Transcript | Global Lessons in Digital Resilience

1
00:00:11.900 --> 00:00:26.930
C -: Hello, everyone, and welcome to this event on digital resilience, part of the World Bank's Tokyo Digital Academy program, supported by apolitical. My name is C -, and I'm a Y here at Apolitical.

2
00:00:27.240 --> 00:00:34.480
C -: It'd be great to hear from all of you. So do post in the chats where you're joining us from in the world. And what organization you work for

3
00:00:34.750 --> 00:00:39.530
C -: today. We'll be exploring case studies of digital resilience from Japan and Singapore

4
00:00:39.840 --> 00:00:44.600
C -: before heading into an expert panel, discussion with speakers from all around the world

9
00:01:48.070 --> 00:02:04.969
C -: So I'm delighted now to hand over to our partners at the World Bank Group. We're very lucky to have M here. The Global Director of Urban Resilience and Land Global Department at the World Bank Group, who will give a couple of minutes of opening remarks for us.

10
00:02:07.090 --> 00:02:08.409
M: Thanks a lot, C.

11
00:02:08.520 --> 00:02:18.700
M: Good morning. Good afternoon. Good evening. To everyone who joined us. It is a pleasure for me to open today's seminar on global lessons in digital resilience

12
00:02:18.990 --> 00:02:27.400
M: hosted by the Digital Transformation Global Department of the World Bank and the Tokyo disaster risk management Hub.

13
00:02:27.550 --> 00:02:37.590
M: which sits under the World Bank's global facility for disaster, risk, disaster, reduction, and the recovery which we call Gfdr.

14
00:02:38.980 --> 00:02:50.950
M: As you know, disasters, whether from natural hazards or man-made threaten development gains weaken economies, and often hit the most vulnerable, the hardest.

15
00:02:51.110 --> 00:02:56.830
M: As disaster risks escalate in both frequency and intensity.

16
00:02:57.120 --> 00:03:00.360
M: We must find new ways to strengthen resilience.

17
00:03:00.680 --> 00:03:05.700
M: Digital technologies are becoming an important part of this effort.

18
00:03:05.930 --> 00:03:09.140
M: Early warning systems risk mapping

19
00:03:09.520 --> 00:03:18.370
M: and emergency response systems are helping countries prepare better, respond faster and recover more effectively.

20
00:03:19.110 --> 00:03:21.599
M: Resilience does not happen by chance.

21
00:03:21.740 --> 00:03:29.290
M: Digital infrastructure and services must be designed to withstand shocks, redundancy.

22
00:03:29.460 --> 00:03:35.300
M: reliability, and the continuity need to be built into the system we rely on.

23

00:03:35.420 --> 00:03:38.970
M: not as afterthoughts, but from the beginning.

24
00:03:39.900 --> 00:03:47.949
M: Every dollar invested in resilient infrastructure can generate up to $4 in returns.

25
00:03:48.100 --> 00:03:51.919
M: protecting livelihoods and support fast recovery.

5
00:01:29.180 --> 00:01:39.730
C -: Okay, so I'm very delighted now to hand over to our 1st speakers. We have from the Nomura Institute.

6
00:01:40.320 --> 00:01:47.550
C -: and that is T and G.

7
00:01:48.010 --> 00:01:49.109
C -: Please go ahead.

8
00:01:51.050 --> 00:01:54.380
G: Yeah, thank you, C. I'm projecting my material.

9
00:01:59.290 --> 00:02:01.409
G: Can you see the material right now?

10
00:02:04.480 --> 00:02:05.210
C -: We can see it.

11
00:02:05.710 --> 00:02:07.500
G: Yeah, thank you. C.

12
00:02:07.630 --> 00:02:35.880
G: So Hi, everyone. My name is G. Nri, I usually welcome supporting the formulation of digital poetry and assisting private sector companies in leveraging digital and AI technologies today on

behalf of Nri. T and I will be speaking about the use of digital technologies in disaster, management, and resilience in Japan. So, T, could you please briefly introduce yourself.

13
00:02:37.070 --> 00:02:47.509
T: Okay. Hi, my name is T from Nomara Research Institute. I'm mainly involved in new business development and demonstration project support in Digital field.

14
00:02:48.250 --> 00:02:54.169
T: I'm particularly experienced in business related to remote sensing data such as cataract data.

15
00:02:56.960 --> 00:02:59.370
G: Thank you. So now let's get started.

16
00:03:00.880 --> 00:03:19.179
G: Okay, first, st let me give you an overview of disaster impacts in Japan. According to data from the Undrr. Japan ranked 3rd in the world in terms of economic losses caused by disasters over 20 year period.

17
00:03:20.020 --> 00:03:23.540
G: As many of you know, Japan is highly disaster prone.

18
00:03:24.820 --> 00:03:34.959
G: and more recently, the 2024 Noto Penisha earthquake which occurred in Ishikawa Prefecture in Japan, caused significant damage with

19
00:03:35.100 --> 00:03:37.820
G: over 400 authorities.

20
00:03:39.320 --> 00:03:49.480
G: So given these situations, both the public and private sectors in Japan have been accelerating digitalization for disaster, preparedness and response.

21
00:03:53.220 --> 00:03:55.509
G: The use of additional technology is

22
00:03:55.610 --> 00:04:01.920
G: indispensable for addressing the challenges faced by stakeholders during disasters.

23
00:04:02.230 --> 00:04:16.649
G: For example, government agencies are required to rapidly evacuation information as a disaster approaches, and in the recovery phase they are tasked with damage assessments and

24
00:04:16.820 --> 00:04:18.750
G: distortion activities.

25
00:04:18.890 --> 00:04:27.830
G: Meanwhile disaster victims face challenges, such as a lack of information and difficulty making decisions.

26
00:04:28.000 --> 00:04:34.049
G: These technologies are highly useful and indeed essential in addressing these issues.

27
00:04:35.480 --> 00:04:46.710
G: So this is agenda for our presentations, we will present how digital technologies are being utilized in Japan's digital management categorize categorizing into

28
00:04:46.840 --> 00:04:49.770
G: 3 key areas based on their effectiveness.

29
00:04:50.140 --> 00:04:55.960
G: So T, could you please explain the topic 1st and second, thank you.

30
00:04:56.780 --> 00:04:57.600
T -: Okay?

31
00:04:58.260 --> 00:05:04.180
T -: And now I'd like to introduce the issues, solutions, and important points for each topic.

32

00:05:04.540 --> 00:05:08.100
T -: First, st we will discuss disaster, victim management.

33
00:05:08.360 --> 00:05:10.500
T -: This slide, provide a summary

34
00:05:10.710 --> 00:05:18.340
T -: in disaster, victim management. It is difficult to integrate various databases and identify individual victims.

35
00:05:18.760 --> 00:05:23.080
T -: I will introduce 2 case studies to address these issues.

36
00:05:23.540 --> 00:05:26.639
T -: Finally, I will summarize the important points.

37
00:05:29.200 --> 00:05:34.199
T -: First, st I will explain what the disaster victim management system should look like.

38
00:05:34.740 --> 00:05:41.810
T -: There are 2 key points, centralized information management and privacy and data security

39
00:05:42.980 --> 00:05:52.180
T -: disaster, eviction management involves various type of information, such as resident information building information and damaged datas.

40
00:05:53.900 --> 00:05:57.590
T -: If this information is scattered across multiple systems.

41
00:05:57.800 --> 00:06:01.950
T -: it becomes difficult to retrieve the necessary information smoothly.

42
00:06:02.360 --> 00:06:07.770
T -: Therefore, centralized information management is particularly important.

43
00:06:08.500 --> 00:06:13.030
T -: By doing so it will help ensure the safety of victims.

44
00:06:16.200 --> 00:06:18.859
T -: This slide explains 2 main issues.

45
00:06:19.080 --> 00:06:22.999
T -: The 1st is ensuring system interoperability.

