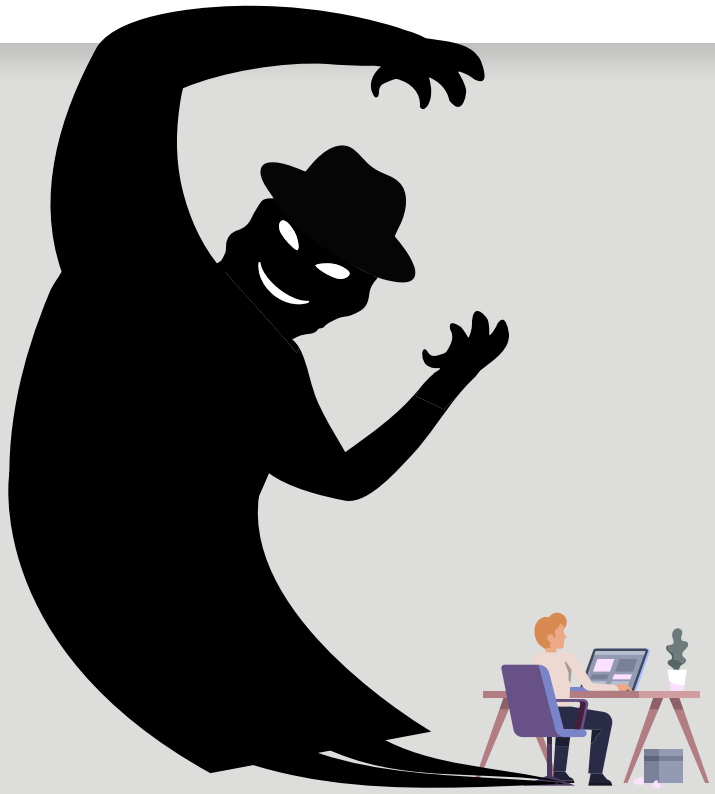
arrow

# Cyber Security

## How to keep your business safe

It's been estimated that globally, hackers attack a target every 39 seconds,[2] while the number of incidents has grown by 67% in the last five years[3]. Yet as more personal and business data is collected by businesses, this threat is only likely to grow.



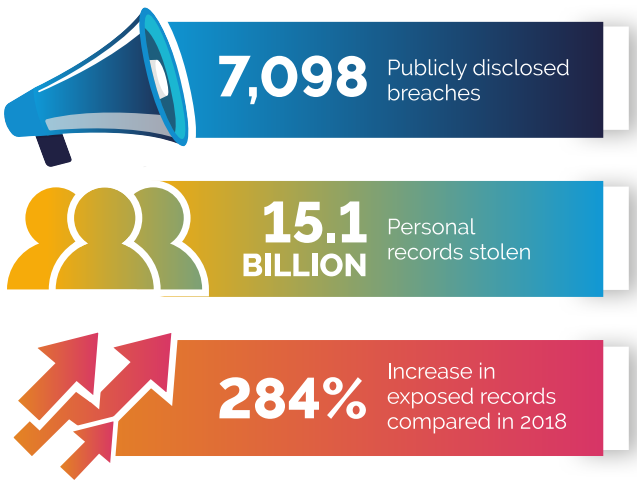
# The rising threat of cyber crime

Cyber crime is big business. In the last few years, both the number and sophistication of attacks aiming to steal key personal and business data have grown dramatically, with both nation states and organised criminal gangs increasing their efforts.

Therefore, these activities have become increasingly identified by firms as a top threat to their operations. Indeed, one study by Allianz rated cyber incidents as the number one business risk for 2020, ahead of business interruptions, changes of regulation such as Brexit, natural disasters and climate change[1].

Yet despite this, many firms are still unprepared for these threats, with poor-quality or incomplete defences that are unlikely to pose a significant barrier to a hacker. So what should companies do about this to ensure they are effectively securing their assets?

### A Growing Threat - Global Cyber Attack Stats for 2019[4]



# Why security is everyone's responsibility

With protecting data becoming a top business priority for any firm, it is no longer something that should be treated as a concern only for the IT department. Instead, every member of the organisation from the board level down will be held responsible for protecting their digital assets.

Senior staff are the key in achieving this, as they typically set the tone for the organisation as a whole. If they are seen to be making security a priority, others will follow. But if they're complacent, this attitude will permeate throughout the company - with the potential for serious repercussions.

