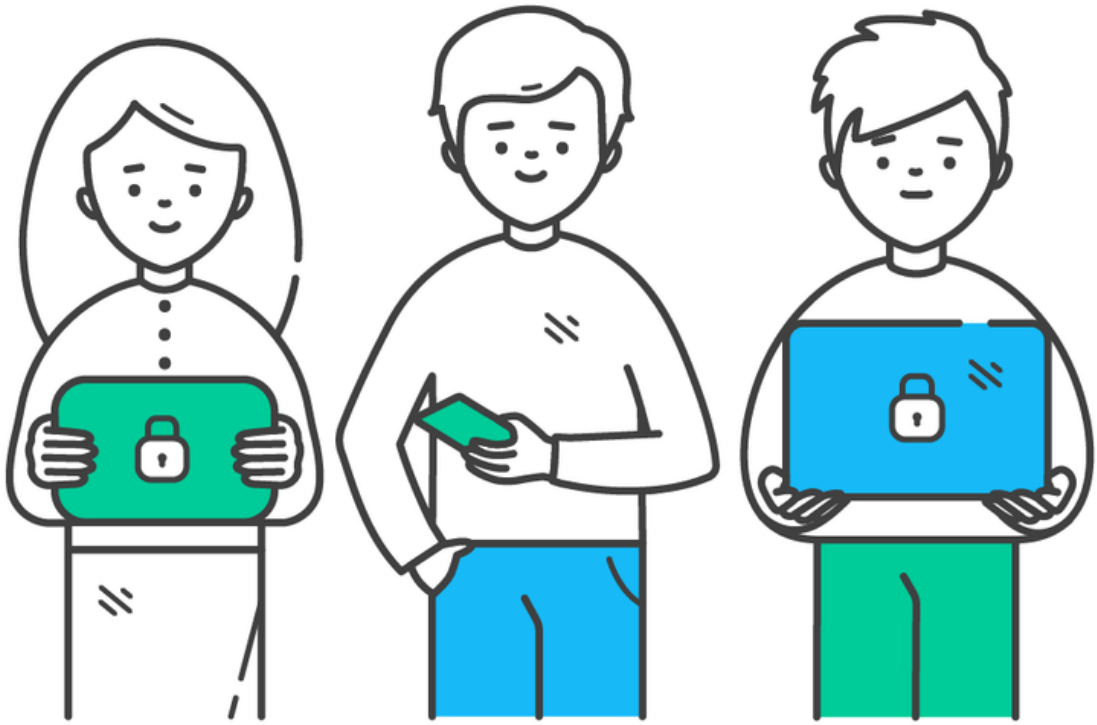
The 2020 Complete Guide to Security Awareness Training



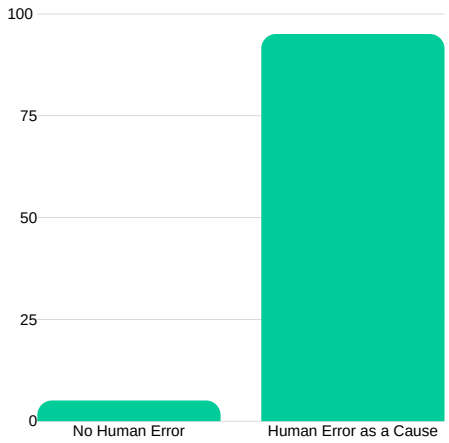
Contents

Introduction: The Threat of Human Error

Cyber threats come in many forms. Malware remains a significant danger, with the 2017 WannaCry outbreak that cost businesses worldwide up to $4 billion still in recent memory, and other new strains of malware being discovered on a daily basis. Phishing has also seen a resurgence in the last few years, with many new scams being invented to take advantage of unsuspecting companies. Just one variation, the CEO Fraud email scam, cost UK businesses alone £14.8m in 2018.