46
00:06:23.310 --> 00:06:32.929
T -: In most cases the necessary information is scattered across multiple databases, so it is necessary to integrate them smoothly.

47
00:06:33.610 --> 00:06:37.809
T -: In doing so it is important to ensure interoperability.

48
00:06:38.880 --> 00:06:45.699
T -: The second issue is establishing a means of identifying victims in times of disaster.

49
00:06:45.950 --> 00:06:51.869
T -: It is difficult to identify victims because many people don't carry identification with them.

50
00:06:54.590 --> 00:07:01.179
T -: Here I introduce entity solution that enables centralized information management.

51
00:07:01.690 --> 00:07:07.170
T -: This solution integrates various disaster, related information into a single database

52
00:07:08.180 --> 00:07:17.659
T -: victim can quickly obtain disaster certificates and receive insurance payments promptly in a typhoon disaster.

53

00:07:18.110 --> 00:07:25.769
T -: Over 80% of the victims were able to obtain disaster certificates within one month after the disaster.

54
00:07:28.270 --> 00:07:31.009
T -: This is a screen image of the solution.

55
00:07:31.250 --> 00:07:37.030
T -: You can specify the area you want to check on the map and view information about that area.

56
00:07:40.930 --> 00:07:47.620
T -: The second case study is partner identification using transportation. IC. Cards by Jr. East.

57
00:07:48.850 --> 00:08:01.970
T -: first, st transportation cards are distributed to victims, and when they go to evacuation centers or receive relief supplies, they hold their cards over a card reader to identify themselves.

58
00:08:02.600 --> 00:08:08.670
T -: This system was actually used during the 2024 Noto Peninsula earthquake.

59
00:08:09.590 --> 00:08:15.000
T -: By the way, Japan has a partner identification number system called my number.

60
00:08:15.300 --> 00:08:21.620
T -: and it was originally expected that my number would be used for identification in disasters.

61
00:08:22.290 --> 00:08:31.700
T -: However, few people actually carried their my number cards with them during the evacuation, so the transportation cards served as an alternative.

62
00:08:33.169 --> 00:08:36.910
T -: At this end of the topic I will summarize the key points.

63

00:08:37.419 --> 00:08:48.739
T -: As mentioned earlier. Interoperability and personal identification are important, and it is essential to develop the necessary digital infrastructure for this purpose.

64
00:08:49.480 --> 00:08:53.180
T -: On the other hand, a disaster could happen today.

65
00:08:53.610 --> 00:09:00.909
T -: Therefore, it is important to build the management system depending on the current state of digital infrastructure.

66
00:09:01.390 --> 00:09:08.719
T -: This ensures that disaster victim management can be carried out effectively. Even if a disaster happens today.

67
00:09:09.450 --> 00:09:17.790
T -: this slide provides examples of your next actions that should be taken depending on the current state of digital infrastructure.

68
00:09:18.630 --> 00:09:23.460
T -: For example, if there are no optional partner, identification means

69
00:09:23.940 --> 00:09:29.210
T -: it is important to prepare an alternative. Using de facto standard means.

70
00:09:30.320 --> 00:09:32.520
T -: We will now conclude this topic.

71
00:09:35.870 --> 00:09:40.359
T -: Next, I would like to talk about assessing disaster situations.

72
00:09:41.460 --> 00:09:43.380
T -: This thread is a summary.

73

00:09:43.890 --> 00:09:47.339
T -: In order to assess a disaster situation.

74
00:09:47.490 --> 00:09:51.439
T -: it is necessary to integrate cross organizational data.

75
00:09:52.630 --> 00:09:58.179
T -: However, in many cases cross organizational cooperation isn't working well.

76
00:09:59.850 --> 00:10:05.130
T -: in this topic I will introduce 2 case studies and summarize the key points.

77
00:10:08.400 --> 00:10:12.829
T -: First, st I will describe the role of disaster, situation, assessment.

78
00:10:14.360 --> 00:10:20.479
T -: The general process consists of data, collection, data, analysis and decision-making support.

79
00:10:21.490 --> 00:10:24.030
T -: There are important points at each step.

80
00:10:24.950 --> 00:10:30.350
T -: and it is important that operations run smoothly throughout the entire process.

81
00:10:31.600 --> 00:10:34.589
T -: This enables the quick safety of victims.

82
00:10:37.600 --> 00:10:40.029
T -: This thread explains 2 main issues.

83
00:10:40.370 --> 00:10:43.980
T -: The 1st is cross-organizational data integration.

84
00:10:44.460 --> 00:10:53.239
T -: In recent years there are many data sources available, such as satellites, drones, social networking service, and CCTV.

85
00:10:53.580 --> 00:11:01.400
T -: By integrating data across organizations, you can understand the overall picture and details of the damage.

86
00:11:02.380 --> 00:11:09.290
T -: The second issue is ensuring the effectiveness of operations during disasters.

87
00:11:09.400 --> 00:11:11.749
T -: Unexpected problems may arise.

88
00:11:12.240 --> 00:11:19.910
T -: It is essential to identify potential problems in advance by simulating disaster. Scenarios at the operational level.

89
00:11:21.070 --> 00:11:23.680
T -: Here are 2 use case case studies.

90
00:11:24.850 --> 00:11:29.480
T -: First, st inspect this crisis visualization system.

91
00:11:30.770 --> 00:11:35.919
T -: Information from satellites, vehicles, and other sources is integrated.

92
00:11:36.380 --> 00:11:44.589
T -: Then, using AI technology, it assesses the current disaster situation and makes prediction for the future.

93
00:11:45.570 --> 00:11:48.860
T -: This crisis information is deployed on the map.

94
00:11:51.790 --> 00:11:59.190
T -: The next case study is an optimization of drainage, pump truck placement based on Jaxa satellite data.

95
00:12:00.630 --> 00:12:04.590
T -: Flooded areas were identified by analyzing satellite data.

96
00:12:05.410 --> 00:12:08.689
T -: The image on the left is an actual satellite image.

97
00:12:08.820 --> 00:12:12.520
T -: and the image on the right shows the flooded areas.

98
00:12:12.820 --> 00:12:21.010
T -: I read it improve a disaster situation. Report can be provided 2 h after satellite observation

99
00:12:21.820 --> 00:12:26.259
T -: based on this report drainage pump trucks can be optimally placed.

100
00:12:29.940 --> 00:12:33.249
T -: As you know, satellites are important data source.

101
00:12:33.540 --> 00:12:38.159
T -: but during disasters it may not work smoothly.

102
00:12:38.680 --> 00:12:47.019
T -: Therefore Jaxa conducted disaster with many private companies and central government agencies.

103
00:12:48.130 --> 00:12:53.730
T -: The entire process from observation request to information provision was carried out.

104
00:12:54.890 --> 00:12:57.349

T -: This story revealed some programs.

105
00:12:58.010 --> 00:13:04.240
T -: For example, it was pointed out that it would be better to provide information sooner

106
00:13:05.750 --> 00:13:09.720
T -: by taking measures against such programs. In normal times

107
00:13:10.330 --> 00:13:14.650
T -: effective operations can be carried out in the event of a disaster.

108
00:13:17.420 --> 00:13:21.509
T -: These are the satellite operators which participated in this tutorial.

109
00:13:21.770 --> 00:13:24.859
T -: They include both public and private sectors.

110
00:13:31.670 --> 00:13:36.719
T -: These are the analysis companies that participated in this story.

111
00:13:36.900 --> 00:13:38.650
T -: There are 10 in total.

112
00:13:42.140 --> 00:13:45.790
T -: At the end of this topic I will summarize the key points.

113
00:13:46.510 --> 00:13:52.349
T -: The the point is that although there are many data sources available in recent years.

114
00:13:52.770 --> 00:13:57.620
T -: It is not always possible to utilize them effectively during a disaster.

115
00:13:58.240 --> 00:14:08.019

T -: So it is important to conduct disaster stories during normal times to confirm operational procedures and identify unexpected programs.