## The consequences of security failings

A key factor in this is that the financial consequences for cyber security failings are higher than ever, with new, tougher data protection rules greatly increasing the size of the fines regulators are able to dish out. The most consequential change has been the introduction of the GDPR regime in May 2018, which is beginning to show its teeth.

In 2019, for example, some of the biggest fines ever recorded were handed out by the Information Commissioner's Office for cyber security breaches. British Airways, for example, was hit with a penalty of £183 million for a data breach that saw customer financial details stolen,[5] while the Marriott hotel group received a penalty of £99 million for a similar incident[6].

***"Personal data has a real value so organisations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the public."***

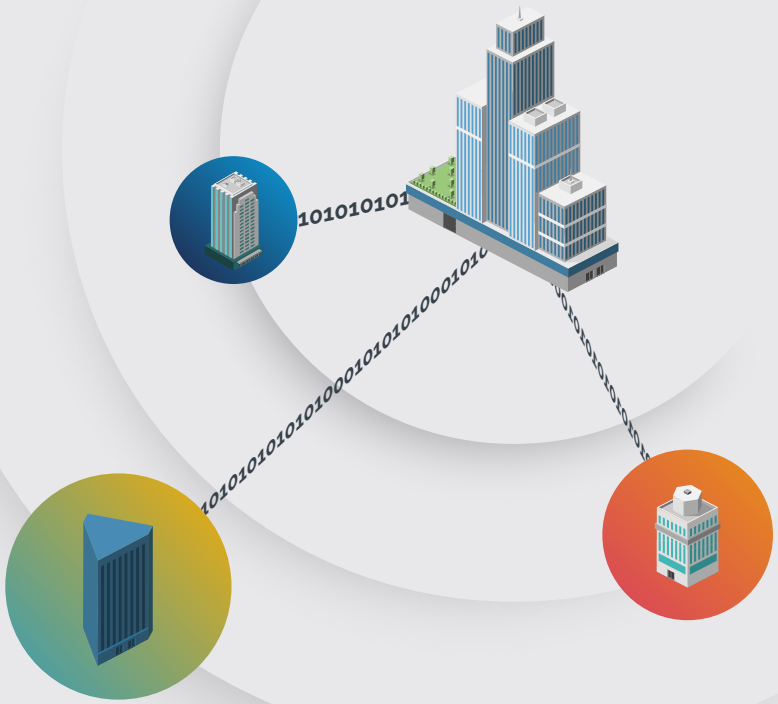
***Elizabeth Denham,***
***Information Commissioner[1]***

This is without taking into account the costs from lost business, recovery operations and damaged reputations that can arise from a cyber incident. With GDPR including tough reporting requirements for breaches, the days of trying to sweep any incidents under the rug are gone, so firms will have no choice but to publicly deal with the fallout of a breach.

## The risks facing smaller firms

Many smaller firms may see these consequences as a worry that is reserved for the largest enterprises, which hold huge amounts of personal data. But in fact, these companies are often not the most attractive targets for criminals. While the rewards for gaining access to the biggest companies can be high, there is also often a much higher degree of difficulty in targeting large companies with expansive resources to devote to security.

As a result, smaller firms are increasingly finding themselves in the crosshairs. These can be hugely valuable targets for hackers, as they will still hold valuable information, but they often have much less robust defences due to a lack of financial resources and expertise.




### Consequences of Cyber Attacks in 2019[9]

**32%** of businesses experienced an attack in the last 12 months

**39%** of these businesses identified at least one attack per month

**27%** had to devote staff resources to dealing with breaches

**21%** of incidents stopped staff from carrying out daily work

What's more, they may also be viewed as a gateway into larger firms. Many small companies may be suppliers to larger enterprises or have other relationships that attackers can exploit to bypass the tougher defences of the bigger firm.

Indeed, in 2019, it was estimated by Verizon that 43 per cent of data breaches involved small businesses[7], and these can be highly costly. Research by Analysys Mason found that the smaller the firm, the larger the relative impact of a cyber attack - and with one in four small businesses saying their defences aren't up to scratch[8], a breach could even threaten the survival of smaller firms.

# Understanding where the gaps are

The first stage in protecting against these threats must be to have a complete picture of your entire IT environment, in order to identify exactly where your weak points lie. This may not be as simple as it first seems, as in today's complex environment, there will be a wide range of touchpoints connecting to your network, many of which may not be clearly visible.

