ASIA AND THE PACIFIC
Regional Innovation Centre

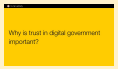
public digital

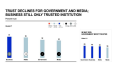
Module #4 - Building trust in digital government

Digital Transformation Training Modules

Time	Slide #	Script (text and actions)
Building trust in digital government (180:00:00)		
Introduction (02:30)		
00:15	1 	Share screen Hello and welcome everyone. Thank you for coming along to the fourth session of a series of seven modules on digital government.
01:00	2 	This is meant to be an interactive session. We'll pause regularly for activities and discussions. But do not hesitate to interrupt us anytime for questions or comments. You can do this either by raising your virtual hand, or by using the chat. Unless you have connectivity issues, I'll ask you to keep your video on. But please stay on mute unless you're speaking.

00:05	3 	Today we will be talking about ‘Building trust in digital government’.
00:30	4 	At the end of this training session, you should be able to: ● Understand the common barriers and enablers to people’s trust in digital government ● Understand how to categorise data ● Understand the importance of privacy and global legal frameworks around it ● Apply basic cyber hygiene principles ● Explain the principle of security by design
00:40	5 	Let’s zoom in on today’s session. There are three main questions we’d like to cover: 1. What are the main barriers and enablers to people’s trust in digital government? 2. What are the global trends in data protection and why does it matters? 3. What can you do to improve cyber security? Any questions before we start?

1. Barriers and enablers to trust in digital government (60:00)		
a. Common barriers to trust in digital government (13:00)		
00:05	6 	Let's start then!
05:00	7 	**Group discussion** Why is trust important for digital government? Note: This could be a sli.do activity
00:30	8 	In the policy brief called "trust in public institutions: a conceptual framework and insights for improved governance programming", the UNDP defines trust. It says that trust is about people's belief that the way their government behaves will conform with a certain set of positive expectations in situations of uncertainty. Source: https://www1.undp.org/content/oslo-governance-centre/en/home/library/policy-brief--trust-in-public-institutions.html
01:00	9	While levels of trust in institutions vary significantly across countries, there has been a decline in trust in public institutions in recent decades. The Edelman 2022 Trust Barometer shows that only 52% of the global

		population trust their government to do what is right. The covid-19 crisis has exacerbated economic insecurity and perceptions of poor or corrupt government, further accentuating the decline in institutional trust. Rebuilding public trust in the light of the current crisis demands services that work for everyone and are more inclusive. Source: https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2021/08/PB_108.pdf https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022%20Edelman%20Trust%20Barometer%20Global%20Report_Final.pdf
01:30	10 	Trust in digital systems was put to the test during the pandemic. The covid-19 crisis sometimes forced some governments to take rushed decisions on the use of digital solutions - like contact tracing apps. As a result, there were concerns about people's human right to privacy. Governments cannot afford to lose people's trust in digital. The pandemic has shown how critical digital services are. Digital services need to embed the right to privacy into technological design. Source: https://www.uclg.org/sites/default/files/eng_briefing_technology_final_x.pdf
03:00	11 	Users' trust is important for the adoption of digital services. We saw very briefly in module 2 how design patterns can help strengthen users' trust in using online services. Today we will focus on other ways to encourage trust in sharing information online and using digital services.

		Before we look at enablers of trust, let's look at common barriers: ● **Lack of digital awareness**: some people fear using digital services because they don't want to venture into the unknown. ● **Bad experience of government, and especially of online services**: people's experience of public services influences their level of trust in new digital services. If they've had bad real life experiences with government organisations, they're likely not to trust them online either. And if their first online experience of public digital services does not go well, they can be reluctant to further use them. But this works the other way around too. If people are satisfied with public digital services, their level of trust in their government is likely to increase. ● **Fear of data breaches and cyber attacks**: ○ Without good data governance and stewardship, public organisations can unwillingly expose personal data, leading to breaches of privacy. This can deter people from using digital services. ○ But even with good governance and stewardship, personal data can be stolen or exposed in cyber attacks, which number is increasing. People may fear for their data, like credit cards' information. ● **Poor perception of government, and fear of governmental data abuse:** people can be reluctant to use digital services not just for cyber security reasons, or fear of accidental data breaches, but for fear

		of governmental 'abuse of data'. An abuse of data occurs when people's data is used for malicious purposes. For example, in dictatorship regimes, using people's data to identify political opponents, and curtail their freedom of speech. Or using people's data to discriminate against minorities, denying them access to public services on the basis of their religious belief or sexual orientation.
01:30	12 	Trust is easier to lose than to earn or restore, so preserving public trust has always been crucial for governments. This can be done through • Increased transparency and accountability (eg. sharing information about budget spending and public contracts awards) • Responsive, effective and inclusive service delivery • Enhanced citizen participation The way governments use data and technology can impact the level of trust people have in government, for better or for worse. If a government delivers user-centred, reliable services, and offers easy access to public information, then technology participates in building trust. On the other hand, poor online services or misuse of users' personal data, can deteriorate trust.
b. Building government digital services that are trustworthy (47:00)		
06:00	13 [redacted]	Let's watch a video that helps make the difference between trust and trustworthiness. Only show the first 6 minutes.