116
00:14:08.600 --> 00:14:12.940
T -: This slide raises several examples of unexpected programs

117
00:14:13.810 --> 00:14:22.210
T -: by resolving these problems in advance. It will be possible to assess the disaster situation smoothly during the disaster.

118
00:14:23.110 --> 00:14:25.489
T -: We will now move on to the next topic.

119
00:14:27.830 --> 00:14:29.655
G: Okay, thank you. Take hold.

120
00:14:30.300 --> 00:14:46.679
G: The 3rd topic is on improved soundness of information space. So this slide provides a summary. I will explain how to maintain soundness and robustness of the information. Space and the information flow in the event of a disaster

121
00:14:48.980 --> 00:15:00.769
G: in the event of disaster. Victims receive emergency alerts, evacuation, information, infrastructure, information and other information, and and they make decisions.

122
00:15:01.020 --> 00:15:10.259
G: So in this situation, it is extremely important that the information space is sound, meaning that the right information reaches the right people.

123
00:15:11.750 --> 00:15:27.270
G: However, as you know, the spread of false information and information that is difficult to verify is a global issue in Japan, for example, false rumors that crimes committed by foreigners are spreading

124
00:15:27.390 --> 00:15:31.849

G: that that spread, and nearly 90% of people believe them.

125
00:15:35.230 --> 00:15:39.469
G: There are psychological and sociological factors behind the phenomenon.

126
00:15:39.570 --> 00:15:48.959
G: Psychologically, anxiety caused by disaster is considered to be an important factor contributing to the spread of false information.

127
00:15:49.150 --> 00:15:57.060
G: Sociologically, the spread of false information is seen as a reaction by people caught up in ambiguous situations.

128
00:15:57.230 --> 00:16:03.299
G: This shows that the spread of false information is not limited to Japan, but this is a global issue.

129
00:16:06.740 --> 00:16:13.559
G: So the 1st solution to this 1st solution to this issue is disaster activation, chat, board.

130
00:16:14.170 --> 00:16:33.889
G: research and development and social implementation are being promoted by the Sip National Project, led by the Cabinet office in Japan, which will enable both disaster victims and government agencies to correct information in a sophisticated and robust manner.

131
00:16:35.610 --> 00:16:57.390
G: First, st disaster victims can receive individually optimized information through Ryan Ryan is the most widely used Chatbot in Japan. For example, if you send a chat message, saying there's a fire that Chatbot will confirm the necessary information and send out evacuation information for him or her.

132
00:17:00.010 --> 00:17:06.780
G: Another major feature is that it offers significant benefits to the Government Government.

133
00:17:07.400 --> 00:17:20.409

G: Information information entered by disaster victims is sorted by AI and displayed on maps used by the fire and disaster, management, agency, and other government agencies.

134
00:17:20.650 --> 00:17:27.399
G: so thereby improving the efficiency and sophistication of this queue operations.

135
00:17:30.510 --> 00:17:41.960
G: In this way disaster victims and government agencies can exchange information in both directions, thereby improving the flow of information and make it more efficient.

136
00:17:42.090 --> 00:17:49.440
G: This is a meaningful initiative, and many users responded that it was useful in a demonstration experiment.

137
00:17:50.430 --> 00:18:00.770
G: On the other hand, in order to implement this system on the wider scale, data, standardization and other measures will continue to be required.

138
00:18:03.280 --> 00:18:08.360
G: Another solution here is fast around from media Company J express.

139
00:18:08.510 --> 00:18:19.079
G: This solution uses social media and new news apps as a source of information removes noise such as fake news or fake news, or

140
00:18:19.300 --> 00:18:28.980
G: on Deepfake like that, using AI and shares the information with Government agencies, thereby contributing to the Hershey for the information.

141
00:18:30.600 --> 00:18:42.899
G: So these solutions contribute to the dissemination of information, free of force and misleading information, and partially contribute to the resolution of these kind of issues.

142
00:18:45.380 --> 00:18:50.770
G: Okay, finally, here are the key takeaways from this presentation from us.

143
00:18:52.270 --> 00:19:12.110
G: 1st regarding topic, one enhanced management of disaster victims by advancing the development of disaster victim management in accordance with the digital infrastructure status of each country, we can create disaster prevention measures that leave no one behind.

144
00:19:14.080 --> 00:19:31.029
G: Next, regarding topic 2 advanced disaster situation, assessment as a variety of data sources that can be utilized increases. It is important to prepare for the implementation in advance from the normal times.

145
00:19:32.680 --> 00:19:39.660
G: Finally, regarding topic 3 improve soundness of the information space.

146
00:19:40.190 --> 00:19:53.999
G: The key takeaway is that not only delivering reliable information to disaster victims, but also incorporating the information they provide into administrative decision-making process

147
00:19:54.140 --> 00:19:59.920
G: contribute to a more robust information space.

148
00:20:02.190 --> 00:20:21.629
G: So we plan to publish a more detailed report on the use of digital technology in the field of disaster, prevention, and resilience in Japan as we introduced here, and the report is scheduled to be released by the World Bank in July or later. So please keep an eye out for it.

149
00:20:21.760 --> 00:20:26.649
G: Okay, that's that, concludes Nri's presentation. Thank you very much for your attention.

150
00:20:28.810 --> 00:20:36.859
C -: That's lovely. Thank you, G and T. Those insights are really incredible. It seems like an exhaustive report, and we look forward to reading that in July

151
00:20:36.970 --> 00:20:45.479

C -: I'm going to move us quickly on to our 2 other case, studies another from Japan, and then a final presentation from Singapore

152
00:20:45.570 --> 00:21:12.620
C -: to deliver those I will hand the stage to Mr. Y -, director of the Disaster Management Office from the Ministry of Land Infrastructure, Transport, and tourism, and then we'll hear from H. Meng, Cha, the director of Govtech Singapore. Mr. -'s remarks will be translated into English by an interpreter. Live in the session, so please proceed with your intervention. Now, Mr. -.

153
00:21:16.470 --> 00:21:17.245
Mr Y -: Oh!

154
00:21:26.190 --> 00:21:27.772
Mr Y -: Coming to the.

155
00:21:28.540 --> 00:21:30.010
HH -: Can you see my screen.

156
00:21:30.230 --> 00:21:31.009
C -: We can.

157
00:21:31.250 --> 00:21:32.529
HH -: Hi mia!

158
00:21:33.170 --> 00:21:42.830
Mr Y -: Like er.

159
00:21:42.830 --> 00:21:45.610
HH -: Thank you very much for the introduction. My name is Kuriama.

160
00:21:46.700 --> 00:21:53.120
Mr Y -: A technical emergency control force, mesh, mass.

161
00:21:53.390 --> 00:21:57.559

HH -: 1st of all, I would like to explain what technical emergency control force is

162
00:22:06.840 --> 00:22:16.720
HH -: in a disaster, a large scale, natural disaster, affected area. It is necessary to promptly restore infrastructure facilities.

163
00:22:18.120 --> 00:22:27.990
Mr Y -: Yeah.

164
00:22:28.450 --> 00:22:45.959
HH -: So technical emergency control force is a team that is dispatched by the Ministry of Land infrastructure, transport, and tourism to make an assessment to the on the extent of damages caused by natural disasters for the purpose of rapid restoration of infrastructure facilities.

165
00:22:47.870 --> 00:22:52.750
Mr Y -: So kai shimas.

166
00:22:52.930 --> 00:23:00.340
HH -: Now, I would like to introduce you to the an application that supports the activities of techforce.

167
00:23:01.880 --> 00:23:07.830
Mr Y -: The.

168
00:23:08.520 --> 00:23:15.509
HH -: So the activities of techforce includes a survey on-site survey and preparation of reports.

169
00:23:16.610 --> 00:23:28.120
Mr Y -: Hi masu.