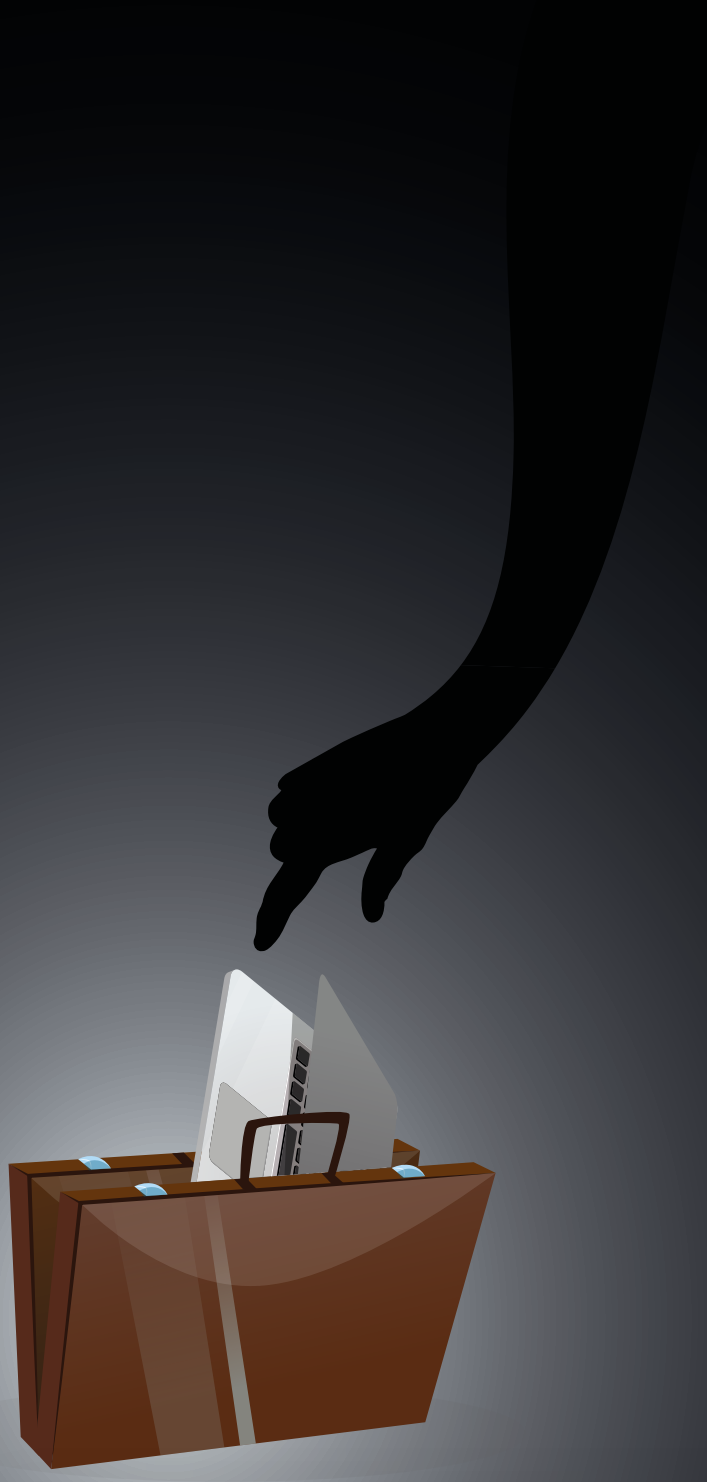
While you may have strong defences such as firewalls and antimalware software to protect your perimeter from intruders, it's vital these defences are extended to every endpoint on your network. This can be considered much like protecting your home - you may have strong locks on the front and back door, but do you have an upstairs window left open that a determined thief could gain access through?

This is an issue almost every company will face, as even if firms do not permit the use of devices such as personal smartphones, it is very difficult to prevent users accessing key information anyway if it is more convenient. Even something as simple as using a work email account via smartphone on the morning commute could potentially expose data, whether it's through connecting to an unsecured Wi-Fi network or even someone looking over an employee's shoulder.

## A new generation of endpoints

A key factor is understanding what devices and applications are connecting to your network. For example, personally-owned mobile gadgets are one of the biggest vulnerabilities for any business, as you often have little or no control over how and where these connect and what potential vulnerabilities, such as malware, they may be exposing the network to.