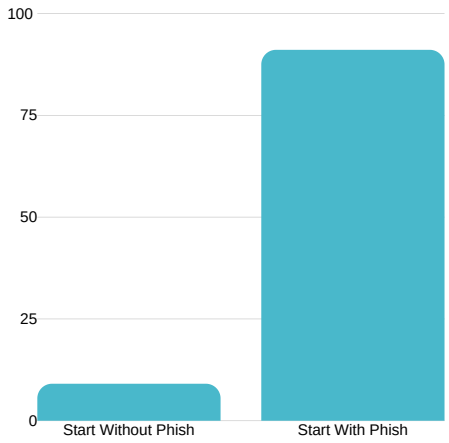
Which cyber threat was the most damaging the previous year or which will be the greatest new threat the next year often becomes a talking point around the end-of-year period. While it's important to keep up to date with the threat landscape, there is an underlying point that these discussions often fail to surface. With such a variety of threats targeting businesses, and new ones evolving daily, it is impossible to predict which type of attack will target your organisation next, or prepare defenses for a specific form of attack before it hits. Thus, if a business is to defend themselves, it becomes imperative to be able to defend against as wide a range of attacks as possible, and to look for the common themes that tie these attacks together.

Percentage of breaches where human error is a cause



Source: IBM

Percentage of cyber attacks that start with a phishing email



Source: Symantec

The Role of Human Error

Almost all successful cyber breaches share one variable in common: human error. Human error can manifest in a multitude of ways: from failing to install software security updates in time to having weak passwords and giving up sensitive information to phishing emails. Even as modern antimalware and threat detection software have grown more sophisticated, cyber criminals know that the effectiveness of technical security measures only go as far as they are properly utilised by humans. If a cyber criminal manages to guess the password to an online company portal, or uses social engineering to get an employee to make a payment to a bank account controlled by the cyber criminal, there is nothing that technical solutions can do.

In 2014, IBM conducted a study into the cyber breaches that occurred among thousands of their customers in over 130 countries. This study was the most wide-reaching look into the causes of cyber breaches that had been performed at that point, but its results have since been found again and again in similar studies. One of the key findings of the IBM study was that human error was a major contributing cause in 95% of all breaches. In other words, had human error not been a factor, the chances are that 19 out of 20 breaches analysed in the study would not have happened at all.

Since human error plays such a vast role in cyber breaches, addressing it is key to reducing the chances of your business being successfully targeted. It also allows you to protect your business from a far wider range of threats than any single technical solution could - and can potentially empower your workforce to actively look out for and report new threats they may encounter. Mitigation of human error must be key to business cyber security in 2020 - and in the next section we'll look at the best ways to go about it.

How to Address Human Error?

Two factors have to be present in order for human error to manifest: opportunity and decision. Opportunity means that there is a situation where a human is allowed to make a mistake: for example, letting end users handle software updates rather than forcing security updates through with patch management. Decision is the action of the individual: in this case, the lack of action in installing security updates when they are available.

A comprehensive mitigation effort includes both reducing the opportunity for error as well as improving the decisions made on the part of the end users. Taking action in both areas is essential to ensure that human error is thoroughly addressed. In the case of patching, for example, a technical measure such as introducing patch management may reduce the opportunity for human error to a minimum in most cases - but it is still essential to account for situations where the technical solutions has a temporary lapse, or if a new situation such as a BYOD policy where users are allowed to use their own devices without patch management is introduced. In other cases, such as with phishing emails, technical measures such as spam filters and breach detection software have a very limited effect in reducing opportunity for error when faced with a targeted attack. In those cases, the only effective way to mitigate human error is by teaching end users how to make better judgments.

67%

Increase in security breaches 2013 to 2019.

Source: Accenture

How to Improve End-User Decision Making?

In order for end users to make the right judgment in a security situation, four different factors have to be present. The first of these is quite straightforward: the user has to recognise that they are in a situation where security is potentially at stake. Without recognising the situation as such, the user may not even realise that they are making a decision at all through their inaction. Secondly, the user has to know what the correct course of action is. This doesn't necessarily require the user to completely understand the threat, but often is as simple as reporting the situation to a person in the IT or security department who can look into it. Thirdly, the user must know why security matters, so they understand the importance of not ignoring security procedures and are aware of the potential implications of a breach. While these three factors are all essential for improving security outcomes, it is at this crucial point that businesses often falter. In order for better decisions to be made in real-world situations, the fourth factor must also come into play: pain avoidance.

Issues such as weak password security and failure to patch software persist in organisations across the world, despite many computer users understanding why these issues are critical to security. The reason that action is not taken despite knowledge is due to what we refer to as pain avoidance. Having a unique and strong password requires more time to create, and more effort to remember, than a short, weak, or reused password. Despite a user knowing better, this 'pain' caused by creating a strong password is often strong enough to make the user go against their best judgment. This is compounded by the fact that, despite many users taking the correct action under optimal circumstances, busy and urgent work situations as well as stress can make security measures feel even more 'painful' to users.