170
00:23:28.490 --> 00:23:38.469
HH -: So what they do is they travel in the affected area to take measurements and to draw sketches, and also to take many photographs.

171

00:23:39.950 --> 00:23:51.910
Mr Y -: Maesta.

172
00:23:52.230 --> 00:24:13.950
HH -: So in the past, after the members of the Tech force complete their field survey, they bring back all the data they have collected during the survey to their base, and go through the data they have collected, and also and put together a report for the purpose of restoring infrastructure as soon as possible.

173
00:24:15.150 --> 00:24:20.320
Mr Y -: T.

174
00:24:21.040 --> 00:24:30.230
HH -: So what they had to do in the past was, that was after a very tiring field survey. They had to put together a report.

175
00:24:30.490 --> 00:24:38.830
Mr Y -: Sagemonodesta.

176
00:24:39.670 --> 00:24:48.800
HH -: So this type of work resulted in long working hours of the staff with a huge amount of workload.

177
00:24:49.870 --> 00:24:58.170
Mr Y -: Shi maesta.

178
00:24:58.740 --> 00:25:10.030
HH -: So the for the purpose of making their work more efficient, and to reduce the workload, we have started developing a tech force tech application

179
00:25:22.350 --> 00:25:36.809
HH -: in the tech app. All the data that were collected in the during the field survey were sent or stored in the cloud system, and all the data on the cloud system can be shared by all of the people involved.

180

00:25:37.930 --> 00:25:43.500
Mr Y -: The.

181
00:25:44.200 --> 00:25:53.719
HH -: And by directly storing the data to Techapp, the organizing of the photos. And the data has become easy.

182
00:25:54.990 --> 00:26:09.220
Mr Y -: Masta.

183
00:26:10.430 --> 00:26:31.020
HH -: And, furthermore, since all the data collected during the field survey can be shared by the people working in the office through the cloud system. So, therefore, outdoor work, which is field survey and the compilation of the report which is the back office work, can be conducted in parallel.

184
00:26:45.760 --> 00:26:58.969
HH -: so, as a result of the app development. The work of the tech force has become more efficient, and the workload of the members of the tech force has significantly be reduced

185
00:27:04.790 --> 00:27:08.989
HH -: to conclude my presentation. Thank you very much for your kind attention.

186
00:27:12.920 --> 00:27:14.859
C -: Thank you very much, Mr. Kuryama.

187
00:27:16.640 --> 00:27:32.179
C -: that's wonderful. And thank you, HH, as well for the translations. We'll probably need you again for the question. Sessions. I would like to pass immediately, please to Ho -, from Singapore, who, we will present, slides on his behalf. I believe.

188
00:27:32.470 --> 00:27:34.109
C -: to present case study.

189
00:27:35.250 --> 00:27:38.590

H: I actually, I think I should be able to drive it. Let me let me give it a go.

190
00:27:38.990 --> 00:27:39.590
C -: Okay.

191
00:27:44.020 --> 00:27:46.629
H: Let me know if everyone is seeing the slides.

192
00:27:46.630 --> 00:27:48.929
C -: We can see your screen sharing.

193
00:27:49.380 --> 00:27:56.590
H: Great and try to get oops. I'll try to get into presentation mode. Sorry?

194
00:28:07.350 --> 00:28:15.010
H: Oh, jeez, alright. Okay, is it still? Okay? Everyone can see.

195
00:28:15.297 --> 00:28:17.600
C -: We can see that H-. Please go ahead.

196
00:28:17.600 --> 00:28:32.221
H: Okay, thanks. So much. So good evening, everyone. So again, thanks to World Bank and apolitical for having me on this webinar. So I'm gonna be talking about a softer topic than the previous 2 presentations. And this is around the shared responsibility model, and

197
00:28:32.550 --> 00:28:54.679
H: how the Singapore government is trying to move towards that, especially when it comes to digital resiliency in the cloud. So a short introduction. So my name is Ho -. So I'm director of core engineering products at Govtech, Singapore. So our group basically works on engineering products and tools to help other government developers as well as the vendors that work on government projects. So cloud hosting is one of the

198
00:28:54.800 --> 00:28:58.830
H: components within tools and components within my group.

199
00:28:59.790 --> 00:29:24.619
H: So I'll start with this 1st slide. And actually, this 1st slide is not meant to be kind of read. I kind of want to portray that when it comes to resiliency that there are so many things that we really need to think about. Like, you know, we have to think about people, the knowledge and the mindset. You know whether people are thinking and designing in resilient manners. We need to also have processes. And that leads to better incident management

200
00:29:24.620 --> 00:29:35.879
H: and best practices. Technology which I mentioned before. That's 1 of the things that my group does. Do. We have platforms, for example, and also do we? Are we thinking about concentration risk

201
00:29:35.880 --> 00:29:37.210
H: apologies? That's not

202
00:29:38.300 --> 00:29:58.719
H: sorry. Excuse me. Yeah, let me continue. So. Are we thinking about concentration, risk, and all that when we design our platforms and infrastructure? Then, lastly, we have how the industry kind of partakes in digital resiliency. So where trust and partnerships are concerned, you know, do we have trustworthy vendors to have trustworthy tech partners to provide the resiliency that we need.

203
00:29:58.720 --> 00:30:24.739
H: Then, lastly, I'm sure many governments out there are also thinking about Black Swan events in the event that something really bad happens, and you have to move out to the cloud and what options are available. So there's a lot of things to consider. So I'm not going to with my 8, 10 min. I'm not going to talk about all of them. So today I'm going to focus on the highlighted portion in red, which is about establishing a shared responsibility model. When we work with

204
00:30:24.740 --> 00:30:44.690
H: vendors and technology partners within the government. I selected this topic because I felt that a lot of the things that we can achieve by having a shared responsibility. Way of thinking actually helps in all the other areas as well. So I'll try to talk through some of these. And of course, if you have questions and all that, please feel free to stop me.

205
00:30:45.600 --> 00:30:59.629

H: So what is the shared responsibility model. Actually. So I I firstly, this is not a new concept. It's not something that I coined up, or the Singapore Government coined up. Actually, a lot of the Cloud Service. Providers already advocate this model when they deal with their commercial partners.

206
00:30:59.940 --> 00:31:21.210
H: But I think in the public sector this mindset is Southern practice, and I think it is also probably, or even absent sometimes, and it is probably because there's a there's a longstanding, traditional approach of, you know, clearly separating and assigning who's responsible for what? Which probably had an unintentional side effect of

207
00:31:21.380 --> 00:31:33.960
H: making the way that we build and run. It projects very, very siloed and and and then therefore then we would assign blame sometimes, in a very cruel and unnecessary in a blunt fashion. So

208
00:31:34.220 --> 00:32:00.059
H: what we really need to do is to actually start thinking about shared responsibility across all levels of involvement when it comes to it projects. So what what do I mean by that? So you see a couple of circles here, and then there's a little overlap portion that says shared responsibility. It's the same for all the for all the circles. So for where agencies are concerned, the agency's own internal teams that you know, build their pro, build, their products, and build their projects

209
00:32:00.060 --> 00:32:23.569
H: need to have some form of shared responsibility with the vendors and the contractors that are working on them, and then, between agencies and digital between the agencies and digital enabling agencies like Govtech, for example, right? There also needs to be a shared responsibility, because Govtech is the one that's providing some of the digital platforms and tools that these agencies rely on.

210
00:32:23.750 --> 00:32:46.602
H: Then, where the larger government is concerned, there also needs to be shared responsibility between the technology partners and the cloud service providers that actually run the digital infrastructure and services that we all depend on. So these are these are all overlapping, and it has to happen at all levels of the government. So

211
00:32:47.750 --> 00:33:03.310

H: in in a nutshell, shared responsibility really just means having a mutual understanding and ownership over problems, concerns and improvements. And when we talk about digital resilience, this simply means that, are we

212
00:33:03.310 --> 00:33:22.769
H: cooperating enough to be able to detect and resolve outages when it happens. And more importantly, when something does happen, we want to make sure it doesn't happen again. Right? So are we working together effectively to prevent these incidents from happening in the 1st place. So this is the whole idea behind shared responsibility when it comes to digital resiliency.

