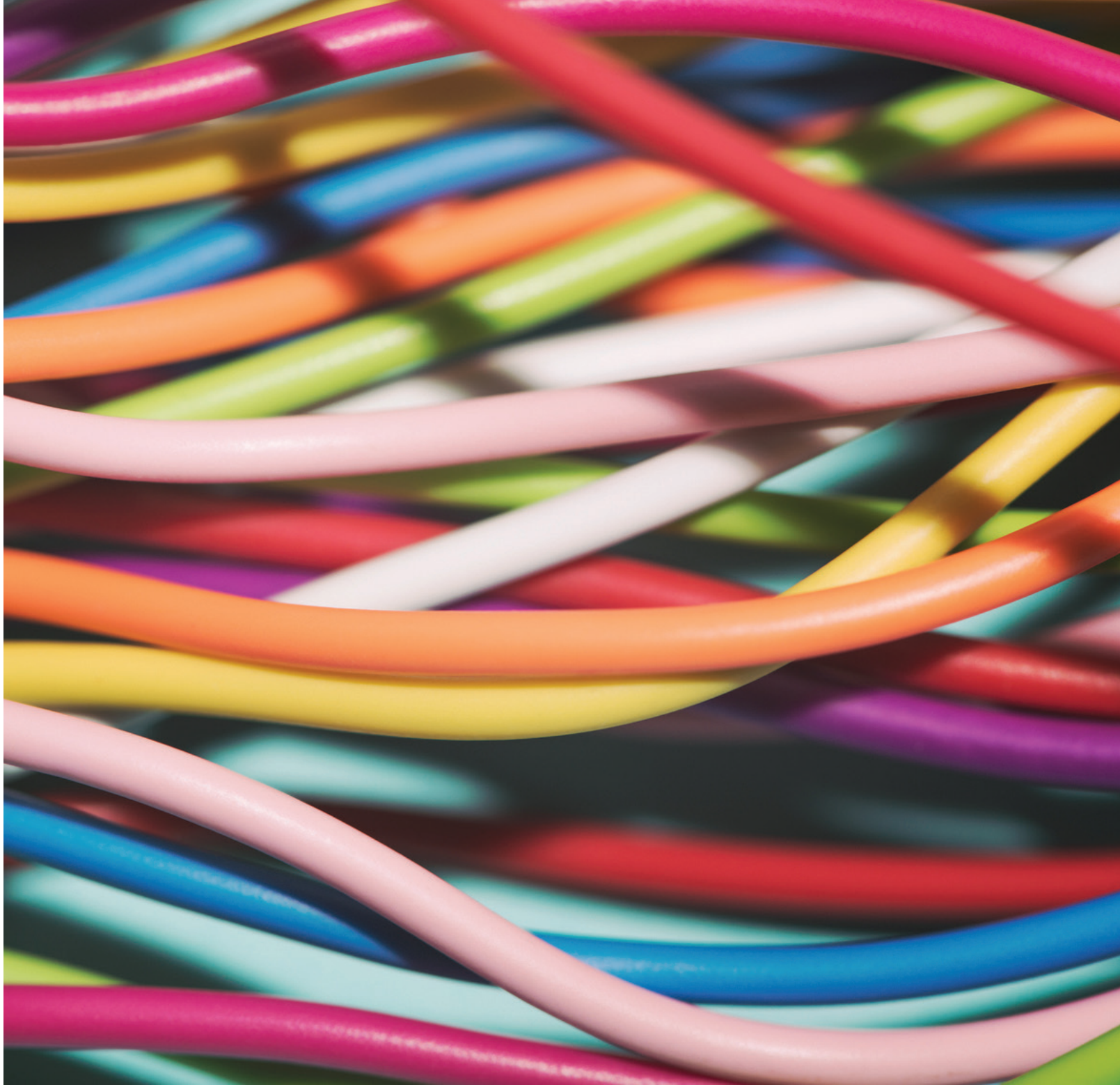
RSA

CYBER RISK
A CLEAR APPROACH



Businesses, large and small, are now more reliant on IT than ever before.

As technology evolves, so does the way we use it to streamline and enhance our operations and processes. But this reliance on technology also makes companies more vulnerable to cyber threats.

Traditional insurance policies may not have been designed to cover these new and evolving risks, which is why specific cyber policies are becoming more and more important to businesses.

The RSA Cyber Risk product has been developed specifically with this type of risk in mind, covering threats from the most innocent data breach to the most malicious hacking attack. It is built around a simple 24/7 notification service so that we can react quickly in those critical early hours. This helps reduce an incident's impact and gets the business back on its feet when it is most vulnerable.

A real cyber risk example

A recruitment firm was faced with a data leak when a disgruntled employee did not have access rights removed during the leaving process. They were able to access sensitive personnel information, which was then posted on a social media site.

