CARDNET

Cybersecurity and fraud

Protecting your business

LLOYDS BANK

Securing your data and staying compliant

Understanding your data

In recent years, many business models have shifted towards the collection, storage, and use of data. The ability to better target consumers using data gives businesses significant commercial advantages. However, many small and medium sized businesses who do not think of themselves as data-centric in fact collect a great deal of information and are vulnerable to cyberattacks and fraud as a result.

Understanding the data your business collects is key. There are two key challenges here. The first is to recognise the data your business collects. Data can include information on payments collected, social media followers, records on company finances, names on a loyalty programme or mailing list, information on employees' names, addresses or bank details, and other information which businesses use.

For example, a restaurant might have recipes and menu preferences, a hotel chain might hold data on guests' visiting frequency, and shops might store information about suppliers' services and prices, and so on.

The second challenge is to accept that some of this data could be valuable to fraudsters.

For example, after a hacker who was paid to help Uber find security vulnerabilities accessed names, email addresses, phone numbers, and drivers' license numbers, he turned rogue, and demanded $100,000 from the company to delete the data*. His leverage was not based on the information itself, but on his ability to publicly embarrass Uber. They responded by paying him. The lesson – and the challenge – is to see that a company's data may be more valuable to others than it appears internally.

Cybersecurity and fraud

Key facts

The quantity of data created and copied each year will reach 180 zettabytes (180 followed by 21 zeros) by 2025. It would take 450 million years to pass through one broadband connection.

Source: The Economist

45%

of all micro/small businesses identified a cybersecurity breach or attack in 2016/17.

Source: Government Cybersecurity Breaches Survey 2017

92%

of organisations still think their information security capabilities are a cause for concern.

Source: EY Global Information Security Survey 2018

$3.86 million

the global average cost of a data breach in 2018. This is up 6.4% compared to 2017.

Source: IBM.com

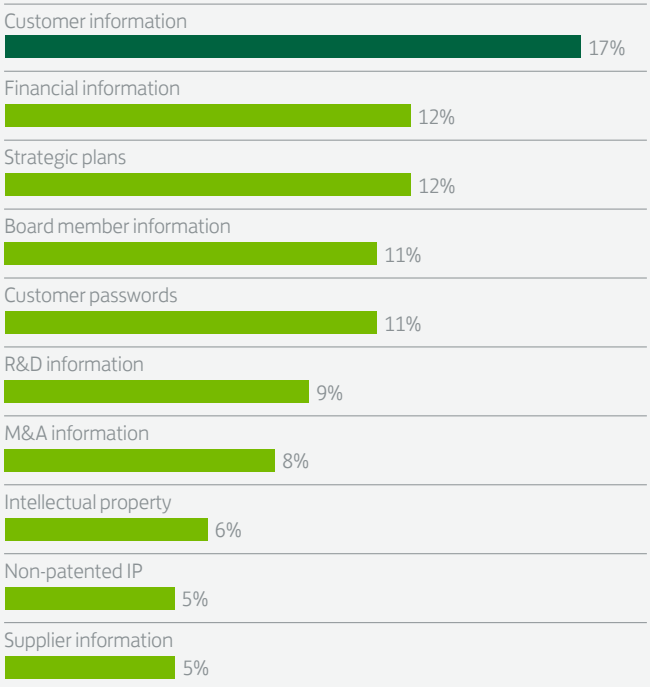
* https://www.nytimes.com/2018/01/12/technology/uber-hacker-payment-100000.html

Legal rights and wrongs

Cybersecurity is no longer just a commercial imperative. It is now a legal imperative too.