It is this last factor that can only be resolved through cultural change. End users have to feel that the pain caused by following security best practices is less than the satisfaction gained by not doing so. Technical measures such as password managers are essential in this, as they make acting in a secure manner far easier: if employees don't have to create or remember their own passwords, they have no reason not to use secure ones. Simultaneously, the threshold for performing the correct action must be lowered through cultural change. This means putting security at the forefront of decision making, and ensuring that users never feel they are 'wasting time' by taking appropriate security precautions. Security should be discussed among employees, and questions and points that end users bring up about security issues in their own roles should be paid attention to and rewarded. This helps users feel like security isn't just an afterthought, but something that is always worth spending the time on.

Effective security awareness training addresses not one, but all four of these factors. This means identifying situations where data or systems could be compromised, understanding best practices, knowing what the potential consequences of breaches are, and finally helping to push through a cultural change to create an environment where security considerations are always taken into decision making.

32%

The share of UK Businesses that experienced a breach in 2018.

Source: UK Government

What's the Best Format for Security Awareness Training?

Security awareness training isn't all one and the same. The way in which training is performed, structured and presented will have a major effect on its effectiveness in genuinely improving security outcomes in your organisation. In this section, we'll take a look at what exactly is the best way to perform security awareness training for your end users.

Why Old-School Training Failed

Security awareness training used to mean making end users sit through an annual sessions consisting of hours of lectures and slideshows. The idea was that users would remember something of what they saw and heard - and in the worst case scenario at least the box for 'educating users' could be ticked. How did it fare in actually improving security outcomes though? It didn't work, and everyone hated it.

There are a number of reasons why this type of annual lecture-based training isn't effective. The first of these is that in an annual training session, there will simply be too much information at once for any employee to digest and remember. Even if users are given learning material to take with them or are sent occasional reminders, chances are that most of the material in the training session will go in through one ear and out the other, and forgotten in mere moments.

Lectures and slideshows are not entertaining or engaging formats for end users to learn from. They fail to raise the interest of employees in the same way that video and interactive content do, and too often are filled with unnecessary information that isn't relevant to every end user. Slides filled to the brim with small text are sure to make any employee fall asleep halfway through the session.

The final, major reason why traditional training isn't effective is that it doesn't make use of learning through repetition. If there is a year between learning sessions, users simply won't remember what they've learned - and awareness of security issues in general will plummet in the days and weeks after training. Security can't be a one-time thing, but must be year round in order to be effective.

Security awareness training has increasingly shifted to online software-as-a-service solutions. Cloud-based training offers some immediate benefits over traditional methods, but isn't necessarily the ultimate answer to security awareness unless it delivers in certain areas that are essential for genuinely improving security outcomes.

How to Make Training Truly Effective

Having a truly effective security awareness training program is possible - but there are some important criteria you need to follow to genuinely engage your users.

Breaking Down Material

There is a limited amount of information that a person can absorb at a time. This is especially true when it deals with topics that most employees won't have much previous knowledge on. In order for the amount of learning material to not overwhelm end users, it has to be appropriately broken down into segments, each with their own clear, simple message that's presented to users in an easily-digestible fashion.

Continuous Learning

Another benefit of breaking down learning material is that it allows learning to easily be made continuous, rather than a one-time thing. Breaking down learning into parts allows these sections to be sent out regularly throughout the year, helping keep security awareness consistently on the minds of end users. As repetition is key to learning, this is crucial for ensuring that users actually remember what they've been taught.

Relevant Material

Ensuring that learning content is relevant to end users is essential for making sure they stay engaged. When an end user is presented with information that they feel is not relevant to them, they will quickly start losing interest and paying less attention. Learning material needs to not only avoid jargon and technical terms, but be made with real-life situations in mind that the average end user would actually encounter in their day-to-day working life. For example, most employees don't need to know the specifics of regulations or malware attacks, but simply how to conduct themselves in a manner that reduces those risks - and how to appropriately report risks that they may encounter.

7

The average number of items a person can hold in short-term memory at one time.

