SPECIAL REPORT

LATEST ON CYBER RISK

insured.™

This report is sponsored by ACE

A new cyber risk landscape

Recognising that cyber crime is changing and set to increase in frequency and sophistication will ultimately help companies deal with its threat

Cyber risk is constantly evolving; attacks are growing in sophistication and frequency. This is evidenced by recent large-scale hacks such as that suffered by UK broadband and telecoms supplier TalkTalk. The new cyber risk landscape has seen also seen an increase of crime from organised criminal gangs are becoming more ambitious.

The key to addressing the risk successfully is appreciating that there are different levels of cyber crimes being committed. Along with the high-profile attacks on large companies, there are small attacks that target individual citizens – all of which pose a serious risk to brand and business.

"Cyber-attacks are becoming far less scatter-gun in approach and are now highly targeted," says Stuart Poole-Robb chief executive at KCS Group.

"Often, months of social engineering, largely internet-based research on a specific target, is used to prepare for a 'spear phishing' attack. Sometimes these use email addresses that are virtually indistinguishable from that of a trusted executive; they may comprise detailed personal information, making the message appear even more genuine.

"Frequently the false communications chain will result in a member of staff divulging security information or making a bank payment to a new account. Sometimes, all the unsuspecting target need do is click on an attachment to open up the entire corporate network to the latest malware, compromising all its confidential data and leaving its financial assets at the disposal of the organised criminal gangs.

> *'It's a very appealing area of criminality and we are seeing more and more criminals getting involved'*
>
> **Vincent Hinderer,** CERT-Lexsi

"Often, these spear phishing attacks take place late on Friday afternoons when staff are often tired and rushing to get away for the weekend."

The overall trend feels like Moore's Law, according to Xavier Verhaeghe vice-president technology solutions EMEA at Oracle. "There is a continuous growth in information and cyber risks, and organisations and individuals try to balance the need for privacy and usability with the overall risk of information theft," he says.

The risk is driven by firms' increasing reliance on technology as they become more aware of the potential of being better connected and making more use of data. As operations become more sophisticated, so too do their vulnerabilities – especially now that hackers are prepared to invest serious time and money in order to succeed.

Many experts believe that over the next few years cyber attacks will increase in number, sophistication and specialisation.

"Essentially, it's a low-risk crime with a low risk of getting caught," says Vincent Hinderer cybercrime expert at CERT-Lexsi.

"It's a very appealing area of criminality and we are seeing more and more criminals getting involved, from teenagers through to older, experienced lawbreakers.

"Criminals are specialising in particular areas and offer their services on a consultancy basis to other criminals and this allows relatively inexperienced criminals access to a high level of expertise," he says.

"For example, we are still seeing attacks that leverage email but these are becoming more sophisticated with a greater degree of personalisation. Criminals are getting better at social engineering; being more believable and finding new ways to get people to click on links or open the attachments that will expose them to Malware."

This type of attack is made easier because there is much more data now available about people in an open source format online, and criminals can use things like social media profiles to find out about those they are targeting.

"Like the firms they target they have become marketing experts," says Hinderer.

"They learn from experience which type of scams work, and which don't, and make their plans accordingly."

The nature of the threat

Carmina Lees director security business unit, UK and Ireland at IBM says there are three broad areas of online risk:

Malicious insiders such as disgruntled employees who exit the company but still have access to old privileges pose as an **insider threat** as do inadvertent actors who fall prey to social engineering schemes that grant access to outside attackers.

In 2015, **trojans, malware and malvertising** have been playing their part affecting many organisations, and continue to do so. The banking industry alone has seen its fair share of attacks such as Dyre, Tinba, Sphinx and Shifu.

Over the second half of 2015, IBM security researchers started to see a huge rise in the number of calls concerning **ransomware**. This is a piece of malware that prevents or limits users from accessing their system or data. It forces victims to pay the ransom through certain online payment methods in order to grant access to their system.

Attackers have evolved to use encryption to hold data hostage and demand payment for the decryption key. This threat is big money and 'Ransomware-as-a-Service' has evolved as a toolkit for attackers to purchase. Ransomware illustrates why patching is a vital activity for businesses to engage in. However, most companies don't do it consistently, leaving themselves vulnerable to attack.

The rise of BYOD and shadow IT

Money-saving ideas that let the criminals in

The growth of Bring Your Own Device (BYOD) was a result of attempts by organisations to save money on kit by encouraging staff to use their own devices, such as smartphones and tablets, for work-related tasks – a decision that has always been regarded as suspect from a security standpoint.