But it's not just mobile devices firms have to worry about. For instance, any time an employee plugs in a USB flash drive they've brought from home to transfer a file, they could be unwittingly bringing in malware to the network. Elsewhere, the huge range of Internet of Things devices being introduced to businesses could pose security vulnerabilities, as these often do not have effective protections such as encryption.



## Protection beyond your perimeter

While many people's idea of a data breach may be as the result of a direct hacking attack that penetrates the perimeter, in fact this is just one of the ways a data breach could occur. For instance, the loss or theft of a business laptop or mobile could expose data, and this will be treated by regulators in much the same way as a digital data breach. In 2017, for example, insurer RSA was fined £150,000 after the theft of a hard drive containing the details of nearly 60,000 customers[10].

Data that's held in the cloud should also be considered. While enterprise-grade cloud systems will have robust security protections to prevent data breaches, the devices being used to access them may not. Cloud computing offers many advantages to users, including the ability to store and access data from anywhere.

Good policies for mitigating these risks are therefore a must. This should include both guidance to users, such as reminding them never to connect devices to public Wi-Fi networks, through to software solutions that can block the installation of unapproved apps or wipe a device remotely should it be misplaced.

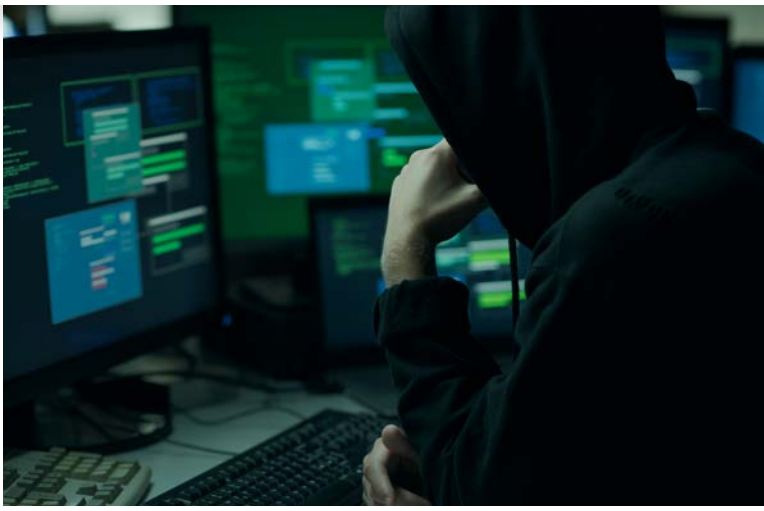
# The weakest link - your users

Ultimately, you can have the toughest, most advanced technologies in the world protecting your data, but they will all be worthless if the people using them aren't taking enough care.

In fact, **one analysis of ICO data conducted by CybSafe found that in 2019, as many as 90 per cent of data breaches in the UK could be traced back to human error**[11].Therefore, ensuring your people are aware of what to do - and what not to do - is just as important a part of your cyber security strategy as having the right technology.

There are a wide range of errors that can be made by users. Poor or reused passwords can give hackers a backdoor into sensitive systems, for example, while badly-configured privileged accounts can allow employees to access and change data they are not supposed to, undermining security. Even data entry errors when sending emails can end up with sensitive data going to the wrong person.

**User errors that result in data breaches**

## Managing the social engineering threat

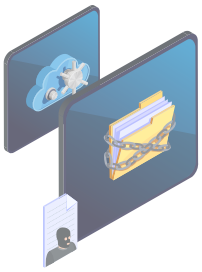
One of the biggest challenges for businesses is addressing social engineering attacks. These are among the most common methods used by criminals to gain access to sensitive data and take advantage of human psychology to trick people into handing over information. To use the analogy of protecting a home, if a traditional hacking attack is the equivalent of picking the lock, a social engineering attack is like convincing the homeowner to invite them inside.

One of the most common ways to do this is phishing attacks, where attackers send users emails pretending to be from recognised contacts or businesses. According to CybSafe's study, such methods accounted for 45 per cent of all reports to the ICO in 2019.

These may entice users to download a malware-filled attachment, or direct them to fill out a form on a fake website that can capture login details, for example, but there are a wide range of tactics used by criminals to trick people into handing over data.

Spear-phishing attacks, for example, are more targeted than standard phishing attacks, taking advantage of personal information. For instance, some scammers impersonate senior executives and ask more junior employees to send over sensitive details, something that can be highly effective as employees will be reluctant to question a request from the CEO.