Source: Verywellmind

Repetition

Is the key to learning according to scientific research on memory-building.

Source: Front Hum Neuroscience

15-30s

The average duration that items are stored in short-term memory.

Source: Simply Psychology

Recollecting

from short-term memory through testing is the key to building long-term memory.

Source: Cognitive Psychology

Practical Advice

It's all good and well teaching employees about the risks out there and how they can be countered - but what's essential is that employees walk away from training with actual steps in mind that they can put to use right away in their daily work activities. Giving employees the chance to put their training to test right away also helps build memory - and can be achieved using tools such as phishing simulation.

Video and Interactive Content

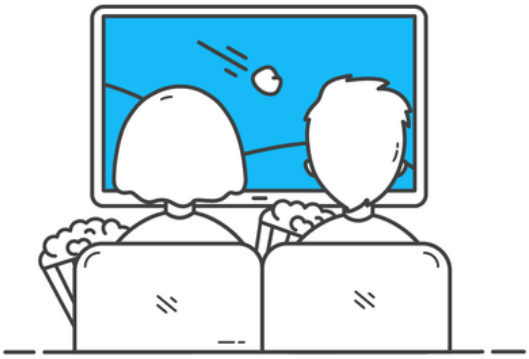
Not all content is the same. Text-based content becomes tiresome to users quickly, and should only be used when complemented by visual, more engaging content. Videos are great for keeping users entertained - as long as they are high-quality and enjoyable to watch. Humour can be used to great effect to make security awareness videos more appealing to end users. Interactive content is also great for engaging users. Many people learn by doing - answering questions or otherwise taking part in their learning - and interactive content can also give users a sense of achievement for getting through a course.

Questions and Testing

It's essential that after training sessions users are tested on what they've learned. This helps you know that users have learned key points and are walking away having learned something - but also helps the learning process of users as they recollect the information they have just learned from their own memory.

A Part of a Security Culture

The most essential part of a security awareness training programme's effectiveness, however, has as much to do with factors outside the training as the training itself. In order for training to be effective, it has to be a part of a security culture where security is always given the consideration it needs, and users are actively encouraged to bring up concerns and ask questions. A good security awareness programme contributes to this by presenting security as something that is continuous and active, rather than one-time and passive - but it is essential that the organisation supports this effort outside training as well.



Why Training Has to Become Part of a Security Culture

Security awareness training will not be effective in improving security outcomes if it is not accompanied by cultural change. Comprehensive training will teach end users how to recognise situations where security is at risk and how to deal with them appropriately - but this knowledge is not going to be put into practice unless the user feels that security is valued in their culture.

With the growing number of threats present, as well as the increasing complexity of business services and access to data and systems from mobile devices, it is impossible to know where the next threat or accidental leak to your business might appear. This is why security shouldn't be about ensuring that your end users choose strong passwords or follow other specific steps - but rather about empowering them to be active guardians of your business, its systems, devices and data.

How to Build a Security Culture?

Culture is all about values. In order for employees to care about security, it needs to be highlighted as a value throughout the company. This means ensuring that security isn't seen as the responsibility of the IT or infosec team - but as a responsibility shared by all employees.

Cultural change and the company's values have to come from the top. Senior management has an important role to play in emphasising the role of security in the business - but it is essential that they grow, rather than dictate, the new culture. This means encouraging employees to take an active role by asking them to bring up concerns relating to their own roles, and prompting them to ask questions and become engaged with security issues.

75%

The share of people that 'don't know a great deal' about protecting themselves online.

Source: NCSC

33%

The share of businesses that have cyber security policies in place.

Source: UK Government

50 Days

The average time taken to resolve a malicious insider attack.

Source: Accenture

This way, users feel like they are involved in the security process, and start actively thinking about the security considerations in their own roles. A manager or someone in IT may not be completely familiar with all the processes of an employee's workflow - which is why it's essential that users themselves understand that they need to take steps to ensure the security of data and systems.

The senior management also has a role in establishing priorities for the business. Anyone that works for an airline will tell you that safety is always, without any exception, the top priority. Everything else comes second. While in most other businesses security isn't a life-or-death issue, it's important to remember just how damaging any breach can be to a business. If customers no longer feel like they can trust an organisation with their personal information or their business, it could be the end of the company. It should be made clear to all employees that security always comes first - and that it's always better to ask and make sure than to be sorry afterwards.

