Transcript: Cyber Attacks on Government: What You Need to Know

00:00:25.000 --> 00:00:36.000
So lovely to see the numbers ticking up. Welcome. Oh, a little Zoom reaction there. Hi. We'll just give everyone a second to join. So excited to get started with today.

00:00:36.000 --> 00:00:44.000
Always takes a minute for everyone to arrive. Hello and welcome to this panel event, Cyber Attacks on Government, What You Need to Know.

00:00:44.000 --> 00:01:09.000
My name is Jessica Van Onslin and I'm the Director of Communications here at Apolitical, coming to you today from a very sunny Brighton on the south coast of the UK. It would be great to hear from all of you, so do post in the chat where you're joining us from and maybe what organization you work from. It's always lovely to get a sense of who's on the chat. So open it up. Let us know who you are. Always great to say hi. We've got our lovely concierge saying hi to everyone.

00:01:09.000 --> 00:01:37.000
One there as well. Today, we'll be exploring emerging cyber threats targeting governments in 2025, These strategies for protecting digital government services and actionable tactics for Building Cyber Resilience. This is a topic that is like super close to my nerdy heart. I'm completely fascinated by cyber attacks and I cannot believe the caliber of guests we have today to speak to you. So I personally am super excited to jump into today's session.

00:01:37.000 --> 00:01:47.000
For those of you who may be joining us for the first time, just welcome. Apolitical is the world's largest community for government used by over a quarter of a million public servants like you.

00:01:47.000 --> 00:02:00.000
And policymakers from more than 170 countries. Our mission is to make governments smarter, and we do this by putting the best knowledge and skills at the fingertips of public servants around the world.

00:02:00.000 --> 00:02:21.000
I'm going to introduce our panelists in a second, but first, it's always nice to just hop in and see who's joining us on the chat. So hi. We have Abdul joining us from Birmingham. Hello. We have Jessica from the Ontario Public Service. Very nice. In Kingston. Hi from Nigeria. Welcome, Nigeria. As a fellow African, always exciting to see someone pop up on the chat there.

00:02:21.000 --> 00:02:28.000
We've got Diane from Vancouver, beautiful Vancouver, lovely. Lots of Canadians actually. Welcome.

00:02:28.000 --> 00:02:31.000
Love our Canadian crew. Hi, Artem from Ukraine. Really nice to see you.

00:02:31.000 --> 00:02:48.000
More Toronto Halifax, fantastic. So do keep introducing yourselves. It's always really great to see you. We're so pleased to have you here I want to extend a really special welcome to those of you who are already members of Apolitical's misinformation and disinformation community.

00:02:48.000 --> 00:02:55.000
If you're not in the community, we're thrilled to extend an invitation to join your peers across the global public service in this forum.

00:02:55.000 --> 00:03:07.000
So the community is the place designed for public servants and policymakers committed to identifying and pushing back against misinformation and disinformation, something that I'm sure we're going to touch on in today's conversation.

00:03:07.000 --> 00:03:22.000
You should see a little link pop up at the bottom of your screen that should take you to the community. If you're interested, or you can find it by clicking on the resources button at the bottom of your Zoom screen and then you can follow the join the community link there.

00:03:22.000 --> 00:03:28.000
I'm going to get a few technical notes out of the way before we get into today's conversation. A little bit of housekeeping.

00:03:28.000 --> 00:03:40.000
This event is recorded for on-demand viewing on the apolitical website. We know we have a lot of Australia and New Zealand folks registered. So if you're watching this on demand later, hi. And thanks for coming back to watch.

00:03:40.000 --> 00:03:47.000
Please don't record it yourself. Contact details for privacy concerns are in the apolitical homepage footer.

00:03:47.000 --> 00:03:52.000
And closed captions are available and can be toggled on or off on your screen settings.

00:03:52.000 --> 00:04:00.000

Before we introduce our three amazing speakers, and I know that Francesca, one of our speakers, has just joined us. Welcome.

00:04:00.000 --> 00:04:10.000
We are going to run a few quick polls to get a sense of where you're coming into today's discussion from. My speakers, that can also be really interesting just to get a sense of our audience today.

00:04:10.000 --> 00:04:35.000
The first poll is, how confident are you in your own ability to detect and respond to potential cyber threats? That could be suspicious emails or phishing attempts in your daily work? How confident are you I'm just watching the answers roll in, give everyone a second to answer. Yeah. Do you consider yourself like quite skilled at being able to possibly detect a threat or is something you

00:04:35.000 --> 00:04:49.000
I'm not entirely sure about. Still got some answers rolling in here. I think we have a clear winner, but I'll give it another second before I share the results. All right. I think we've kind of settled on an answer here.