213
00:33:23.910 --> 00:33:52.309
H: So I think by now, some of you probably already form, and from some thoughts about why shared responsibility is important. Firstly, I think, and probably the most important aspect of having shared responsibility is that we all then get to improve our ownership. So this this helps to improve the collaboration and and feedback that we have between all the different vendors, the partners, and and the Csps that are involved in our digital projects, and also stop a lot of

214
00:33:52.310 --> 00:34:10.570
H: silo behaviors and blaming that I mentioned, especially when an outage or incident happens. So once we establish that, then what follows is that roles and responsibilities become clear, and very importantly, we reduce assumptions. Assumptions are very dangerous when it comes to resiliency, because.

215
00:34:10.842 --> 00:34:32.130
H: if you have assumptions on who is responsible for providing or ensuring resiliency, then you you are basically forgoing ownership, saying, Oh, maybe someone will take care of it, or you know, and that person, probably. No, that's not my responsibility. I thought you were supposed to do it. So this is the this are the gray areas. These are the things that we want to avoid, because it creates a lot of gaps and unknown steps

216
00:34:32.270 --> 00:34:34.970
H: that would then show up when an incident happens.

217
00:34:35.190 --> 00:35:02.419
H: and only then, and and because for for a lot of us, you know, who deal with our compliance and audit. Actually clearing these roles and responsibilities is actually also very important, because when something does happen, and every government, including the Singapore

Government, inevitably will have a digital outage at some point, and we want to make sure that these roles and responsibilities are clear when it comes to liquidation and damages that we may have to owe, that we may have to request from the vendors and the tech partners

218
00:35:03.190 --> 00:35:31.409
H: the 3rd important point of having shared responsibilities is actually encourages best practices, because once you know what you are responsible for and what the layers below and on top of you in the technologies that is responsible for, then you can design correctly for the resiliency that you need at your level, and knowing this also means that you can then avoid wasting money and effort over over designing for resiliency, when someone at your at the lower layer, for example, already provides for it.

219
00:35:31.620 --> 00:36:00.360
H: And last, but not least, as I mentioned, when an incident does occur, having shared responsibility and makes it very, very clear where the problem areas might be? Who are the responsible parties which then leads to ability to be able to identify, you know, and and escalate, if necessary, in order to get that to get at the resources that you need in order to fix the issue. And this could be engineering. And this could be from a product perspective.

220
00:36:01.540 --> 00:36:17.650
H: So I'll I'll give an example of shared responsibility. Again, shared responsibility is quite a wide area. It could involve things that are contractual. And then there's also a technical aspect to shared responsibility. So I won't go too much into the contractual, because this is again different government to government.

221
00:36:17.650 --> 00:36:32.580
H: but from a technical perspective. In the Singapore Government we have a platform that we call government on Commercial Cloud, which is actually a team wrapper across all the 3 major Csp, so we support aws, we support azure. And we support Google Cloud

222
00:36:32.580 --> 00:36:36.699
H: and the the overarching concept of

223
00:36:37.047 --> 00:36:54.859
H: the government on commercial cloud is that it does something called account vending, which means when a government development team or vendor who wants to work on a government project wants to hold something on Aws, for example, they would go to our government on

Commercial Cloud platform. It's a self service portal, and they basically can vent themselves an account.

224
00:36:54.930 --> 00:36:55.860
H: And

225
00:36:56.090 --> 00:37:03.675
H: when they do that we will build in certain gut rails, security policies, common logging and monitoring, as well as identity management.

226
00:37:04.570 --> 00:37:06.549
H: and vendor account

227
00:37:07.300 --> 00:37:15.710
H: apologies to the to the the development team or the vendor, and then they can directly use it, just like they would any normal

228
00:37:16.150 --> 00:37:26.883
H: of account. I wanted to bring this up, because this is an important aspect of where shared responsibility of which are the owners of Gcc. Comes in so depending on

229
00:37:27.380 --> 00:37:40.209
H: how you use the cloud. There are generally 3 different ways like you can treat it like I as an infrastructure as a service which means things such as the virtual machine, the OS. And of course, the application you're still responsible for.

230
00:37:40.210 --> 00:38:08.020
H: and you can see on the parts in green here. This is where the in the shared responsibility model, the vendors are responsible. Sorry the application teams are responsible for, and then there are parts that you can see boxed up in red. This is where Govtech or Gcc. As a Platform's responsibility is. So the Gcc. Platform is responsible for making sure that those security policies that I mentioned, identity controls, and especially

231
00:38:08.460 --> 00:38:35.460
H: the networking aspects where it connects back to government intranet, for example, these are actually guarded. They are crown jewels, and we keep a close eye over it. But otherwise the

application team is actually free to configure some of these things. So they also. So they take some of that responsibility away from us, and they make sure that they configure the identity controls and the and let's say they open a firewall, for example to their own agency. So they are responsible for that that piece.

232
00:38:35.790 --> 00:38:57.119
H: And then you see the blue color pieces within those boxes. These are responsibilities of the Cloud Service Provider in this case aws Azure or Google, which means, if something goes wrong with, let's say your virtual machine goes down or your storage suddenly stops working. You are unable to retrieve your data. These are responsibilities that the Cloud Service Provider needs to take.

233
00:38:57.120 --> 00:39:09.450
H: So now now you see that in the is model. There's like this separation between what Govtech, as the owner of the government or Commercial Cloud platform has ownership of which are the ones that are

234
00:39:09.450 --> 00:39:17.789
H: the Agency Project teams ownership where the sharing of that ownership is. And lastly, you have the pieces where the Cloud Service providers come in

235
00:39:17.850 --> 00:39:35.820
H: and the rest of the columns on the on the left, right Pas, which stands for platform as a service, and Saas, which stands for software and as a service are also other different ways that you can use the cloud for, and each of these layers are just higher abstractions on top of your normal infrastructure as a service.

236
00:39:35.830 --> 00:39:59.069
H: So in the platform as a service example, for, like some of the runtime in the Middleware things, for example, let's say you would use for those who are familiar. In aws we have the elastic container service. This is covering actually until runtime and middleware, and because it covers up to that level. Therefore the shared responsibility of that of ensuring those services run properly is now with the Cloud Service Providers.

237
00:39:59.080 --> 00:40:27.000
H: Then the agency needs to manage a little less. And of course, we, as the owners of Gcc, we also have to. We also can manage less. Then you go to the extreme right. And that's where you have software as a service. So these are referring to literally services that you can launch in the

Cloud Service providers that are almost ready to use out of the box. For example, sagemaker for those who are data scientists and all that. So in in this model, when using those services, the Cloud service provider actually take up the bulk of the ownership.

238
00:40:27.000 --> 00:40:49.990
H: and the agency ownership is really just to make sure that you know you configure it correctly, and you allow the right users to come in. Of course, the data that you pump into this software as a service is also your responsibility. And in this model, you see, actually very little of Govtech's involvement, because software, as a service generally is exposed to the Internet, so the agency is responsible for opening up their firewalls and all that, and Govtech doesn't

239
00:40:49.990 --> 00:40:58.210
H: generally gets involved in in those conversations. So this is just an idea of how shared responsibility can be done from a technical perspective.

240
00:40:59.650 --> 00:41:24.070
H: So for those who are thinking how to get started again, a lot of it has to do with mindset changes. I think that is the most important piece we really have to move as public sector away from the conventional model of what we call the blame game, so that we need to establish mutual trust and respect, and that can only come if everybody understands the benefits of coming together and co-owning outcomes.