## Ensuring you provide the right guidance



To prevent such attacks, effective employee training is a must. This should involve educating employees on what to look out for in order to avoid falling victim to these threats. For example, when it comes to phishing, it should highlight telltale signs that a message is not genuine. Is it unsolicited? Are there spelling or grammar errors? Does the link URL match what would be expected?

This should involve the creation of a clear policy outlining what employees will be expected to do and the process for reporting a suspected social engineering attempt. For example, you should make it clear that personal data should never be sent by email, or accessed from non-approved devices. While it may prove impossible to stop every event, setting out what is and isn't acceptable behaviour for users can go a long way.

However, it's not enough to do this just once. Cyber security training needs to be an ongoing endeavour to ensure employees are aware of emerging threats and are not slipping back into bad habits.

For example, one persistent issue for businesses is poor password practices. Every year, lists of the most commonly-used passwords are published, and every year without fail, the same combinations crop up, which indicates that even though users are warned repeatedly about the danger of this, messages don't sink in and convenience overrides security.


# Protection from the outside in

To bring all these factors into a single security strategy, it's vital to take an 'outside in' approach - starting with protection for the edge of your network and progressively working towards every endpoint within it.

## Key essentials for any security solution

Going back to the analogy of protecting your home, a comprehensive security system starts with your perimeter fencing and protecting the doors. But it must also ensure windows are kept secured - even those you may think are out of reach. Meanwhile, on the inside, motion detectors that can spot intruders and safes to doubly secure the most valuable items are a must to ensure protection at every point.

The same is true for your firm's network. Firewalls and intrusion detection and prevention solutions can block the most obvious points of entry, but must be complemented with other tools to ensure protection at every stage.

For instance, other key steps include an effective patching regime to ensure outdated, vulnerable apps aren't offering hackers an open window. Keeping software up-to-date is a relatively simple - if time-consuming - step, but it's one that far too many businesses overlook.

Indeed, research from Tripwire shows one in three breaches in Europe (34 per cent) are the result of unpatched applications[12], and some of the highest-profile hacking attacks of recent times have been traced back to these issues, such as the 2017 Equifax attack that compromised the details of some 143 million people[13].

Data backups are another essential step - one that is especially important as attacks such as ransomware become more common. While prevention is always better than cure, firms that have good, frequently updated data backups will be in a much stronger position to ride out such attacks with minimal business disruption.

## The right technology to comprehensively protect your business

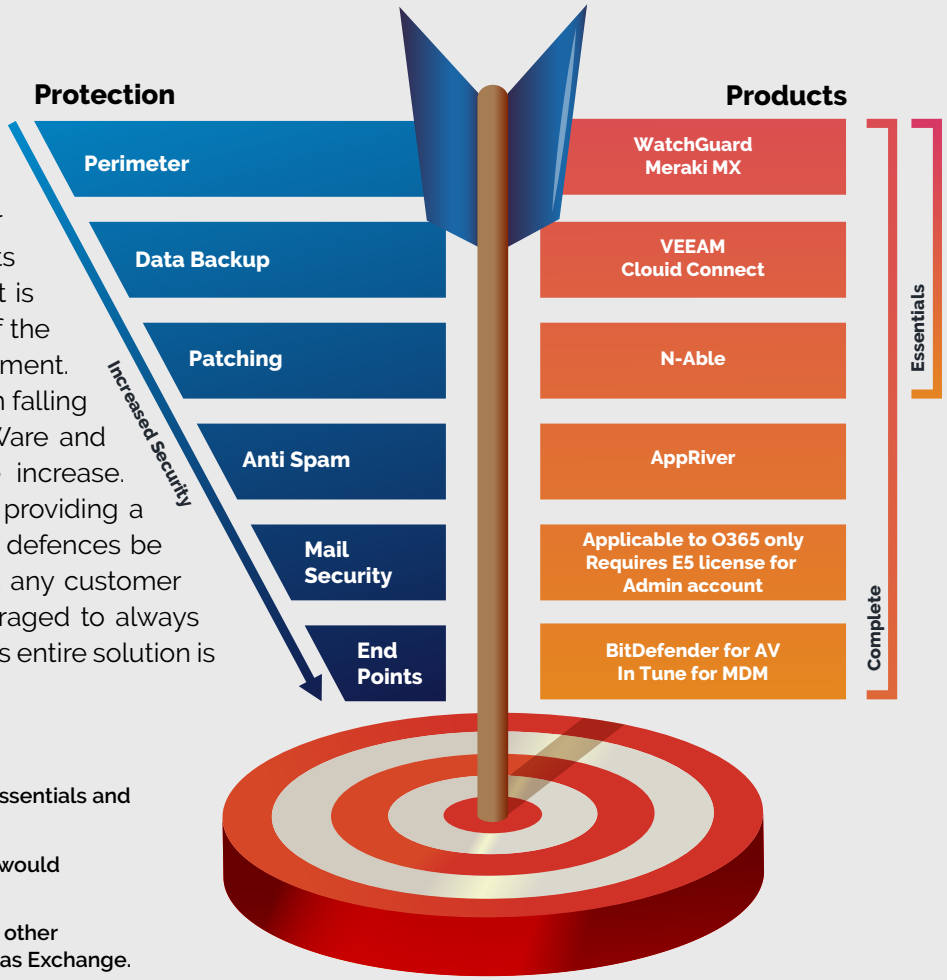
Perimeter defences, backups and patching programmes should be at the heart of any system as part of a comprehensive system. Unified Threat Management tools such as Watchguard, backup solutions like Veeam and antivirus tools including BitDefender all play their part in creating a more secure environment.