"With employees using their own mobile devices for business and personal activity, firms are now tasked with supporting the new social, virtual, and mobile employee and the applications they access," says Carmina Lees, director security business unit, IBM UK and Ireland. And those applications and activities are often far from secure.

In February 2015, IBM researchers analysed 41 of the most popular dating apps and found that 60% of those apps had medium to high severity security vulnerabilities. They also found that about half of companies have employees who use dating apps on work devices.

The data hack on dating firm Ashley Madison – whose smartphone app allows millions to access its services – serves as a harsh example of the vulnerability of online services. Some 39 million members (about 9.7 gigabytes-worth of data) had personal details stolen, including names, home addresses, sexual fantasies and credit card information.

With about 7.18 billion mobile devices in the world, the shift to mobile devices as the primary form of connecting to corporate networks is increasing rapidly.

In addition, due to work pressures employees often choose convenience over security and according to IBM research: one out of every three employees shares corporate data to third-party cloud apps without the knowledge of their employer; one out of every two millennials share work data to outside cloud apps and by 2020, these millennials will make up 50% of the global workforce; while 60% of employees understand that accessing and uploading data to these third-party applications violates their employers' security and privacy policies, but still do so.

Also, as different devices run on different operating systems and software, this offers determined hackers new ways to infiltrate an organisation's IT system.

The proliferation of data collection, information availability and access devices and routes is also propelling risks to new heights. Those risks come from a wide variety of players in the scene, from 'script kiddies' – teenagers using downloadable tools – to low-key data theft through to espionage by state actors."

Xavier Verhaeghe, technology solutions vice-president EMEA at Oracle adds: "It is getting easier by the day to access information, or manipulate applications, if the organisations involved don't focus on keeping up with the threats by better data governance and IT security measures."

Addressing the risk posed by multiple devices is not just limited to controlling the devices themselves and the websites that staff access

"The only real solution is to standardise both the type of device used by staff and the software used," says Stuart Poole-Robb chief executive at KCS Group. "Whatever device staff use to access social media, they should be made aware that social media websites, such as Facebook and LinkedIn, must be used with caution. They should be educated never to reveal details such as the dates of a business trip on social media. Nor should they provide information on a public profile to enable social engineers to build up an accurate personality profile."

It is important to remember that addressing the risk posed by multiple devices is not just limited to controlling the devices themselves and the websites that staff access.

As a direct result protection is getting more difficult: traditional perimeter security is not efficient and effective anymore.

"A lot of the investments go into network security although a lot of the threats go via other routes like privileged users and more sophisticated access to data," says Verhaeghe. "Even with carefully managed and approved external apps and cloud tools, it is impossible to try to define the perimeter and assume total protection via this way."

Security architecture needs to include levels of protection in different areas such as networks, but also governance, privileged user access management, access governance, data and audit vaults and more recently with the evolutions of security-in-silicon.

A new mindset

Keeping pace with change

The rise of the Internet of Things requires a new mindset, a new way of looking at things, about how we consume technology, says Simon Mullis, global technical lead, strategic alliances at FireEye. "The challenge now is security as a whole and how we manage it, how we measure it and how we keep up with the pace of change," he says.

"There is a massive change to the way people communicate, which has happened very rapidly, and risk managers need to change the way they think to address this."

People are no longer as active when it comes to using technology – picking up a phone, turning on a PC. They are becoming inactive service users, instead, unaware of how devices are constantly communicating with each other. This has a massive impact on risk.

"There is also a blurring of roles between customer and vendor," says Mullis. "For example, you might have a medical device that feeds data to the user to help them manage their health, to the manufacturer to help it improve its product, and perhaps to an insurer. Data is moving in every direction."

The long-held assumption that the answer to security risk is to build higher walls just does not work any more. "There is a growing awareness that a breach is now inevitable," says Mullis. "At some point disclosure will occur and,

'There is a growing awareness that a breach is inevitable'

Simon Mullis, FireEye

most likely, not on your terms. Risk managers need to understand this. Companies can block as much as possible, but the attackers want to breach the wall and, as they grow in sophistication, it is looking more likely that they will succeed."

Firms need to develop a combination of threat intelligence and expertise about how this risk applies to them and use the information to make it more agile, resilient and able to react faster. Doing this requires risk managers to think about the way staff on the network behave. "The target has moved from the data in the data centre to the person who accesses it," says Mullis. "We are moving away from protecting computers and databases and towards looking after the data itself – and responsibility for data is not just the responsibility of the IT guys.