241
00:41:24.070 --> 00:41:42.080
H: So take, for example, for government officials. Right then this would mean that, you know, when when the problem happens, you need to stop that inclination, that it must be your fault and you fix it. I paid you for it. Therefore you're responsible. So we need to stop doing that as government officials, we need to own the problem.

242
00:41:42.220 --> 00:42:12.150
H: This outrage that happens is not the vendor's fault. You are the owner of this digital service, and therefore you should have responsibility to make sure that doesn't happen, and for where vendors are concerned the the other side of the picture will be. They need to be transparent. They shouldn't hide issues or things that are going badly, you know, just because they do not want to offend the government or the agency that's engaging them for the project, and they shouldn't use contracts as shoes. A lot of people do that, but that is the Ntcs of shared responsibility.

243
00:42:12.540 --> 00:42:28.109

H: And for the rest of the industry. For example, then it's very important that we have management and leaders that understand the concept shared responsibility, willing to basically cut across silos and foster collective ownership

244
00:42:28.110 --> 00:42:42.850
H: and behaviors. And one of these behavior is to be blameless. We often go into incident, resolution, and we blame. Oh, which team was it? Which individual was it that made the change. Oh, this vendor is bad. We're going to blacklist them in the future. No, these are these are these are blame assigning

245
00:42:43.508 --> 00:42:48.390
H: behaviors, and they do not encourage shared responsibility. If everybody has that kind of

246
00:42:48.610 --> 00:42:58.389
H: thinking that oh, it's okay to share when things go wrong hopefully before she hits the fan, then, at least, we have a chance of fixing it and addressing the problem earlier.

247
00:42:58.480 --> 00:43:20.979
H: Then for for those who are into public private partnerships, obviously, craft tech does quite a quite a number of trying to choose vendors and tech partners who also have that same mindset. So that is important. So it might take a while for industry to kind of slowly catch up to this kind of concept. But again, the smaller players, you might have better luck in the smaller players actually, rather than the big incumbent ones.

248
00:43:21.922 --> 00:43:31.439
H: So, thirdly, I think using technology to help with some of these shared responsibility comes in useful. The government on commercial cloud platform that I mentioned earlier.

249
00:43:31.460 --> 00:43:58.640
H: where Govtech plays a part in managing some of that shared responsibility is an important one, and because we have a platform. We also kind of act as a glue and as a platform owner over the 3 Csps we are able to do things like help to negotiate and facilitate discussions between the agency as well as the tech partners in this case, the Csps that government on commercial cloud support. So we we play that role to bring people together and foster that shared responsibility mindset.

250
00:43:58.670 --> 00:44:14.960

H: And because we have a common platform. So we we use the term platform engineering to describe what we're trying to do with platform engineering and with a common platform. We are then able to do things like standardized monitoring and observability. For example, I think one of our Japanese.

251
00:44:15.000 --> 00:44:33.550
H: a presenter, shared just now about so. It was about disaster, recovery situations, and not that right when natural disasters happen. But he also mentioned that there are a lot of data sources that needs to be correlated in order for the disaster responders to be able to act correctly and quickly. And this act of

252
00:44:33.550 --> 00:44:52.329
H: taking different data sources and trying to bring them together is exactly what we're trying to do. But in our landscape of Cloud Residency simply means people to collect locks, matrices, and events to get in the same place, standardize them. So all parties, from vendors to the agency, to the Cloud Service Provider can see the same thing.

253
00:44:53.370 --> 00:44:53.709
C -: What I mean.

254
00:44:54.470 --> 00:44:55.040
H: I'm sorry.

255
00:44:55.420 --> 00:45:00.100
C -: We're gonna have to interrupt because we we need to progress onto the

256
00:45:00.655 --> 00:45:05.040
C -: onto the next section of the of the webinar. If that's okay.

257
00:45:05.040 --> 00:45:07.930
H: I'll finish up. This is really the last slide already. Yeah.

258
00:45:08.160 --> 00:45:11.537
H: no worries. Yeah. So I'll I'll just quickly finish. And and lastly,

259

00:45:13.390 --> 00:45:28.179
H: when it always helps. If there's some kind of like official guidelines or policies that you know how to establish that responsibility. And this just makes it very clear for the agency or public offices to also implement that in their contracts and in their negotiations with the vendors. Yeah.

260
00:45:28.340 --> 00:45:32.529
H: So I think I think that's it. So thank you very much. Yeah. Sorry for taking up too much time.

261
00:45:32.530 --> 00:45:59.549
C -: No, thank you very much, She-. And hopefully you can stay and answer some questions for our audience today. So I want to move us on very quickly to our closing panel, where we have some very distinguished people from around the world, including She-. So we have Yasuhiru Kawaso from disaster risk management specialist at the World Bank's global facility for disaster, reduction and recovery.

262
00:45:59.550 --> 00:46:26.030
C -: We have - cifuentes fellow at co-develop in New York and former digital government director, the ICT Ministry of Colombia. And hopefully, we still have Stella Mukan, the Digital government practice manager at the World Bank's Digital Vice Presidency. But I do know that because we started late and had to move on, some people may have had to exit already, but I was going to try and catch Stella with one question before

263
00:46:26.030 --> 00:46:48.399
C -: before she goes, if she is able to join us. Sorry, I know it's a triumph of brinksmanship. But, Stella, we've been talking throughout this digital resilience, Webinar, about what Japan is doing, what Singapore is doing before you have to leave us. What do you think governments should do 1st to get ready for large scale digital adoption, especially in fragile and low resource settings.

264
00:46:50.000 --> 00:46:55.699
S: Thank you, C, and thank you. Everyone who joined. I think the context is very important.

265
00:46:55.850 --> 00:46:59.949
S: and building on what Thiawo has just mentioned.

266
00:47:00.140 --> 00:47:06.410
S: What he mentioned about shared responsibility. Mindset really resonated.

267
00:47:06.530 --> 00:47:11.519
S: and his point on focusing on the people

268
00:47:11.790 --> 00:47:17.830
S: and focusing on the problems. But people face in certain contexts.

269
00:47:18.270 --> 00:47:28.205
S: either it's related to humanitarian related challenges or to disaster related challenges. So

270
00:47:30.150 --> 00:47:42.540
S: maybe one priority that governments could think about in this shared responsibility with this shared responsibility. Mindset is really look for partners.

271
00:47:43.402 --> 00:47:49.730
S: Look in the specific country context and see whom on whom they can rely

272
00:47:49.990 --> 00:48:18.960
S: outside of the government. In many of our these countries, you have both international development partners supporting with digital transformation initiatives. You have technology partners. And of course, you have the local ecosystem. So, bringing all these partners together, mobilizing their resources and contributions both to tackle some immediate challenges

273
00:48:19.635 --> 00:48:37.339
S: immediate priorities, but also bring them along to shape the more foundational digital investments that the country needs to build. And we we learned today from Japan, from Singapore what these foundational investments really are

274
00:48:37.480 --> 00:48:52.220
S: which will require time which will require resources. So having a more agile approach towards addressing some specific challenges that are priority now

275
00:48:53.056 --> 00:49:05.049
S: and building on responding to this urgent priorities with an integration by design approach, because some of these

276
00:49:05.160 --> 00:49:07.729
S: initiatives can be leveraged

277
00:49:07.840 --> 00:49:33.430
S: to build the future of investments in the foundational in the foundations, but they can also be integrated in whatever a government has already in place in terms of digital public infrastructure. So I think partnerships is very partnerships are very very important. They would allow us not to reinvent, not to duplicate and respond to real problems on the ground.

278
00:49:34.530 --> 00:50:03.260
C -: Lovely. Thank you so much, Stella. Glad to catch you, Y. I know you're similarly pressured for time. I did want to ask you one question if I could. Before you have to go, we live in a world at the moment where there are so many emerging technologies and artificial intelligence, remote sensing, digital twinning. I was just curious. Which would, you see, playing a critical role in the future of disaster. Preparedness given, you are a risk management specialist.