Consequently the Insured found themselves in breach of privacy legislation, liable to pay costs including notification, damages, expenses, and credit monitoring.

AROUND

52%

OF

BUSINESSES **THINK** THEY HAVE CYBER COVER*

IN REALITY **LESS THAN**

10%

ACTUALLY DO*

*Source: HM Government & Marsh UK Cyber Security Report March 2015

THE IMPACT ON BUSINESSES

Most businesses now rely in some way on computer software or systems to operate, handling everything from customer databases to fully automated manufacturing processes.

This dependence on technology as a fundamental cornerstone of operations leaves businesses more exposed to cyber risks than ever.

Although it tends to be the high profile cyber events which make headlines, thousands of smaller incidents are happening on a daily basis. 81% of larger businesses and 60% of smaller operations suffered a cyber breach in 2014 alone*.

These attacks can cripple businesses, regardless of their size, affecting their day-to-day running and in consequence both their finances and their reputation. Something as simple as an attack to take a website offline can cost thousands of pounds in lost revenue.

Yet, despite cyber attacks posing a potentially devastating threat to a business, many traditional insurance products don't fully cover these risks. Instead they are usually aimed at the tangible parts of the business, from employees to physical contents, and ignore the potential risk to non-physical assets like data.

HOW CAN CYBER RISKS AFFECT BUSINESSES?

Cyber risks can have far-reaching consequences on the way a business operates. Here are just a few ways in which they can cause real problems:

- Virus or hacking attacks which stop customer transactions
- Corruption or damage of data
- Theft of intellectual property
- Loss of customer, supplier or critical process data
- Consequent liability to a third party, including associated litigation, fines, costs, awards and damages
- Subsequent damage to reputation as a result of the attack.
- Loss of Gross Profit or Gross Revenue.

A real cyber risk example

A hotel chain that allows customers to book online suffered an operational error when a data centre switchover did not complete fully. Their online booking system was down for over 8 hours resulting in immediate lost revenue.

60%

OF SMALL BUSINESSES SUFFERED A CYBER SECURITY BREACH IN 2014*

How would your client run their business without access to their systems?

*Source: HM Government & Marsh UK Cyber Security Report March 2015

COMMON CYBER RISK SCENARIOS
WHAT WOULD YOUR CLIENT DO IF...

	RISK	HOW RSA CYBER RISK CAN HELP
AN EMPLOYEE OPENS A PHISHING EMAIL AND INTRODUCES A VIRUS TO THE SYSTEM THAT CORRUPTS CRITICAL SUPPLIER DATA? 	Something as simple as opening an email can cripple a business' systems, corrupting data or even deleting it completely. This means vital information including contracts, transactions or process coding can be lost, bringing a halt to the business until the data can be restored.	Forensic investigation and data restoration costs cover can provide an IT expert to trace, identify and resolve the source of the issue, eliminating the virus and recovering any lost data to allow your client to continue with their business as before. Also, our Cyber Business Interruption cover will compensate for lost income as a result of any downtime, subject to an agreed waiting period.
AN EMPLOYEE ACCIDENTALLY LOSES A LAPTOP FULL OF CONFIDENTIAL CUSTOMER DATA? 	Loss of customer data can halt the operation of a business or lead to costly litigation as a result of breaching privacy legislation. It also has a potentially less tangible but even more serious knock-on effect on your client's reputation, fostering distrust with customers and hurting profits.	Assistance from public relations specialists can help reduce the possibility of significant damage to business reputation. Our cover can also offset the costs of notifying and reassuring customers and the payment of legal fees or compensation if required.
A HACKER ACCESSES A NETWORK AND INSTALLS RANSOMWARE? 	This leaves a business with no access to their data files and can include a ransom demand. Depending on which files the criminal has locked, this can cause serious interruptions to anything from distribution to customer transactions. In the worst cases it can grind the whole business to a standstill.	Our Cyber Extortion cover can help to determine the cause of the problem, limit adverse publicity and either mitigate or eliminate any credible threat stemming from the extortion. Data restoration costs to restore or replace data which is lost or damaged are picked up too. Our Cyber Business Interruption cover will also compensate for any lost profits as a result of an inability to trade.

^Source: Verizon Data Breach Investigations Report May 2015

23%

OF PEOPLE OPEN PHISHING EMAILS^

Do you think all employees could spot a trick email?

11%

OPEN THE ATTACHMENTS IN THOSE EMAILS^

Do you know how easy it is for a system to get infected?

THE COST OF FIXING A DATA BREACH OF 1,000 RECORDS IS BETWEEN

£33–£35

PER RECORD^

Could your client afford the cost of recovery if vital data was lost?

EVERYONE MAKES MISTAKES

Even with the latest security programs and toughest processes, human nature is still liable to introduce vulnerabilities. No matter how well trained they might be, people can often be the weakest links in a security system.