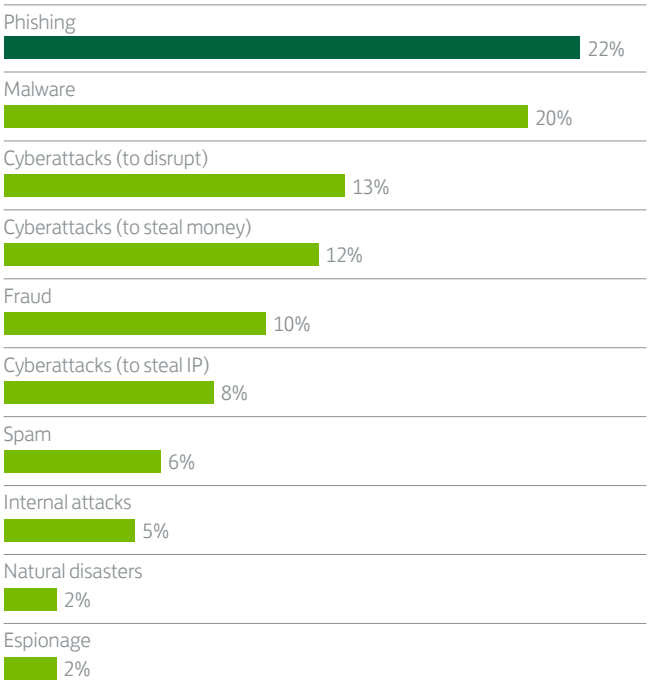
There are broadly three key pieces of legislation with which businesses should be familiar: the General Data Protection Regulation (GDPR), the Networks and Information Systems (NIS) Directive, and the Data Protection Act 2018. Introductory guidance for small businesses on each is provided by the Information Commissioner's website here.

TOP 10 MOST VALUABLE INFORMATION TO CYBER CRIMINALS



Source: EY Global Information Security Survey 2018–19

TOP 10 BIGGEST CYBER THREATS TO ORGANIZATIONS



Source: EY Global Information Security Survey 2018–19

There are not only significant fines for non-compliance, there is also an emerging culture, led by the Data Protection Commissioner, in which companies' data protection policies and practice is a factor in the eyes of the law, with real consequences for enforcement actions, such as fines. In other words, if there is a data breach at your company, the legal consequences will depend, to a great extent, on how prepared your company is. Although businesses are unlikely to be sanctioned for being the victim of a breach itself unless it is the symptom of lax security, they might be punished if a subsequent investigation reveals that they have made no attempt to secure their data, write and implement data security policies, conduct impact assessments, train employees on good data practice, and generally minimise the damage from any breach.

Legal rights and wrongs

Practices

Many threats can be avoided by ensuring that basic good data practices are adopted throughout the organisation.

Alan Calder, founder of IT Governance Ltd, an IT consultancy, explains how they do it: "We train our staff to recognise phishing with regular internal updates and reminders," he says. He also makes sure the company is proactive about testing and improving their security processes. "We carry out monthly penetration tests," he says, "investigate each incident, and deploy whatever improvements we identify."

Lost laptops or smartphones are a key cybersecurity risk. Prevention involves fostering a company culture where it is unacceptable to do anything which makes such a loss more likely, such as carrying a company laptop to restaurants, bars or pubs, or any destinations where it is not needed.