01:00	14 	As the video showed, a prerequisite to building trust is for governments to be trustworthy. This diagramme, inspired from the OECD 'data-driven public sector framework' summarises the main drivers of public trust in government. Governments need to: ● Deliver a good public service experience ● Adopt an ethical approach to building digital services and using data ● Protect the privacy of people's data, and ask for their informed consent before using their data for clear and pre-defined specific purposes. Data privacy is a fundamental human right. International treaties make it mandatory for governments to preserve it. ● Invest in cyber security and develop risk mitigation strategies to protect their users' data ● Be transparent and promote transparency
(i) User experience		
00:30	15 	Good user experience can help increase people's trust. The opposite is also true. Let's take an example.
02:00	16 	Have you ever seen this screen, after clicking on a link? This looks bad. Service users expect to be able to use public services online 24 hours a day, 365 days a year. Many users have limited choice over how and when they access government services. If a service is unavailable or slow, it can

		mean those users aren't able to get the help they need. Here's another example of a bad user experience that can undermine users' trust: if you are making a transaction online and you don't get any feedback at the end of the transaction on whether it was successful or not, you might click multiple times on the 'submit' button thinking that the transaction was not successful. That would result in multiple transactions being submitted and surely you wouldn't want to re-use such a service in the future. So a good user experience helps to create trust in the digital service.
(ii) Ethics		
01:00	17	Ethical digital services are designed to do no harm whether directly or indirectly. Ethical services offer the same experience to any user, whoever they may be. They don't discriminate against anyone. With the increasing use of data and automated decision-making algorithms, ethical concerns have grown. For example, in the United States, judges used a digital tool to help them assess the likelihood of recidivism of defendants, based on historic data patterns. The tool was based on algorithms that would give a recidivism probability score to defendants. Judges would then decide to hold defendants in prison or not while awaiting trial. It was found that this tool was biased against black people. Black people were twice more likely to be given a high score of recidivism for no reason. This is because the tool was fueled by historical data, which was itself biased against black people, due to a long history of racism and discremination in the country. This is an example of what ethical issues can look like, when building digital services. We will talk about data ethics in

		further detail in our next module.
(iii) Privacy and consent		
01:30	18 	The third ingredient for building trust in government digital services is protecting privacy and consent. In the digital era, there have been increasing opportunities for developing personalised services, tailored to our specific needs, based on our internet browsing habits. There is nothing wrong with this as long as people willingly agree to let organisations access the data they produce to provide them with a better service, or targeted ads. However there is an issue, if people's personal data are shared with organisations or used for purposes of which they are not aware, or have not consented to.
01:00	19 	This is the concept of data privacy. Data privacy is the right to have control over who can control your data, and for what purpose. Consent is when individuals whose data are being collected are aware of the purpose of the data collection and agree to give data about them for these purposes. We'll explore further the concept of privacy and global trends in this area later in this module.
02:30	20	In this blog post, Taiwan Digital Minister Audrey Tang talks about how to cater for privacy in service design.

		Audrey Tang's Office was involved in the design of an SMS contact tracing system during the covid-19 pandemic. To limit the transmission of the virus, they decided to quickly develop a contact tracing solution. But instead of centralising people's data or yielding control over people's data to multinational corporations, they worked with civic technologists. Together, they invented a contact tracing mechanism based on text messages (the 1922 SMS) which they managed to deploy within a week. By scanning a QR code with their phone's built-in camera and sending a toll-free text message, people could keep track of their itineraries. This allowed contact tracers to confirm the footprints of infected people and their contacts, without revealing any private information to venue owners. When contact tracers apply for information about specific phone numbers, they submit requests through this platform to browse them. The phone number holder could then reverse-audit contact tracers' requests and activities. All records were deleted after 28 days. Source: https://govinsider.asia/digital-gov/audrey-tang-digital-minister-taiwan-women-in-govtech-2021/
(iv) Security		
00:05	21 	The fourth enabler of trust in government digital services is security.