Whether it's a case of writing down a password or opening a malicious email, people introduce weaknesses to network security all the time, and that's before you consider the danger of rogue employees. It's worth considering protection even if your client's security programs and processes seem strong.

40%

DOWNLOAD WORK FILES TO PERSONAL DEVICES**

50%

TAKE CONFIDENTIAL INFORMATION WHEN LEAVING**

30%

MOVE DATA TO FILE SHARING APPS WITHOUT PERMISSION**

**Symantec at Security Matters Forum March 2015

WITHOUT THE CORRECT COVERAGE...

A simple virus in a system can have a bigger impact than your client might initially think.

What may seem like a problem for just the IT department could have a damaging knock-on effect on other departments and even the brand image.

THE IT DEPARTMENT

Vital time and resources will be diverted from other tasks in order to contain and fix the problem at its source. If the IT department doesn't have the necessary expertise to tackle the issue, your client might have to outsource help, upping the costs of fixing the problem, and increasing downtime.

THE FINANCE DEPARTMENT

A hit to a business' reputation, the unavailability of a website or the cost of notifying and compensating customers can impact the bottom line. And any legal action or fines and penalties imposed will only add to the cost.

THE BRAND

If customer data is compromised or a business is unable to fulfil contracts, it can severely impact their reputation amongst customers. They may feel like they can't trust the organisation to keep their information secure, or rely on them to supply critical products, and therefore take their business elsewhere.

THE SHAREHOLDERS

With the loss of income and the potential negative impact on reputation, shareholders may be inclined to sell their shares. This could cause share prices to plummet and the business' reputation in the financial markets to be similarly damaged.

A real cyber risk example

A very small independent drinks seller/bottler found a virus in one of their systems involved in the bottling process, which meant not enough bottle lids were produced for the batch of bottles. This resulted in waste and consequently the Insured suffered a Loss of Revenue through lost sales.

WHO IS UNDER THREAT FROM CYBER RISKS?

THE SHORT ANSWER IS EVERYONE.

Whether your client runs a manufacturing plant reliant on computer automation, a data warehouse or a retail outlet, any company which uses electronic equipment and computers is at risk. Although the type of incident may vary from business to business, with vastly different intentions or consequences, anyone with a reliance on computers or a body of data has a dangerous vulnerability to cyber risks.

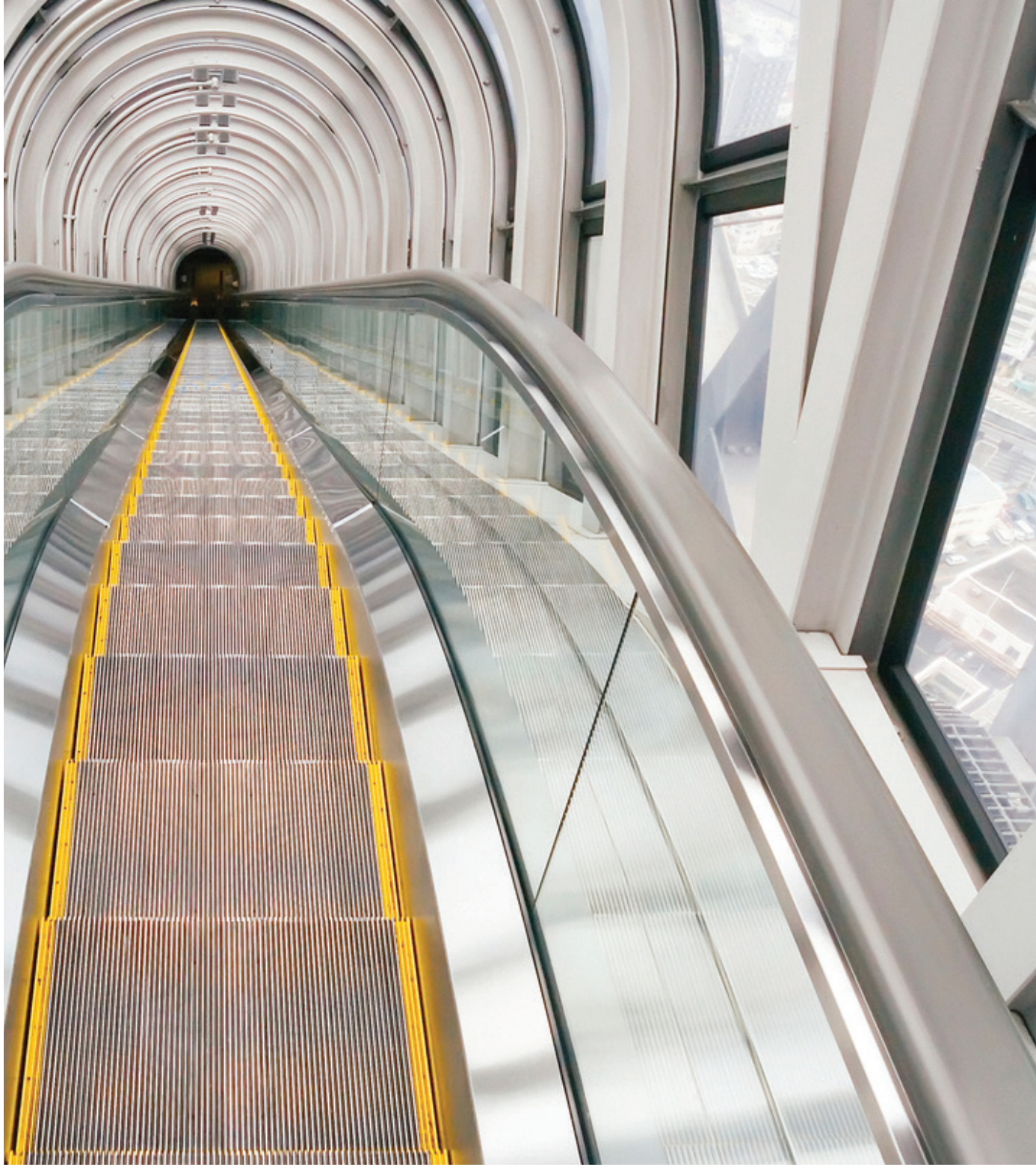
Your client needs to be able to respond – and fast.

