment banker Stephen Hester, under pressure from RBS's majority shareholder, the UK government. At BT, Sir Mike Rake was also stripped of his chief executive by the government, when Ian Livingston was made trade minister in 2013.

Sir Win Bischoff
Financial Reporting Council/JPMorgan
A change at the top always presents risks. The best boards plan well ahead to reduce — if not eliminate — those risks by developing internal talent, having a good knowledge of external availability and [weighing] the timing of any change. Some talented disappointed candidates will be tempted by headhunters to leave. That, however, provides great opportunities for those more junior to advance more rapidly.

Sir Philip Hampton
GlaxoSmithKline
There are two key issues. The first is the simple "red bus" moment [when someone is suddenly incapacitated by accident or illness] from an unplanned departure, caused by key people being poached, falling ill or worse. The main thing is to try to have outline agreement within the board on likely timeframes for individuals, so their ambitions can be matched as far as possible with the company's needs. Internal options risk [desperately competitive] *Hunger Games* behaviour among candidates. The best way to address this is for everyone to know that poor behaviour is terminal to chances of progression.

Jean Pierre Mustier
UniCredit
With the median chief executive tenure for the S&P 500 being around six years, time is short to identify, train and test internal candidates. Hence succession planning should be one of the key priorities of a chief executive from his first day in the job, for him to choose in his management team key individuals who could step up into his job over time. At least it was for me. The key issue will be to develop their leadership qualities and emotional intelligence. An external candidate solution [is] always risky.

Ruby McGregor-Smith
Mitie
I took the view as I step down from a chief executive role after a decade that a decade is enough for a chief executive of a listed stock. The board knew this last year so we could start proper planning then. Deadlines work as everyone can work towards them.

Lady Barbara Judge
IoD
Succession planning is one of the most important components of modern corporate governance. Even where there is no expectation that a key person will leave anytime soon, boards should be thinking years ahead as to who would be an appropriate successor. Obviously it would be better to keep the process discreet, but boards understand that rumours will spread. Sometimes this provides healthy competition.

Samir Desai
Funding Circle
Successful teams, in sport, business, politics or elsewhere, are not reliant on a single person. Boards should promote a strong leadership team to protect the business against an executive's departure, particularly in founder-managed businesses, to ensure continuity for customers and employees.

Sir Mike Rake
BT
Having experienced the sudden loss of a chief executive, made a minister by the government, the following is clear: first, it is important to have a medium term development plan for high potential executives. Second, it is essential in parallel to have a plan for unexpected events, differentiating between a holding [and] a permanent appointment. Third, it is wise to have senior members of management below the chief executive level to be given an opportunity for external mentoring/board/ shareholder exposure as this will always benefit individuals as well as the company and gives more choice. Last, it is useful to have an ongoing desk review of potential candidates employed elsewhere.

John McFarlane
Barclays
The principle for senior appointments is to ensure that the best individual in the world available to the organisation should be appointed. Insiders have the benefit of knowledge of the company and therefore have a head start in key requirements. Of course, the merit of outsiders is importing a different perspective and skills. The mission internally is to broaden them earlier in their careers, otherwise they end up as senior specialists. I believe particularly in benchmarking internal talent against global benchmarks, as a check and balance against internal rating bias.

David Roberts
Nationwide
I am a strong believer in rigorous assessment of candidates by chief executive and board, supported by external benchmarking to avoid internal bias. Essential is a very clear understanding that any form of destructive or overly competitive behaviour is a sure fire route to disqualification.

David Morgan
JC Flowers
[Before Jack Welch left, GE made sure it had] at least three internal chief executive succession candidates available when it [became] time for change. Once the decision on the new chief executive is made, the unsuccessful internal succession candidates leave. A united top team, led by a focused, undistracted chief executive, [is] very valuable.

FT City Network
To read the full debate on 'key person risk' and succession planning, go to: ft.com/citynetwork

Contributors

Patrick Jenkins
Financial editor

Kiran Stacey
South Asia correspondent

Brian Groom
Miranda Green
Geof Wheelwright
Rhymer Rigby
Mackenzie Weinger
Freelance journalists

Harriet Arnold
Commissioning editor and assistant editor, Special Reports

Steven Bird
Designer

Michael Crabtree
Picture editor