01:00	22 	Data security refers to the measures taken to prevent unauthorised access or use of data. It's the protection of devices, services and networks - and the information on them - from theft or damage. Security attacks can be extremely costly not only in terms of financial cost, but also in terms of reputation. Indeed, an organisation suffering from a data breach can lose its users' trust, same with governments. The prospect of digital security attacks which cripple infrastructure and damage the ability for people to access services is not a hypothetical risk, but a reality.
01:00	23 	In 2018, the personal records of 1.5 million patients were stolen by hackers in one the worst cyber attacks faced by Singapore so far. The hackers infiltrated the computers of SingHealth, Singapore's largest group of healthcare institutions with four hospitals, five national speciality centres and eight polyclinics. Prime Minister Lee Hsien Loong and a few ministers, had their outpatient prescriptions stolen as well. Source: https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most
01:00	24 	More recently in 2021, the Asian division of AXA was hit by a ransomware attack. Three terabytes of data were stolen and posted on the dark web. The dark web refers to encrypted online content that is not referenced by usual search engines and that requires specific software or browsers to access. It is used to keep internet activity private and anonymous and while some people use it for legal activities, the dark web is well-known to be used for illegal activities. Source: https://www.reuters.com/article/us-axa-cyber/axa-division-in-asia-hit-by-ransomware-cyber-attack-

		idUSKCN2CX0B0
04:00	25 	In general, cyber attacks occur in 4 stages: 1. **Survey** - investigating and analysing available information about the target in order to identify potential vulnerabilities. Attackers will use any means available to find technical or physical vulnerabilities which they can attempt to exploit. They will use scanning tools on social media and search engines to collect and assess any information about an organisation's computers, security systems and personnel. Attackers will also use social engineering (often via social media) to exploit user naivety and goodwill to phish for less openly available information. 2. **Delivery** - during the delivery stage, the attacker will look to get into a position where they can exploit a vulnerability that they have identified, or they think could potentially exist. Examples include: attempting to access an organisation's online services, sending an email containing a link to a malicious website or an attachment which contains malicious code, giving an infected USB stick away at a trade fair, creating a false website in the hope that a user will visit 3. **Breach** - exploiting the vulnerability/vulnerabilities to gain some form of unauthorised access. At this point, the attacker gains access to the system and is in a position to attack it. 4. **Affect** - carrying out activities within a system that achieve the attacker's goal. The attacker may seek to explore an organisation's systems, and establish a persistent presence by taking over a user's account. Determined and undetected attackers continue until they have achieved their end goals, which

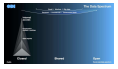
		may can include: ● retrieving information they would otherwise not be able to access ● making changes for their own benefit, such as creating payments into a bank account they control ● disrupting normal business operation, or deleting the whole operating system from users' computers We will be looking at the different types of common cyber attacks and simple steps that you can take to prevent them later in this module.
(v) Transparency		
01:00	26 	In the video we watched earlier, Onora O'Neill said that "trust requires an intelligent judgement of trustworthiness. So those who want others' trust have to do two things. First, they have to be trustworthy, which requires competence, honesty and reliability. Second, they have to provide intelligible evidence that they are trustworthy, enabling others to judge intelligently where they should place or refuse their trust." This reflects the importance of transparency for governments.

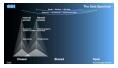
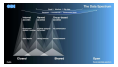
05:00	27 	As governments start integrating emerging technologies in their decision process, data used to feed into systems for instance AI algorithms are essential. However, people are not always informed about the data being used, how and by whom. People need to understand: ● For what purpose their data are being collected, analysed, stored and used so that they see the value created from their input ● Who uses their data, and is accountable for the way it used ● How their data are being used **For what purpose:** more and more, governments are trying out new technological approaches in service delivery. If done well, the use of technology like AI algorithms can indeed help optimise scarce resources. However, this must be done with the highest standards of transparency and accountability. Governments must be able to show the evidence of the positive impact of technology, how it benefits people. Currently, in most governments it is difficult to find out what algorithmic systems are used and where. This is a problem because it makes it impossible to get a true sense of the scale of algorithmic adoption in government and therefore to understand the potential harms, risks and opportunities with regard to public sector innovation. **How their data are being used:** this refers to the concept of explainability. Making algorithms transparent does not mean publishing the code behind them. Few people would be able to understand it. Making algorithms transparent means making it explainable so that anyone can understand how they work. For

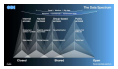
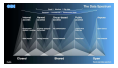
		example, if an algorithm is used to automate a decision that impacts whether someone's request for social housing is accepted or not, that person must be able to challenge and contest the decision. The algorithm should not be a black box that a layman cannot understand. People must be able to know how decisions are made. **Who uses their data:** this refers to the concept of accountability. Public accountability means that people or their representatives are able to exercise effective oversight and control over the decisions and actions taken by government organisations, in order to guarantee that government initiatives meet their stated objectives and respond to the needs of the communities they are designed to benefit. This extends to the use of third-party suppliers too. It is common that public bodies contract out third-party providers to deliver a service. If something goes wrong, the ultimate accountability should still sit with the public body. Public organisations must ensure that whoever gets access to public service users' data, they use it in a way that does not harm them and that is consistent with the purpose for which users agreed to give their data in the first place. **If their data was breached:** If their data has been breached, people must be informed immediately of the breach, as well as the actions that have been taken considering the situation.