00:04:49.000 --> 00:04:56.000
It is somewhat confident is the majority, 67%. If we wrap that up with very confident, you're actually quite a confident bunch.

00:04:56.000 --> 00:05:26.000
Feeling you're literate, feeling you can spot these threats, you know, you're fairly certain. Few of you not so confident, and only 2% of you not confident at all. But I guess you are on a cyber attack threat webinar, which just goes to show that you're thinking about these things already. Fantastic. That's poll number one. The second poll is, when was the last time you participated in any formal cyber training, cybersecurity training or a refresher course? When was the last time you were trained? Was it really recently within the last three months, maybe the last six months, within the last year, more than a year ago or terrifyingly, have any of you never attended

00:05:34.000 --> 00:05:44.000
Any cybersecurity training. I think our guests will be watching to see with interest. Be honest, it's anonymous. We definitely want to hear the results.

00:05:44.000 --> 00:05:57.000
When last did you get cybersecurity training? Okay, this one is a little bit closer than the previous one. I'm going to give everyone another second To answer, oh yeah, this is looking quite balanced. Okay, sharing results.

00:05:57.000 --> 00:06:06.000

The winner here is within the last three months. Yes, fantastic. So your organizations are training you. Another big chunk of you, 21% within the last six months.

00:06:06.000 --> 00:06:20.000
Good 20% within the last year. I think we're all quite curious to see who's never attended any cybersecurity training. And that is a surprisingly high 10% in government. 10% of you have never attended any cybersecurity training.

00:06:20.000 --> 00:06:25.000
Feel free to share more details in the chat if you want to.

00:06:25.000 --> 00:06:36.000
The final poll, which type of cyber threat do you think is the biggest risk to governments in 2025? We're coming up for a big year. What does the year ahead look like in your opinion?

00:06:36.000 --> 00:06:41.000
Ransomware attacks, deep fakes and misinformation. Maybe it's supply chain attacks.

00:06:41.000 --> 00:06:51.000
Insider threats, data breaches, and if it's something else, which we haven't listed here, pop it in the chat. We'd be really interested to hear what's on your mind, what you're sort of thinking are the biggest threats.

00:06:51.000 --> 00:06:59.000
Going into 2025. Lots of furious voting going on there, quite interesting. I'll give that another second.

00:06:59.000 --> 00:07:08.000
Speakers as well, something for you to think about when you answer some questions. We'd love to know what you're thinking are the biggest risks for governments into 2025.

00:07:08.000 --> 00:07:16.000
But to share the results here, we have a clear winner. The majority of you think that the biggest threat going into 2025 is going to be data breaches.

00:07:16.000 --> 00:07:29.000
A good 45%, that's almost half of you. A quarter of you, deep fakes and misinformation. And I certainly know Ilana, one of our guests today, might touch on that. Ransomware attacks. We were just talking about ransomware.

00:07:29.000 --> 00:07:53.000
Attacks before we came on air. So that will definitely come up. Insider Threats. Fantastic. I'm just going to nip into the chat actually and see if any of you have anything else? Oh, hi Kali from Bhutan. Fantastic. We don't often see Bhutan here, so you are so welcome. If you have

anything else that you think is going to be a big threat that we missed that wasn't reflected in our poll, stick it in the chat. We'd love to hear a little bit more about that.

00:07:53.000 --> 00:08:08.000
Thanks for taking part in those. And now I get to introduce our three speakers. I am thrilled with excitement to do this. We're fortunate to have three brilliant guests today. We have Francesca Bosco, Ilana Cohen and Jonathan Scott joining us today.

00:08:08.000 --> 00:08:25.000
I'll start by introducing Francesca. Francesca is chief of staff and the head of foresight at the Cyberpeace Institute, where she leads strategic engagement in programs leveraging multi-stakeholder cooperation with civil society, academia, corporates, philanthropy, and public institutions.

00:08:25.000 --> 00:08:34.000
The Institute's aim is to reduce the harms from cyber attacks and disinformation to anticipate the challenges posed by AI and emerging technology.

00:08:34.000 --> 00:08:49.000
And to promote sustainable cyber peace. Welcome, Francesca. So great to have you. We also have Ilana. Ilana is the chief legal and policy officer at HackerOne, where she manages the public policy portfolio, oversees all legal matters. Can you imagine?

00:08:49.000 --> 00:08:56.000
And provides strategic leadership to the company. Ilana joined the tech industry after serving nearly four years in the Obama White House.

00:08:56.000 --> 00:09:05.000
Where she was an integral part of designing and implementing the administration's technology and cybersecurity initiatives. Ilan is so delighted to have you.