"Authentication, authorisation and access control become more important, rather than the devices themselves," he adds.

These kind of lessons apply particularly to the management of the Industrial Control Systems (ICS) which major manufacturers rely on day in, day out to manage everything from factory processes to power generation.

While these were not necessarily connected in the past, they certainly are now and yet there remains a stubborn, dangerous misconception at board level that there is an air gap [security measure that isolates companies from external and insecure networks] between these systems. "However these are not often used in business," says Dan Scali, manager, security consulting services at Mandiant, a FireEye company. "There is always some connectivity to other technology on the campus and often back to the corporate network itself.

"This is not necessarily a bad thing, but it needs to be designed appropriately to address the risk and monitored so that if there is some kind of intrusion into the network, it can be dealt with."

All trade journal report that the level of connectivity is only going to increase. "Wearable technology, Big Data, all these trends are becoming increasingly present in ICS," says Scali. "If an air gap does exist it is rapidly eroding under the pressure of new technologies."

The risk of a cyber attack occurring is further modified by the fact that new technology is often fitted to existing systems so, rather than designing in security from the off, it needs to be retrofitted. "Industry doesn't have the appetite to rip out old systems for the sake of security, because security doesn't drive the business," says Scali.

In this environment risk managers need to be proactive. "You need to have an approach that addresses the risk practically as it really exists and this means time needs to be spent adapting cyber security so it can be applied to address risk in the real world."

For example, risk asssessors should ensure they have appropriate network segregation and traffic surveillance. "Businesses can't always keep attackers out but they can act fast to make sure any intrusion doesn't cause a catastrophe," says Scali. "Have an incident response plan. If nothing else know what to do when something goes wrong. Avoiding investment in this area is not smart, even in the presence of other options like insurance. If a company's strategy is 'hope', then that's not enough."

> ***'Time needs to be spent adapting cyber security so it can be applied to address risk in the real world'***
>
> **Dan Scali,** Mandiant

To address cyber risk, risk managers will have to roll their sleeves up and get more involved with operational teams so they can be the voice of these people at a strategic level – and by doing so help their organisation face up to the reality in a connected world.

Xavier Verhaeghe technology solutions vice-president EMEA at Oracle adds: "Growing in importance, visibility and business impact, risk managers need to balance the ease of use with total protection."

THOUGHT LEADERSHIP

KYLE BRYANT, regional manager, cyber liability, Continental Europe at ACE Group

Cyber risk and data theft is mercurial, rapidly changing and poses an existential threat to companies. The risk of an attack, particularly a data breach, is rising quickly. In the UK alone, 90% of large organisations and 74% of small businesses suffered a security breach this year, up from 81% and 60% respectively in 2014, according to latest figures by PwC.

Managing cyber risk cannot be addressed with insurance alone. A collaborative approach is needed to forge resilience in the face of a determined attack. By developing the right kind of relationship between insured, broker and insurer demands a new approach from all sides that is built on transparency and honesty from the off. There needs to be full disclosure and transparency so that we can arrive at a solution that is based on clear intent and the right information.

For insurers, this means taking our engagement with clients up a level and really involving ourselves in their risk and risk management. We need to be there to help them develop their defences and their response when the worst happens so that they can deal effectively with a breach and keep moving forward.

The right insurer realises the sheer scale of what companies are up against, brings all the stakeholders together and offers the kind of support that firms need to prepare for themselves to face this rapidly evolving threat.

This can only be done by having the right expertise and experience available to the insured, whether in-house or through the kind of strategic partnerships that add genuine value.

As this report highlights, cyber criminals are becoming more organised, more expert and more collaborative in their operations. We need to be able to meet them and match them at every level; we have to succeed every time while they only have to succeed once. To do this we must realise that we really are all in this together.

On a company level, a good way of cultivating a joined-up approach is through an information incident response (IR) plan.

The IR team should comprise the following professionals:

- IT security experts who can take the technical lead in handling an incident;
- legal and compliance individuals who can advise regulatory requirements;
- PR and communication personnel to manage external communications about an incident; and
- an executive management to make key decisions.

The team should proceed first by defining the roles of each team member, before an IR plan is developed. The plan should establish the escalation procedure should a risk occur. Clear responses procedures should also be detailed, with information on data breach containment, evidence preservation, risks and impact evaluation, and typical legal and communication response.

After establishing the internal and external breach response teams, it is important to test the plan in order to identify any gaps.

ACE insured.™