Case Study

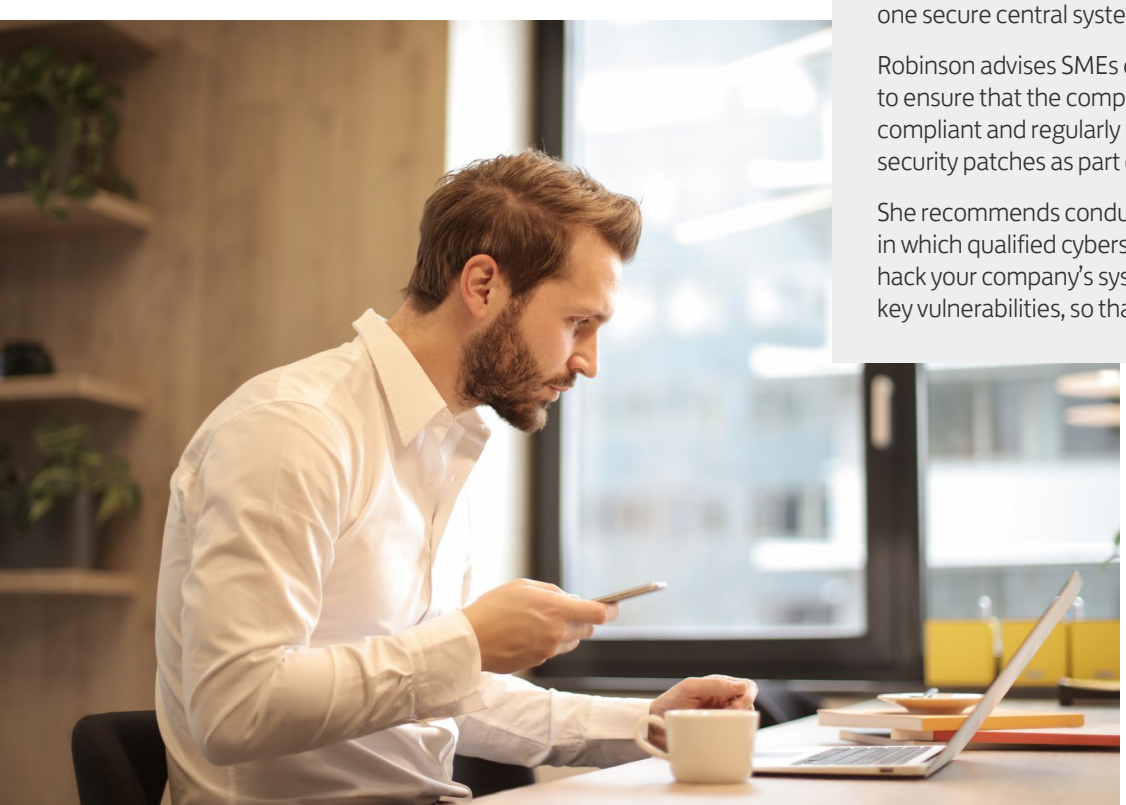
Prior Analytics Ltd, a Customer Relationship Management and Data Security company, takes a number of measures to defend their data against cyberthreats.

"We have developed an e-learning course to educate people on phishing and malware, so they can actually recognise what is not genuine on an email," says Claire Robinson, managing director at Prior Analytics. "That means looking for things like emails which aren't addressed to a specific person or bad spelling and grammar."

Prior Analytics also takes steps to ensure their clients' data is stored securely. After a cyberattack years ago, they conducted a thorough review of their data arrangements. They moved from an in-house server to a secure, UK-based cloud server. The company also invested in a second cloud backup for all mission-critical applications, and consolidated all data into one secure central system.

Robinson advises SMEs choosing a cloud service to ensure that the company they choose is GDPR-compliant and regularly updated with the latest security patches as part of the contract.

She recommends conducting an independent audit, in which qualified cybersecurity professionals try to hack your company's systems and report back on all key vulnerabilities, so that they can be addressed.



Legal rights and wrongs

If an employee has access to work-related information on their smartphone, it is advisable to ensure it is via an interface which can be shut down remotely, such as an app. As a minimum, it is advisable to keep the data accessible behind a password-protected app or equivalent. It is also good practice to avoid sending work emails containing data which could be used to identify customers personally to employees' personal accounts, to minimise the chance of it moving beyond the direct control of the company.

There are a number of precautions companies can take to ensure that if a breach occurs, they are prepared. They should start by auditing the information in their possession. The audit should include an assessment of the relative value of the information and a stock-take of the information the company has, and how and where it is stored. This ensures that when they implement increased security measures, it protects all sensitive, valuable, or personal data.

They should then limit access to the most valuable data. For example, when employees leave the organisation, management should be able to take them off the access list to avoid the risk that ex-employees receive confidential business-critical information or personal data by email accidentally.

External accreditation on cybersecurity also helps to give customers confidence. Alan Calder has made sure that his business meets the standards set by the government to give his clients the confidence that their data is safe with IT Governance.