279
00:50:05.010 --> 00:50:24.550
Y -: Thank you so much. C, like actually chatted about this with my colleagues in our office, many other disaster specialists, and they all agree, like all of these, AI remote sensing digital twins are really all important, not because that can really make the impacts make disaster response much faster or easier. For with this paper?

280
00:50:25.002 --> 00:50:37.329
Y -: So in the Gfdr like, we basically support these activities in the growth. For example, like in the Caribbean countries, we use the drones and AI to basically support the local Gis people to

281
00:50:37.340 --> 00:51:01.749
Y -: identify or like the map, the housing in the area, and also, like overlaying the information with the wind like the potential the typhoons risk there. So the basically before. And of course, people need to like manually map the housing. But now, with AI and the drones. We can basically fast track those like mapping exercise and then overlaying with other information, so that people or the government can be much

282
00:51:01.850 --> 00:51:20.849
Y -: more ready to the disasters. But at the same time we also see like AI. And these drones are not always perfect. And as we also discussed today, like there are many errors. So of course,

the human corrections, the involvement of local communities, are critical. I mean, for involving the local communities aspect like the Gfd. Our team also collaborate

283
00:51:20.930 --> 00:51:24.069
Y -: with the local communities. For example, like we

284
00:51:24.090 --> 00:51:31.550
Y -: support the local communities to basically use their tablet and the phones to map the areas before. No, I mean.

285
00:51:31.550 --> 00:51:51.440
Y -: for example, like, it's very difficult for the experts to basically get all the information in the local areas like the topographies, or like the because it's important to know the topographies and the asset information for the housing asset assessment for the disaster risk assessment in the specific areas, but collecting those information in the local communities. It needs a lot of

286
00:51:51.440 --> 00:52:05.600
Y -: specialist before to go to the field and do the survey. But of course the situation changes very frequently. So if we can ask local communities or university students, or even like the people there using their tablets to get their information to us, using more like the

287
00:52:05.600 --> 00:52:29.570
Y -: participatory approach it's related to the open street map activities. Like we can get more updated information, the local communities so that the information can be more accurate, and also people understand the risk and the information there. So I believe this participatory approach local communities involvement is really helpful. But I believe all your technology. AI remote sensing additional twins can really make the impact to the field. Thank you, C.

288
00:52:30.250 --> 00:52:31.760
C -: Thank you, Yasihiro.

289
00:52:31.940 --> 00:52:43.249
C -: and I can see that we still have Mr. - and HH. You're still there as well. I'm hoping that you're able to translate a question for me, for Mr. -.

290
00:52:44.500 --> 00:52:45.180

HH -: Yes.

291
00:52:45.910 --> 00:53:09.100
C -: Marvellous. Thank you. Given what we've just heard from our speakers, I'm interested to know from Mr. -. If there have been any deviations from the original plan for techforce. You know what were the reasons for those deviations, and how did the ministry adapt its strategy for techforce in response to those deviations.

292
00:53:35.060 --> 00:53:43.200
Mr Y -: Ahoy Korea mode to start.

293
00:53:44.240 --> 00:53:51.760
HH -: So this is Kriyama speaking. Thank you very much for your question. 1st of all, there have been no deviations from the initial plan.

294
00:54:07.450 --> 00:54:21.130
HH -: and what we are doing as of today is we are asking questions. We are taking surveys from the members of the force to identify if there are any challenges, or if there is a need for any improvement, and taking actions as needed.

295
00:54:21.870 --> 00:54:23.090
Mr Y -: Each other.

296
00:54:23.090 --> 00:54:24.570
HH -: That's all for me. Thank you.

297
00:54:25.000 --> 00:54:28.429
C -: Thank you very much, Mr. Kurama, and from you, too, HH

298
00:54:28.680 --> 00:54:57.390
C -: -, I know you're there waiting patiently. You have an incredible view and insight into Latin America's implementation of digital public infrastructure. I am very curious to understand as we've been hearing about resilience and information has been playing such an important part. What you've seen with ideas like data, sovereignty and localization and modularity being incorporated into government strategies in Latin America.

299
00:54:57.390 --> 00:55:20.230
-: Yes, thank you, C. It's been amazing. Because I worked 10 years in government actually deploying this type of initiatives, this type of projects. And now that I'm like in the philanthropic front helping governments supporting governments on this like type of adoptions and deployments, what we've been seeing is that there's like a very important shift from governments in terms of

300
00:55:20.390 --> 00:55:46.450
-: asking and wanting to have one. Of course, data sovereignty. I think that many speakers already addressed that concern, and that willing that will to yeah, protect their data, working with local partners, having the capacity internally to be able to own and collect and use the data. So for sure, data sovereignty is one of those topics.

301
00:55:46.870 --> 00:56:03.029
-: second ownership. And this is important because of what we've been seeing in many governments after covid on digital public infrastructure. They want to localize their budgets. They want to be able to commit, of course, but they want to

302
00:56:03.400 --> 00:56:09.249
-: shift sometimes like the approach on this, on this project in terms of like.

303
00:56:09.410 --> 00:56:15.459
-: I have this need. So I will identify these use cases. I want to work with some market players

304
00:56:15.920 --> 00:56:36.049
-: like ideally local partners again. And I want to avoid vendor looking. And this is an important shift like ownership. It's been there so principles like modularity, optionality, and of course, avoiding vendor looking. It's something that we've been seeing in many governments trying to shift that narrative in terms of like.

305
00:56:36.050 --> 00:56:52.929
-: I love to work with the private sector. I trust them, and they've been an amazing partner for so many years. They help me to deliver. They helped me to be agile. But now I want to avoid those contracts for 10 years, 20 years. I want to own this process a little bit more.

306
00:56:52.990 --> 00:57:04.730

-: and some governments in lack. They've been doing things like in-house. They've been trying to have state owned companies working with the private sector again, but owning the majority of the process.

307
00:57:04.980 --> 00:57:23.890
-: and what I think it's interesting. And this is something that some speakers mentioned. We've also seen a shift in the Gov tech supply side, like in the Govtech ecosystem. Many startups that have been working with governments for many years building their solutions on proprietary licenses. They're shifting their business models to more open source

308
00:57:23.890 --> 00:57:35.079
-: business models, open source solutions. And this is interesting because governments, because of data sovereignty because of ownership principles because of they want to avoid vendor lock in.

309
00:57:35.080 --> 00:57:37.660
-: They're like really looking forward to have more

310
00:57:37.660 --> 00:57:50.279
-: open source solutions, open protocols, open standards, and Govtech ecosystem is actually responding to that need. And this is super interesting to see. And maybe my last

311
00:57:50.350 --> 00:57:55.410
-: comment and something, yeah, some things that we've been seeing. It's

312
00:57:56.700 --> 00:58:22.900
-: I think that philanthropics like donors funders. We've been understanding that. Of course, the governments are very different, even if we're like, just look at the region. There's like some differences, of course, like synergies. But we've been trying to promote a concept that I really liked. And it's like qualified demand and qualified demand means that every time that we're like supporting a project or working with the government. There's a list of criteria that we assess, and that we would love to have unchecked.

313
00:58:23.399 --> 00:58:47.030
-: A use case right like country demand driven should be the project and the initiative. So a use case, a need, a very identified need. For example, climate resilience. It's an amazing topic for to

connect with Dpi right like, because of social benefits because of cash transfer. So qualified demand is a list of criteria. I won't mention that because of time. But

314
00:58:47.400 --> 00:59:00.910
-: you, having use cases identified and having that country demand driven approach. It's something that we we check. And of course I'm not saying like governments, should do everything by their own, and should like own 100% of the processes.

315
00:59:00.910 --> 00:59:10.199
-: But for sure, after Covid, we've been seeing like governments owning more the project and wanting to localize their efforts and working with local partners.

316
00:59:11.920 --> 00:59:18.880
C -: Super. Thank you so much. Era. I have one question for H-, who I think you're still with us.