For a secure business environment, an ingrained principle of least privilege will go a long way toward protecting business assets, data and systems. While the principle of least privilege is often seen as a technical measure - limiting each user to only the privileges that they require for their specific duties - it should also be embedded directly into corporate culture. This means encouraging users to actively report when they have access to more data or systems than they need - helping to limit possibilities of breaches.

In terms of physical measures, items like posters can be helpful in building a security culture, and also contain helpful reminders on topics such as password strength. It's important to remember though that just sticking a poster on a wall won't achieve anything by itself, but they should be used as starters for discussion, or serve in complement to training material that users are already engaged with.

Finally, it's important to make sure that employees feel their contributions to security are valued. When employees ask questions, they should always be given time and consideration, and it should be made sure that they completely understand the answer and why it matters to security. When users bring up security concerns, they should always be rewarded for paying attention and working to help keep the business secure.

What Topics Should Security Awareness Training Include?

It's not only the format of security awareness training that matters, but what you include in it. Training should exhaust all core topics, without being overwhelming to users. While each organisation and each job role will have different requirements, there are some essential areas that are worth ensuring every single end user is aware of - even just briefly.

1. Internet & Email Use

In 2020, it is a rare employee that doesn't use the internet or email in one form or another at work. While businesses are enjoying the great flexibility that the internet allows - and many are entirely dependent on the internet for their operations - it can also provide a major risk to businesses. Users may inadvertently install malware, leak data, give up credentials to phishing emails or fall for any of the many other attacks that cyber criminals are targeting them with.

Training users to use the internet and email securely is essential. Most of this comes down to awareness: knowing that emails can cause data breaches if sent carelessly, and that malicious sites can contain malware. There should also be practical advice in training, such as informing users about the difference between cc and bcc fields, and what the HTTPS encryption symbol on websites means.

2. Removable Media

Even as file sharing and online collaboration services on the internet have become more popular, removable devices are still seeing widespread use in businesses. As useful as removable media devices are, they pose many risks: they are easily lost or stolen, potentially leading to compromise of data, or could be replaced with devices containing malware. A common scam is leaving a virus-infected USB drive in an office parking lot, waiting to be picked up and inserted into a company computer by an unsuspecting employee. In addition, many users are unaware that it's not only storage devices that could pose a risk: even simple USB or charging cables could be modified by a cyber criminal to contain malware.

Educating end users about secure use of removable media comes down to accountability. It should be made clear to users that they have to take responsibility for devices that are under their control - and that they should not plug in any devices that have been unaccounted for into any computer, but instead report them to the IT team or to security personnel.

3. Passwords & Authentication

Passwords continue to be a major headache for businesses, employees and customers alike. Humans simply aren't designed to remember long, complex phrases - especially not dozens of them. This means that employees are constantly tempted to take the easy way out and make them easy to remember - especially when they are required to share access to apps and services with their colleagues.

The majority of end users will be aware of why password security matters, and have the basic gist of what makes a strong password. The focus on training around passwords and authentication should be on focusing practicable advice on how to keep up password security without making life harder for your end users. This means encouraging the use of password managers (if this is something your business permits), asking employees to turn on two-factor authentication for all services and systems with access to sensitive data, as well as teaching employees how to make a password that is both reasonably complex while being reasonably easy to remember.

4. Physical Security

Even as cyber security threats multiply, it is essential that physical security is not overlooked. It is no use protecting data with strong passwords and multi-factor authentication if an unauthorised person can simply walk into the office and pick up a paper copy of a sensitive document right off the printer tray.

When training end users in physical security, it is essential that focus is placed on identifying and mitigating threats relevant to individual end users' day-to-day activities. If your business is based in an office, every employee is going to walk through the office door - so tailgating is an example of a security threat that is relevant to all employees. End users should be trained to actively think about what areas and documents are secure, and ensure that they are always locked securely or accounted for when not in use.

123456

The most popular password worldwide in 2019.

Source: NCSC

73%

The share of online accounts that are guarded by duplicated passwords.

Source: TeleSign

5. Mobile Device Security

Mobile device use in businesses has been growing quickly, and in 2020 this trend is expected to become even more widespread than before. Mobile devices such as laptops, mobile phones and tablets allow employees to work from home, coffee shops, while travelling or just about anywhere they wish, providing flexibility to both themselves and the business. As convenient as mobile devices are, they do come with risks that users must be educated about.