Added to these, anti-spam tools, specialised mail security software and dedicated endpoint security tools such as the mobile security solution Wandera are all elements that should be added to these systems in order to increase the level of security and ensure comprehensive protection against any emerging threats.

We recommend a complete malware prevention system that uses a combination of tools to safeguard every aspect of your environment, beginning with perimeter defences and going all the way through to endpoint protection. This ensures that no matter what type of threat your business faces, it will have the tools on hand to deal with it.

### Arrow Malware Protection System (AMPS)

This product pulls together a number of different Arrow IT security products to create a single IT security solution. It is designed to work from the perimeter of the organisation right into the end user equipment. It's purpose is to prevent an organisation falling victim to MALWARE such as RansomWare and Phishing, which is very much on the increase. Finally, it has the added advantage of providing a reliable and secure backup should the defences be breached. There are two variations but any customer wanting this product should be encouraged to always choose the 'AMPS Complete' option. This entire solution is subscription based.




There are two variations for the product. AMPS Essentials and AMPS Complete.

These are listed in order of priority and what we would recommend to a customer.

The mail security is only applicable to O365. The other elements can be implemented if the customer has Exchange.

# Ensuring you're as safe as possible

It's essential that businesses are proactive when it comes to guard against cyber threats, and this means making early preparations, having a clear plan about what to do, and frequently testing your tools to ensure they work as advertised. You don't want to be in a situation where you only find out your defences have holes in them once a breach has occurred.

It also pays to have a trusted partner you can turn to for advice on how to deploy systems and best protect your business. This is especially important for smaller enterprises where budgets and human resources are limited. Whether it's recommending what steps need to be taken to protect certain critical systems or running workshops to educate employees on security best practices, being able to access the right expertise is essential.

This is also the case if, despite your best efforts, you do fall victim to a breach. In this situation, it's important to have a response plan ready to go that defines what your recovery process will be and what contingencies will need to be enacted to keep your business running. Again, having a trusted partner who can offer expert guidance will be essential here.

With a comprehensive cyber security system that takes an outside in approach to your defences, you will therefore stand to be well-prepared for whatever the coming years throw up. However, cyber criminals and hackers never stand still and are always coming up with new methods of creating data breaches, so you must do likewise when it comes to maintaining and upgrading your security solutions.

# Contact Us

Arrow Business Communications
Enquiries@arrowcommunications.co.uk
0330 440 4444

[1] https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf
[2] https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
[3] https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
[4] https://www.prweb.com/releases/the_total_number_of_records_exposed_in_2019_has_hit_15_1_billion_an_increase_of_284_on_the_previous_year_as_the_number_of_breaches_reaches_an_all_time_high/prweb16905446.htm
[5] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
[6] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/
[7] https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[8] https://www.analysysmason.com/Research/Content/Comments/survey-security-inadequate-ren04/
[9] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf
[10] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/150-000-fine-for-insurance-company-that-failed-to-keep-customers-information-safe/
[11] https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/
[12] https://www.tripwire.com/state-of-security/vulnerability-management/unpatched-vulnerabilities-breaches/
[13] https://www.wired.com/story/equifax-breach-no-excuse/