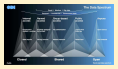
01:00	28 	Here is an example of a service that was developed with security in mind. Do you remember Singpass? SingPass is Singapore's national digital identity platform. It allows people to prove their identity and access government services. It was designed and developed using the following principles: ● Consent-based access ● Protecting data: Singpass recognises the importance of protecting users' data; it encourages the use of data in accordance with the applicable industry regulations and legislation ● Privacy conscious design ● Always-on authentication ● Interoperability: users can access both public and private sector services and transact securely, using different features of Singpass digital identity
01:00	29 	Trust is about doing the right things to secure and protect data but governments must also be ready for cyber attacks. Preparedness and incident response are as important as preventive cyber security measures. Governments must be prepared to respond to incidents and communicate about data breaches to users.
02:00	30 	The Okta incident is an example that shows that trust can be lost due to a lack of communication more than due to a breach itself. Okta provides user authentication services. In January, it experienced a data breach. But it was not until March 2022, when the hackers Lapsus claimed the incident and publicly shared evidence of the breach that Okta communicated about the breach to its customers. And even at that point which was two months after the incident, they could not confirm how many customers had been impacted by the breach. The

		CEO of Okta in an interview with Bloomberg confessed that the trust in their brand had been damaged by this incident. While the company is confident that the security risks related to the breach itself have been mitigated, it is far more difficult for them to restore the trust of their customers due to the lack of transparency and communication when the breach was uncovered in January and the gaps in their response to the incident. Source: https://www.bloomberg.com/news/articles/2022-04-04/okta-ceo-says-breach-is-big-deal-aims-to-restore-trust
15:00	31 	**Group discussion:** • What are the risks associated with the increased use of data in the public sector? • What do you think are the barriers to trust? (eg. lack of digital awareness, bad user experience, harmful use of data)
Break (05:00)		
2. Categorisation of data (25:00)		
00:05	32 	Let's move on to the second item on our agenda.
01:00	33	We've seen that in order to build trust, governments must be trustworthy and that they can do that by

		providing reliable services, using users' data ethically, being transparent about how they use people's data, protecting privacy rights and building secure digital services. In the rest of the session, we'll focus on two aspects of the trustworthiness framework we've just seen: data privacy and cyber security. How do you protect and secure people's data? Do you need to protect all types of data the same way?
00:30	34 	All types of data don't need the same level of protection or security. Categorising data helps: ● Understand what types of data you control ● What you are doing with this data ● How to protect this data
01:00	35 	The UK Open Data Institute has developed a tool called the 'data spectrum'. The 'data spectrum' categorises data from closed to open. Depending on where the data lies on this spectrum, it can be shared, or protected. This applies to government and non-government data.
01:30	36 	Let's start from the left-side of the spectrum which is 'closed'. At the closed end of the spectrum is data that is strictly confidential, and for internal use only (ie. not to be shared). This type of data should not be accessible to anyone unless they need it to do their job, for example payslips. Payslips need to be protected and only accessible to the employee and the person processing the payroll.

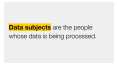
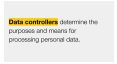
		Usually, data categorised as Closed should have the highest levels of security applied. Such data must be protected not only by limiting who can access it but also through policies or specific contractual obligations such as 'non-disclosure agreement' clauses.
01:30	37 	Moving slightly from the closed end of the spectrum to the right, comes data with named access. We're still dealing with confidential data here. Typically, for this type of data, access is given to specific persons for a specific purpose or limited duration. One example can be recruitment. There is a lot of personal and confidential data in applicants' CVs. This data can be shared with interviewers but it is usually restricted. For instance, let's say that you are on an interview panel for a particular role. You will typically be able to access information for: • applicants who applied for that role only and not for other roles • a limited amount of time which is usually the time for the interview and selection process to complete
02:00	38 	We now move to the middle of the spectrum which is 'shared data'. Shared data is not to be confused with 'public data'. Shared data is usually shared quite broadly within an organisation but not outside. Access to shared data is usually done through authentication as you still want to be able to track who can access the data even if it is shared. Let's take the example of an educational institution. Usually, several groups of employees (or users) within that institution would need access to student data. Student data may include personal information which is still confidential and should not be shared with external parties. However, this information will need to be shared