317
00:59:19.440 --> 00:59:26.489
C -: and you know, just picking up on some of those themes that we've heard the relationships in vendors and government and everyone else.

318
00:59:26.490 --> 00:59:49.930
C -: The thing I've always admired about Singapore is, you seem to have managed a very strong center to your digital and to your architecture. But you also have a federated responsibility model which you touched on in your presentation, and I wondered if you could just talk a bit about creating that balance between a strong center, but also federating responsibility as well.

319
00:59:50.900 --> 01:00:19.569
H: Yeah, so so thanks, C for the question. I think you have already come out with the answer, which is the word balance? Right? So it is hard. It is hard to juggle. The public sector is, after all, a highly regulated organization, just like banking and finance, and in in those sectors. It's very hard for people to imagine. Oh, let's make responsibility, grey between 2 adjoining parties, right if they want right and wrong, one and 2 and 3 is different numbers and left and right is different. So

320
01:00:19.570 --> 01:00:48.740
H: so so I think we need to find a balance. And one of the panelists they mentioned about being agile. I think when we make this kind of balance, we need to understand the trade-offs. If we are

overly stringent on segregating roles and responsibilities, then people are just going to be very compartmentalized into what they do, and they do not want to reach out and help each other, and that kind of stifles innovation stifles agility and ultimately stifles the quality of the digital services that the Government provides.

321
01:00:51.250 --> 01:00:53.399
C -: Cool. Thank you very much.

322
01:00:53.980 --> 01:01:05.620
C -: so I'd like to ask everybody to join me in a kind of a round of digital applause for all of our speakers

323
01:01:05.910 --> 01:01:17.089
C -: very grateful for you, especially when we had some technical difficulties. That meant we had to restart the session and go again. I'll give all of you that thank you very much.

324
01:01:17.870 --> 01:01:36.590
C -: Most importantly. Also, thanks to the attendees who returned. You can see them clapping for everybody who returned, despite the needing to re-engage. What I'd like to do now is, I'd like to hand over to Ida Swarai RIoch, who is the global director and director of strategy and operations

325
01:01:36.590 --> 01:01:55.359
C -: at the World Bank's Digital Vice Presidency. I also hope that Ida forgives me for my Scottish pronunciation of your wonderful and very beautiful name, but I would have asked you that if I'd had the opportunity to beforehand. But yeah, Ida, please over to you for some closing remarks.

326
01:01:55.360 --> 01:01:58.360
I: That's okay. Thank you so much. Can you hear me.

327
01:01:58.620 --> 01:01:59.340
C -: We can hear you. Well.

328
01:01:59.340 --> 01:02:14.870

I: Okay, thank you. Look, C, I I usually before I make a presentation. I always say, if you can pronounce my name well, then, I will pay you and I think you just lost that payment, unfortunately. But never mind, that's okay.

329
01:02:15.050 --> 01:02:31.870
I: So 1st of all, I really want to thank the speakers. It's rare that a speaker repeats a presentation and does a better job than when they did it the 1st time. So I really want to thank the presenters who did this, and you know it was kind of.

330
01:02:31.950 --> 01:02:54.469
I: I was reflecting that we are talking about disaster, risk management, and the ability to recover. And then we have this. And then I saw the recovery. And I said to myself, Well, maybe this is what technology actually is showing us that it is possible to recover even when you have a glitch like that. So again, a really big thanks to the speakers, and thanks to the organizers.

331
01:02:55.089 --> 01:03:07.380
I: It's it's I have had the opportunity to work with Japan in in the disaster risk management area. And it's interesting to see just how much they continue to improve.

332
01:03:07.380 --> 01:03:27.670
I: and how much data is now becoming really sort of giving them the ability to even leapfrog further. And I think it creates a huge opportunity for many countries who are looking to Japan to learn from the experience.

333
01:03:27.670 --> 01:03:57.649
I: But what I also was thinking about is how much we can extend what they are talking about to other areas beyond disaster, risk, and to me, the potential, the opportunity and the ability to be able to move into that direction is something that I think is really interesting. And by definition I do think that there's a lot that the world can continue to learn from Japan, and we don't see this event as a 1 time event. In fact.

334
01:03:57.650 --> 01:04:02.251
I: I was talking to A about, how do we get this?

335
01:04:02.810 --> 01:04:20.889

I: learning from Japan to actually go to other countries, and I know that there are other academies that are being thought of in the Mena region in the Africa region. And why should they start from scratch when there's already a very functional and a very sort of

336
01:04:20.890 --> 01:04:33.290
I: high impact? Academies such as this one? We need to connect them more make sure that they learn from each other the teachers teaching the newer ones, and then the newer ones also learning

337
01:04:33.290 --> 01:04:35.309
I: how to how to move forward.

338
01:04:35.460 --> 01:05:01.029
I: It was really one expression that really struck me, which will stay with me in my mind for a while is soundness of information, and I like that term, because it was about the right information for the right people to do the right thing. And I think this is what it's all about, right. I mean the information we collect and that we collate and we analyze and we use.

339
01:05:01.030 --> 01:05:10.579
I: It's all about, what is the end program that we want? What is the end product. What do we want to influence? And I think what I take out of today's

340
01:05:10.800 --> 01:05:38.960
I: presentation from the different speakers is that there's a multitude in which we can use. But there are some sound foundations that we need, which is, you need to have the right data. You need to collect the right data. You need to make that data safe. You need to make sure that it is data that actually then influences decisions going forward and that those decisions are something that we can rely on in a disaster. You don't want to be recreating anything

341
01:05:38.960 --> 01:05:49.769
I: all the time. You want to actually build on that learn from it, and be able to be much more effective if you are ever in that situation again.

342
01:05:49.770 --> 01:06:17.179
I: And I think to a certain extent, if we take this. And we think about how the global digital world is moving and how AI is moving. In my mind. There's a parallel here. We need to learn from others. We need to see what works, and then we need to adapt it and adopt it and use it within

the context of the countries or the area that we are talking about. And that again, that is actually a case of data, how the data is used, how it is shared

343
01:06:17.190 --> 01:06:38.980
I: and how ultimately that data gives us a much better vision to where we want to go. So I cannot underline enough the importance of this cross sectoral collaboration which came through every single speaker that I heard from today, and the strategic nature with which data sharing can actually

344
01:06:38.980 --> 01:06:58.749
I: improve, how we do work and how we impact the citizens in the country. So again, let me thank you, C, and everybody who has participated. It's really been a fantastic session. I sat through the whole thing, and I would do it again because it was that interesting. Thank you.

345
01:06:59.490 --> 01:07:14.020
C -: Thank you for those comments. That's perfect closing statements. I can't echo enough. I was the director of the Uk's Government digital service for 7 years, and the best part of the job was learning from all the other countries around the world.

346
01:07:14.020 --> 01:07:39.010
C -: We learned so much from each other, and especially in the pandemic. There were a lot of assistance going on, helping. Everyone just wanted to understand what worked, what worked and the connections we built with Singapore and other countries came into play during those times. So I want to thank you. I want to thank all of our speakers one more time for their time and apologies for this, the accelerated agenda.

347
01:07:39.010 --> 01:07:48.290
C -: And I think we're going to put a little poll up on the screen, so that if people feel they've had a good session today. They can.

348
01:07:48.290 --> 01:08:17.889
C -: you know, provide some feedback to us, but that is all we have time for today. We're so glad and thank you to everybody and keep an eye out for an email that will come your way with today's recording and resources for maybe your colleagues or friends who weren't able to join or rejoin. Once we restarted, we'll see you at another apolitical event soon, but otherwise have a great day or evening depending on where you are in the world, or go to bed. Thank you very much, and goodbye.

349
01:08:17.890 --> 01:08:19.449
I: Thanks everyone, bye.

350
01:08:19.450 --> 01:08:20.999
G: Thank you. Bye.

351
01:08:22.300 --> 01:08:23.339
H: Thank you. Goodbye.