IN

60%

OF CASES, ATTACKERS ARE ABLE TO COMPROMISE AN ORGANISATION IN MINUTES^

^Source: Verizon Data Breach Investigations Report May 2015



WHAT DOES RSA CYBER RISK GIVE YOUR CLIENT?

Cyber risks are a real and serious threat to all types and sizes of business, but they're also risks that traditional policies don't address.

The RSA Cyber Risk policy is simple and offers wide-ranging cover, designed to work alongside traditional insurances to cover a business for all the types of cyber risks they face.

More than that, it provides a complete service to handle cyber incidents on your client's behalf, taking on the stress for them and getting their business back up and running as soon as possible.

SIMPLICITY AND PEACE OF MIND:

- A clear and wide-ranging policy so your client knows exactly how we can help
- A design which works alongside other RSA policies to keep things simple
- Cover for all the key eventualities, from malicious attacks to innocent data breaches, extortion to denial of service
- Limits are available as appropriate for the individual risk and we include our full range of covers as standard.

HELP TO QUICKLY GET THEM BACK IN BUSINESS:

- 24 hour incident number available day and night for fast response. Cyber risks are unpredictable and a few hours can make all the difference – we get businesses back up and running as quickly as possible
- Where required, we aim to have our IT forensic experts get in touch within an hour of instruction, going straight to the heart of the problem.
- One number to call with all further action handled from there – you can rest assured that the situation is being handled by an expert, someone who takes the stress so you and your client don't have to.

ONE ALL-ENCOMPASSING SOLUTION:

- Handpicked services including IT Forensics, Legal and public relations help, all local and all coordinated together. Your client can be confident that they are getting the very best help when they need it most
- An end-to-end approach diagnosing the issue, fixing it and getting the business back on track
- A cost-effective way to responsibly manage cyber risks and ensure that the threats posed to your client's business in this highly complex area are minimised.

EXPERTS ON CALL DAY OR NIGHT WITH OUR 24/7 INCIDENT NUMBER

IT FORENSICS

PUBLIC RELATIONS ADVICE

LEGAL ADVICE & DEFENCE COSTS

CREDIT & IDENTITY MONITORING COSTS

ITEMS OF COVER CENTRED AROUND A 24/7 INCIDENT RESPONSE NUMBER

NOTIFICATION COSTS

DATA RESTORATION COSTS

CYBER BUSINESS INTERRUPTION

CYBER EXTORTION

CONSIDER THE RISKS

- **How many customer records does your client hold?**
  Remember: A data loss costs an average of £33-35 per record^. It could be as simple as a lost laptop.
- **How would your clients business operate if they couldn't access any of their systems for a day, a week or even a month?**
  Remember: 60% of small businesses suffered a cyber security breach in 2014*. Don't let your client be one of them.
- **How many employees do they have?**
  Remember: 23% of them will open phishing emails^. You can't always guard against human nature.

*Source: HM Government & Marsh UK Cyber Security Report March 2015
^Source: Verizon Data Breach Investigations Report May 2015

WHEN THEIR REPUTATION AND INCOME ARE AT STAKE, WHO WOULD YOUR CLIENT CALL?

RSA Cyber Risk can help.

To get a quote, simply speak to your usual RSA contact or for further information on our Cyber Cover visit rsabroker.com

RSA