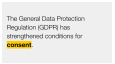
		with many different groups within the institution for them to do their job: teachers, administrative staff, finance etc. The information still needs to be secured and protected but not as strictly as Closed information. You still need to track who accesses the information so that you can take actions if something goes wrong.
01:30	39 	We now move to data that is shared publicly. Data with public access is not confidential and consists of data which you want to share with the public. However, the information might not necessarily be shared with anyone or you may not want everyone to re-use the data the way they want. One example is a Tweet. You can set your tweets to 'public' or you can protect them. If you protect them, only followers will be able to see them. Similar principles apply to other social media posts. Another example is pictures. You may share pictures publicly on a web site or on social media but you may not necessarily want people to re-use it or copy it without your permission.
01:00	40 	At the far end of the spectrum is 'open data'. Open data is data which is shared with anyone and that anyone can re-use, for example bus timetables, or the location of bus stops. We will look at 'open data' in further detail in our next module 'Data: uses, opportunities and risks'.
01:00	41 	**Group discussion** Think about your own organisation. 1. Locate your organisation's data on the ODI data spectrum. Try to find at least one data set for each category of the spectrum.

		2. What is your own assessment of how your organisation is protecting these different categories of data?
14:00	42 	I'll keep this slide up while you think of this.
3. Data Protection (01:25:00)		
00:05	43 	We'll now move to the third item on our agenda: 'data protection'.
00:25	44 	Data protection is often associated with data privacy but there are actually two components that contribute to data protection: data privacy and cyber security.

a. Data privacy (23:00)		
00:05	45 	We'll start with data privacy.
01:00	46 	Data privacy is not a new concept. The right to privacy is a human right which is part of the 1948 Universal Declaration of Human Rights (UDHR). Article 12 of the UDHR: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."
02:25	47 	However, in recent times, there have been several scandals of privacy breaches and a growing concern of seeing governments conducting mass surveillance. Have you heard about the Pegasus project? Pegasus is a phone hacking software that can gather data, location information, record video using a phone's camera, activate the microphone, take screenshots without the owner knowing. The worst is that it can infect a phone without its owner even clicking on an incoming call or message. NSO, the company who developed this software, claims that it has sold the software to 40 governments around the world for investigating terrorist or criminal activity. However, an investigation led by Amnesty International and Citizen Lab found that among the 50,000 victims targeted by Pegasus were journalists, pro-democracy activists or political opponents with no apparent link to criminality or terrorism. The

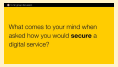
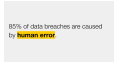
		US Department of Commerce has blacklisted the NSO group. The European Parliament has launched a committee of inquiry to investigate any cases of abuse by member states and the EU data protection watchdog is calling for a ban of Pegasus-like spyware. Sources: https://www.theguardian.com/news/2021/jul/23/pegasus-project-investigations-nso-spyware-mobile-phones https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/ https://euobserver.com/rule-of-law/154365
01:30	48 	With the exponential use of data, there have been increases in people's data misuse, mainly by private sector organisations. But data scandals have happened with public institutions as well. In the UK, details on about 1.6 million patients from a public hospital were provided to Google's DeepMind division during the early stages of an app test. The information was used to develop and refine an alert and diagnosis system that can spot when patients are at risk of developing acute kidney injury. The data transfer was part of the two organisation's partnership, but patients were not adequately informed that their data would be used as part of the test. Source: NHS illegally handed Google firm 1.6m patient records, UK data watchdog finds
01:00	49	The EU enacted the General Data Protection Regulation (GDPR) in 2018. It was seen as a major step forward in the protection of personal data. The GDPR applies to both public and private organisations, all across the EU,

		but it also pushed the data protection agenda forward in non-European countries. And non-European countries must comply with the GDPR when processing data of people located in the EU. The GDPR is about data protection, so, as we've seen, it's both about privacy and security. We'll cover security later. But before we go any further, let's start with some definitions to understand the concept of privacy.
00:30	50 	First, we must define a data subject. A data subject is simply a person whose data is being processed.
01:00	51 	Second, we must define a data controller. A data controller determines the purposes and means for processing personal data. Let's say you apply for insurance and you provide personal information to the insurance company for processing your application. In that case you are the data subject and the insurance company is the data controller.
01:00	52 	Another important concept that the GDPR defines is 'personal data'. Personal data can refer to anything that identifies a person including photographs, name and date of birth, home address, dependents, racial or ethnic origin, religious belief, health conditions, gender etc. Even the IP address of a user or cookies are considered to be personal data.