Users should be educated on how mobile devices can potentially expose company data and systems to unauthorised access. This involves access through lost or stolen devices, as well as malicious software and illegitimate third-party apps.

6. Working Remotely

In 2020, remote work is going to be more popular than ever. The affordability and availability of devices as well as widespread internet connectivity mean that many employees can work from just about anywhere. This allows greater flexibility, benefiting both employees and businesses, but also comes with new risks. Laptops, mobile phones, tablets and other devices can pose a serious security threat if they are lost or stolen. If employees store or access company data from their mobile devices, this data all becomes vulnerable if a device falls into the wrong hands.

When educating users on secure remote working, focus should be placed on helping users identify points where systems or data could become compromised.

7. Public Wi-Fi

As users increasingly work while on the go, chances are that they will connect to business services, networks or data from public Wi-Fi access points. Public Wi-Fi is highly convenient for mobile work, but also comes with security risks.

It's important to teach end users that their data could potentially be intercepted on public Wi-Fi networks. If you allow your end users to access company data or services through public Wi-Fi networks, you should equip them with Virtual Private Network software and educate them on using it in a secure manner.

8. Cloud Security

Over the last few years, business services and data have increasingly shifted to the cloud. In 2020, this trend is coming to a culmination, with many business operations being conducted entirely using web-based tools and services. While the cloud offers great flexibility to businesses, it is essential that users know how to use and access it securely.

Strong passwords and authentication, as well as email security, become of extra importance when your business uses cloud services. A bad actor that guesses an employee's passwords could access your sensitive data from anywhere in the world, which is why it is essential that employees are educated on the measures necessary to keep cloud accounts secure. Multi-factor authentication is especially a must for all services and apps that contain sensitive business data.

9. Social Media Use

Employees - and businesses - spend an increasing amount of their day on social media. It is essential, however, to ensure that the business' security won't be compromised over careless use of social networks.

Focus on social media training should be placed on making users aware that what they share might be available to anyone on the internet - and that even small details from within the office could be crucial to attackers. For example, an innocent selfie from within the office could show a whiteboard in the background with sensitive business information, or even a customer's details.

10. Phishing

Phishing remains a huge threat, with 23% of employees opening phishing messages. Part of the reason why phishing is so dangerous is that it can be performed in so many different ways, from CEO fraud emails impersonating company directors, to password reset emails impersonating online services.

End users are highly vulnerable to phishing emails because they take advantage of social engineering techniques. While most users will be aware of the reasons why installing dodgy websites or downloading attachments from unknown sources could result in a malware infection, phishing attacks are highly effective at duping victims by impersonating trusted colleagues, partners and organisations.

11. Social Engineering

Phishing is only one of many types of social engineering attacks. It's essential that employees are educated on the different types of social engineering attack - from those over the phone to in-person threats - and understand how to properly deal with any potential offender.

12. Security at Home

In addition to threats in the workplace, end users should be educated on how to stay secure at home. This is especially beneficial if users are allowed to work from home - but even if that is not allowed in the company policy, raising awareness of common security issues is still useful for the business.

23%

The average share of employees that open phishing messages.

Source: Symantec

46%

The share of users who install security updates as soon as they are available.

Source: NCSC

Conclusion: A Building Block of the Security Puzzle

In 2020, the organisations that will most effectively overcome the cyber threat are those that help to ensure their employees care - about the business, the customers, and protecting data and systems.

Security awareness training works when end users are truly engaged. This requires learning material to be truly relevant to the day-to-day working lives of your employees, providing practical advice they can take with them right away, as well as using video- and interactive content to help users stay interested and convey information in an enjoyable format.

Security awareness training isn't a silver bullet. It works best in compliment with solutions that reduce the opportunity for human error in the first place. These measures should form a part of a security culture, where security considerations are always given due consideration. Business decisions shouldn't be made only for security implications to be considered afterwards - but security should form a part of decision-making in the first place.

$5.2 trillion

Total estimated global cost of cyber crime 2019-2024.

Source: Accenture

89,271

Number of data breaches reported in the EU in the first year of the GDPR.

Source: EU Commission

63%

Share of breaches that were not detected by antivirus or breach detection software.

Source: UK Government