"We are certified to ISO 27001, with BS 10012 within the management system scope. On the basis of an asset-based risk assessment, we select controls that reflect our risk appetite – and, where client data is concerned, we are quite risk averse." Calder says.

Claire Robinson from Prior Analytics says that her company is in the final stages of the government's CyberEssentials qualification, which certifies that the company is able to guard against the most common cyber threats.

To avoid fraud, it is advisable to conduct regular checks, such as on bank transactions, to ensure that all are recognisable and accurate. It is also worth encouraging all companies in the supply chain to do the same. After all, many suppliers hold data which, if hacked, could compromise the companies they supply.

The National Cyber Security Centre recommend that you

Protect endpoints

- use up-to-date and supported operating systems and software
- deploy critical security patches as soon as possible
- implement application whitelisting technologies to prevent malware running on hosts

Protect the network

- use firewalls and network segregation to protect services
- deploy an always-on antivirus solution that scans new files
- perform regular vulnerability assessments against both internal and external services to scan for any insecure configuration

Protect the information

- implement a policy of 'least privilege' for all devices and services
- use multi-factor authentication to protect sensitive information
- ensure that all services are protected by strict authentication and authorisation controls
- use password managers to help prevent password reuse between systems
- implement a practical monitoring and alerting service

Source: The cyber threat to UK business 2017-2018 report, National Crime Agency

Expert Insight

Q&A with Cate Pye, Associate Partner, UK and Ireland, Security and Government Cyber Lead at EY. EY publishes an annual cybersecurity survey of 1,400 CIOs, CISOs and other executives in this area.

Q: What is the most common kind of fraud cyberthreats for SMEs?

A: Phishing. These are communications, normally delivered via email, which will disrupt or deface the reputation of the organisation, or attempt to steal financial information.

Q: What should people look out for to identify a phishing email?

A: They will normally ask you to click on a link which aims to inspire some kind of urgency or play on the recipient's emotions. It might pretend to be an unpaid invoice or an overdue bill, for example, with a notice saying 'you must pay now' or similar language.

Q: What other kinds of techniques should businesses look out for?

A: Another technique is known as 'whaling', which is best thought of as like phishing only for bigger fish. These communications target the C-suite, individuals who have more power within the organisation, or those with greater access to the systems, such as IT admin functions.

Q: What do you advise businesses do to avoid being harmed by these kind of scams?

A: Things to look out for include email addresses that you don't recognise and links where what it says it is does not match the destination link it would seem to take you to when you hover over it.

I also advise businesses to be wary of unexpected emails. Personally, if I'm not expecting an email from a particular address, I'll usually delete it.

Q: For merchants with limited budgets, where best should they allocate resources between tech training and other potential vulnerabilities?

A: Careless employees and security control. If you're looking for the best bang for your buck, put it into those two areas. 80% of hacking attempts can be stopped by having basic system limitations in place.

Not sharing passwords is a good example of employee behaviour which can prevent a good deal of attacks, as well as having strong enough passwords. In one Australian state, for example, 1,464 government officials used "Password123" as their password. Many organisations can improve their security by simply getting the basics right.

Important Note:

The information shared in this update was accurate at the time of publishing but many of the regulations we discussed are subject to change.

While all reasonable care has been taken to ensure that the information provided is correct, no liability is accepted by Lloyds Bank for any loss or damage caused to any person relying on any statement or omission. This is for information only and should not be relied upon as offering advice for any set of circumstances. Specific advice should always be sought in each instance.

Please contact us if you would like this information in an alternative format such as Braille, large print or audio

Our service promise
We aim to provide the highest level of customer service possible. However, if you experience a problem, we will always seek to resolve this as quickly and efficiently as possible. A copy of our 'How to voice your concerns' leaflet can be obtained by contacting the Cardnet Helpline. The complaint procedures are also published on our website lloydsbankcardnet.com/how-to-complain.

For more information visit
lloydsbankcardnet.com

LLOYDS BANK