02:00	53 	One thing that the GDPR did was to strengthen the conditions for users to consent to their data being processed by data controllers. This means that organisations can no longer use the data of data subjects - the people whose data is being processed - if they have not been correctly informed of how that data is going to be used, and for what purpose, and agreed to it. Organisations have to ask data users in a straightforward way, and give them an easy way to say no, or withdraw their consent.
01:30	54 	The GDPR also has given extensive rights to data subjects, such as the: **Right to access** - right for data subjects to obtain confirmation from the organisation controlling their data as to whether or not personal data concerning them are being processed, where and for what purpose. If asked, the organisation controlling subjects' data shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects. Now, you can go on Facebook, and ask for the entire history of messages you sent, posts you liked, events you attended. It may take a while to download.
00:30	55 	**Right to rectification** - this is the right for individuals to amend inaccurate data and keep data up-to-date. They may do so directly or should at least have the possibility to request for their data to be amended.
01:00	56 	**Right to be forgotten -** also known as data erasure, entitles the data subject to request the organisation controlling his/her personal data to erase it. This is different from the right to rectification because here the records should be destroyed altogether as opposed to be amended. In some cases, the right to be forgotten should be considered in balance with the public interest. If a serial killer asks for a newspaper to erase an

		article about him/her, he/she will most likely see his/her request rejected.
00:30	57 	**Right to restrict processing** - individuals have the right to restrict the processing of their personal data if they believe the information is inaccurate, is being used illegally, or is no longer needed by the controller for the purposes claimed. Usually, restrictions are over a certain period of time only and not indefinite.
01:00	58 	**Data portability** - the right for a data subject to receive their personal data – which they have previously provided in a "commonly used and machine-readable format" and have the right to transmit those data to a third party. This right encourages free competition. So for example if you're not happy with your email service provider, you can easily extract your address book and mail history to use elsewhere, without losing anything.
01:30	59 	Breaches to the GDPR are taken very seriously and the fines can reach significant amounts. Some of the biggest GDPR fines include: ● Amazon for the amount of €746 million. In July 2021, the Luxembourg National Commission for Data Protection issued the biggest fine ever for the violation of the GDPR to Amazon. ● In September 2021, Ireland's data protection authority Data Privacy Commission issued a GDPR fine to WhatsApp Ireland amounting to €225 million after a 3-year investigation. ● In December 2021, the French data protection agency CNIL issued a €90 million fine to Google over the inability to allow youtube users in France to refuse cookies as easily as they could accept them.

00:30	60 	Most countries now have some form of data protection and privacy legislation although the degree to which these laws are stringent around the GDPR principles varies. 71% of countries have implemented legislation on data protection and privacy. 9% of countries have a draft legislation. However, legislation on its own is not enough. Governments need to think about data protection law enforcement. Very often, they lack the capabilities that are required to enforce legislation, and for it to be really effective. Governments should also think about how to integrate those principles and ideas when building digital services. Source: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
15:00	61 	**Group discussion:** 1. How would you assess your current services in terms of individual privacy rights that we discussed: a. Right to access b. Right to rectification c. Right to be forgotten d. Right to restrict processing e. Data portability

		2. What could be done better?
Break (10:00)		
b. Cyber security (50:00)		
00:05	62 	The last item on our agenda is cyber security.
05:00	63 	We discussed earlier that security is an essential enabler of trust. What comes to your mind if I ask you how you would secure a digital service?
01:00	64 	We have seen since the beginning of this training that teams and people are an essential component of digital. Similarly, cyber security is more than a technology problem. A recent study by Stanford University showed that human error is still the number one cause of data breaches. Not technology failure but human error. Professor Jeff Hancock who conducted this research explains the importance of understanding why people make mistakes, what causes human error so that organisations can take steps to prevent them.

		Source: https://www.tessian.com/research/the-psychology-of-human-error/
01:00	65 	Before we look at the different types of cyber attacks, let's first define what we mean by Information Security. Information Security is often defined using the CIA principles: C - confidentiality. We want information to be read and accessed only by the right people. I - integrity. We want information to be changed only by authorised people or processes. A - availability. We want information to be available for us to read and use whenever we want to.
00:30	66 	Cyber attacks aim at affecting one or more of the CIA principles. Some of the common types of cyber threats are: **1. Malware** Malware refers to malicious software designed to intrude into computer systems to harm or destroy them. Common examples of malware are viruses or trojan viruses.
01:00	67 	Emotet is an example of malware which has been very long lasting. It is a trojan that was first discovered in 2014 and it's only in 2021 that Europol managed to take it down. Emotet was delivered by emails that either contained a malicious link or attachment. If the victims opened the attachment or clicked on the link, the malware got installed. The computer then became vulnerable to other cyber criminals. Emotet is reported to have cost the US government up to $1 million **per incident** to remediate. Source: https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-

		emotet-disrupted-through-global-action
01:00	68 	**2. Ransomware** Second type of common cyber threat is ransomware. Ransomware is a form of malware that encrypts the victim's device so that the victim is no longer able to use it or access their data. The attacker then asks for a ransom but there is no guarantee that the data will be recovered even if the victim pays the ransom.
00:30	69 	One of the most widely known ransomware attacks was the WannaCry ransomware in 2017. It used a vulnerability in Microsoft Windows to attack computer systems. It is estimated that around 150 countries were impacted around the world and that it caused a loss of $4 billion across the globe. Source: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/
02:30	70 	**3. Phishing** We have seen earlier that many cyber security breaches do not result from technical failures. In fact, it is common for attackers to exploit the goodwill and trust of people to gain access to systems. This is known as 'social engineering'. For example, pretending to be technical support personnel and asking people for their usernames and passwords. Phishing is a common form of social engineering. Usually, the attacker will send an email to users to try to obtain information from them such as their login details or their bank account or credit card details. Phishing emails can use your real details and passwords to make you think that the attacker is a real contact that you

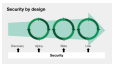
		already know, or to make you think that they have more information than they actually do to panic you into clicking on a message. One common example is to send an email telling the user that their account has been compromised including a link to confirm their username and password. When the user clicks on the link and enters their details, the attacker is able to obtain their information and hack into their account.
03:00	71 	This is an example of a phishing email. For laymen, it will seem to be a real email and it may be difficult to distinguish whether this is really from ebay. Some tips to recognise a phishing email: 1. A genuine email will never ask you to re-enter your login details if your account has been compromised. In general, if there is suspicion that your account has been compromised, a genuine email would warn you of the suspicious activity and when it occurred. It will tell you that if it was not you, you are advised to change your password. It will not provide you a link to do so but rather encourage you to login to the application and use the change password feature. It will also encourage you to report the breach. 2. Verify the email address of the sender. If it comes from a public email domain such as gmail.com or if the domain is misspelt e.g. faceebook instead of facebook, then it is likely to be a phishing email. Corporates would very unlikely use a domain that is public but have their own domain, e.g. undp.org 3. There are spelling or grammatical mistakes in the email. You don't have to be a cyber security expert to recognise a phishing email. It's more about being aware and being cautious. Additional reading: https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email

04:30	72 	What can you do to protect your information? 1. **Update software regularly.** It's human nature to keep postponing software updates as they pop up on our devices simply because that means disrupting our work or our activities but software updates are really important to keep your devices secure. They usually contain patches to vulnerabilities which have been detected and having an outdated software creates a vulnerability that hackers can use. 2. **Never open an email or attachment from an unknown sender.** Do not click links from unknown senders, and even think twice when they come from someone you know. If in doubt, do not click. 3. **Use strong passwords and where possible use multi-factor authentication.** Guidelines on strong passwords have changed over time. The US National Institute of Standards and Technology used to recommend using symbols, and changing passwords every 90 days. Not anymore. Because we're humans and we have trouble remembering numbers and symbols. So NIST now recommends passphrases, i.e. really long passwords. Many systems also use two-factor authentication now where there is another layer of authentication beyond entering the username or password. For e.g. by sending you a code by SMS or by sending a notification to the app on your phone to verify it's really you. 4. **Never send confidential information by email.** Many major webmail providers have suffered data breaches in recent years although now most have implemented two-factor authentication as an additional layer of security. If you don't have a choice, encrypt the information before sending by mail and send the password through another channel, e.g. text message.

		5. **Protect your devices with anti-virus software** and do not connect any external device without having scanned them for malware first. 6. **Check your security policy for accessing government information** and when in doubt consult a security expert. Most governments provide government emails to civil servants. If you have a government email, use it to access government information rather than personal emails. In case you have not been provided a government email, check what your security policy says about using personal emails or check with the cyber security team.
00:30	73 	What can governments do? **Increase cyber security awareness** At a preventive level, governments can raise cyber security awareness. October is globally recognised as the cyber security awareness month. Many countries around the world create communication campaigns that month to increase cyber security awareness.
01:00	74 	Another example is the 'My information is mine' campaign launched by USAID in Mongolia. The campaign raises awareness on cyber security through creative music. In collaboration with Mongolian pop artists Hishigdalai and Gangbay, the campaign released a rap song with messages about online privacy and cybersecurity embedded in a story about love and trust. Source: https://www.usaid.gov/regional-development-mission-asia/press-releases/feb-28-2022-usaid-

		launches-cybersecurity-awareness-campaign
01:00	75 	**Adopt a human-centred approach to cyber security** Security policies are important tools in preventing breaches. But we have seen earlier that human error is the most important cause of breaches and this only means that humans are the most important link in cyber security. Just like human-centred design helps to build better digital service, adopting a human-centred approach helps to design security policies and tools that work for people.
00:25	76 	The UK National Cyber Security Centre has published guidance around developing security that works for people and organisations. The guidance recognises that people shape security and therefore helps to develop a positive culture about security. Additional reading: https://www.ncsc.gov.uk/collection/you-shape-security Short video: https://youtu.be/QiCunzkr2CI
02:00	77 	**Build incident response capabilities** No matter how good your preventive measures are, breaches can occur. This is why having an incident response team and an incident response plan in place are extremely important. Governments need teams of experts that can monitor and respond to cyber incidents as they occur. Building incident response capability is as important as investing into preventive measures. The incident response plan provides guidelines on how an incident will be handled depending on its severity. One important aspect of this is the communication plan:

		who should be informed when there is an incident, how communication will take place and who is responsible for communicating information. Remember the Okta incident we talked about earlier and how lack of communication on cyber incidents can lead to distrust. Finally, it is also important to test it regularly through drills that simulate an incident and helps to test how teams respond to it and identify whether there are gaps in the incident response plan.
02:30	78 	More and more regional platforms of incident sharing and cooperation are coming to existence, which in itself is a recognition of the need for a transnational response to cybercrime. The Asia Pacific CERT (APCERT), for instance, is a coalition of CERTs and CSIRTs within the Asia-Pacific region. The organisation was established in February 2003 to encourage and support the activities of CERTs/CSIRTs in the region. APCERT maintains a trusted network of cyber security experts in the Asia Pacific region to improve the region's awareness of malicious cyber activity and its collective ability to detect, prevent and mitigate such activity through ● Enhancing the Asia-Pacific's regional and international cooperation on cyber security; ● Jointly developing measures to deal with large-scale or regional network security incidents; ● Facilitating information sharing and technology exchange on cyber security among its members; ● Promoting collaborative research and development on subjects of interest to its members; ● Assisting other CERTs and CSIRTs in the region to conduct efficient and effective computer emergency response; and ● Providing inputs and/or recommendations to help address legal issues related to cyber security and incident response across regional boundaries.

		Source:https://www.unapcict.org/sites/default/files/2021-11/Academy%20Module%20on%20Digital%20Government%20and%20Transformation_0.pdf
00:30	79 	We'll finish this session by introducing the concept of 'security by design'. A common misconception is that you can build a service and add security to it afterwards just like you can build a house and then add anti-burglar window bars. It doesn't work that way with security in digital services.
01:00	80 	So when do you need to think about security? Security is not an afterthought in digital. It has to be thought about in all the stages of the service development lifecycle. From the moment you are gathering requirements to when the service goes live, security needs to be integrated. We won't go into too much technical detail here but I just wanted to highlight that security is key to service design and forms an integral part of it. Guidelines and toolkits for developing applications that are secure by design can be found here: https://owasp.org/www-project-security-knowledge-framework/ Share the link.
04:30	81	What can service teams do to ensure they develop digital services that are secure by design?

		1. **Setup multi-disciplinary teams**. To make sure service teams take security into account when they develop digital services is to have information security experts as members of the team. That way, the team has the necessary skills to follow good practices and design secure services. It's important to have security experts involved in the creation of services from the beginning, to inform their development, rather than just at the end, for approval purposes only. For instance if you are designing a service for the Police department that involves lots of personal data, and if you are designing an open data service on sports facilities, the security requirements are different. It's important to capture this early on as it can impact how the service is built. 2. **Implement service standards**. Service standards help service teams design digital services in a consistent way. They offer guidance that help to promote best practice, stop bad habits and help digital teams build better services. Service standards often include security good practices to help government teams consider security at each step of the development of digital services. 3. **Involve multi-disciplinary teams in procurement**. You might not always be developing new digital services. You might need to buy digital services as well. Irrespective of that, governments need to maintain the same high level of security standards. The best way to ensure this is to have someone with the relevant skills in information security involved in the procurement process, whether it is for drafting specifications or evaluating solutions proposed. 4. **Test regularly**. Even after a service goes live, you are not done. You need to plan for regular security testing the same as you would regularly test the service for quality. This is because the threat

		landscape evolves very fast and you need to monitor that your digital services continue to be secure over time. Also, as you iterate the service and deploy new changes, you need to ensure that they remain secure.
15:00	82 	**Group discussion:** 1. What are the biggest challenges that you foresee in building trust in digital services in your context? 2. What are the quick wins and the next steps that you can take to make digital services more secure?
00:30	83 	**Takeaways:** ● Digital government can help build trust through increased transparency, enhanced citizen participation and responsive, effective and inclusive digital services. ● The dimensions of a trustworthy digital service are user experience, ethics, privacy, security and transparency. ● Data categorisation helps to assess the level of protection required for different types of data.
00::30	84 	● Data privacy is a fundamental human right which all digital services should respect and protect. ● Governments have an important role to play in improving cybersecurity by increasing awareness, designing human-centred security policies and building incident response capability. ● Security is not an afterthought and must be included in all stages of the service development lifecycle.
	85	Next session: ‘data: uses, opportunities and risks’.