00:09:05.000 --> 00:09:11.000
And last but definitely not least. Jonathan is the head of cybersecurity at the UK's Government Digital Service.

00:09:11.000 --> 00:09:21.000
Leaving a team tasked with ensuring the critical public services that the GDS remain secure and operational for millions of UK citizens that use them every day.

00:09:21.000 --> 00:09:30.000
Jonathan has over 10 years of practical experience in security, having worked from the UK Home Office and the UK National Nuclear Laboratory. Welcome.

00:09:30.000 --> 00:09:38.000

To find out more about our you can always head to the resources tab here on Zoom and you'll see you'll be able to read their full biographies there.

00:09:38.000 --> 00:09:56.000
Okay, well, enough talking from me. Let's start with an icebreaker to kick things off. Maybe you on the call as well. We'd love to hear from you. I'd be interested to hear everyone's answer to this question. My colleague will post the link to a thread in our misinformation and disinformation community if you want to share your response.

00:09:56.000 --> 00:10:09.000
The icebreaker is what's one non-essential app, website or digital tool that you'd struggle to live without if it got hacked. Jonathan, I'll come to you first. What would you struggle to live without?

00:10:09.000 --> 00:10:25.000
This one was a tough one for me, actually. I was trying to really pin down something that I thought I would really, really miss. I think I'd have to pick like YouTube or Spotify. If anything, just because I like to watch videos when I'm out and about and listen to music when I'm out running. But I think those are two the two that I probably struggle the most without.

00:10:25.000 --> 00:10:34.000
Very good. On social media, let's be honest, Instagram fans out there were definitely thinking about that, I'm sure, as well. Francesca, what would you battle to live without?

00:10:34.000 --> 00:10:59.000
Actually, I was saying there personally Instagram would be most probably number one, but I'm thinking more from an operational standpoint and let's say the day-to-day work. I would say ever like Evernote or like, for example, Notion and i mean all the all the things that are helping us actually going through our daily work yeah would be would be would be hard

00:10:59.000 --> 00:11:17.000
Okay, very good. So a little bit of fun there, but also like you would miss an ocean makes a lot of sense. Ilana, what would really screw up your day if you didn't have it?

00:11:17.000 --> 00:11:18.000
Oh.

00:11:18.000 --> 00:11:25.000
So for me, it's um an app called Blackbaud, which is actually what helps me track my kids homework assignments. And I'm not sure I would be able to hold them accountable, you know, research paper due tomorrow, that kind of stuff so

00:11:25.000 --> 00:11:27.000
I absolutely can't live without it.

00:11:27.000 --> 00:11:37.000
Okay, parents out there, I'm sure Ilana can put the name in the chat if you're like, I need that app in my life. I too want to be grumpy if that was being taken away. It sounds so incredibly useful.

00:11:37.000 --> 00:11:38.000
Very cool.

00:11:38.000 --> 00:11:46.000
Any answers in the chat as well. Youtube, a lot of YouTube fans. Jonathan, you've kicked off a movement there. Definitely.

00:11:46.000 --> 00:12:00.000
Khadija, I'm so glad it's also Instagram. I'm embarrassed to admit I would have a panic attack, I think, if you took away the cat videos and the interior decorating that I spend a lot of time looking at. Fantastic. We'll put yours in the chat as well by all means.

00:12:00.000 --> 00:12:14.000
All right, we're going to jump straight into our panel discussion. We're so eager to hear from these three amazing experts. I'm going to start off with a sort of exploration of the changing cyber threat landscape as we go into 2025.

00:12:14.000 --> 00:12:18.000
This is a question that I'll put to each of you. I'll come to each of you for your view.

00:12:18.000 --> 00:12:39.000
Cyber threats to government seem to be evolving at an unprecedented pace. Maybe AI is supercharging them. From your perspective, how is the threat landscape changed in recent years and what's driving this shift? I mean, how is this translated into the challenges and priorities in your work. Ilana, I'll start with you.

00:12:39.000 --> 00:12:57.000
Sure. Well, this is a tough one to answer because there are so many answers, frankly, it has evolved so much over the last several years.

00:12:57.000 --> 00:12:58.000
And what is the PRC? Sorry to interrupt.

00:12:58.000 --> 00:13:14.000
There is, of course, the threat of nation states and just the activity of the PRC specifically in all of our critical infrastructure that has been Sorry, China. The People's Republic of China and the focus on critical infrastructure, not just in the US, but in a multitude of different nations. That's one area where we have seen a lot of evolution, a lot of activity in the last several years.

00:13:14.000 --> 00:13:34.000

And then I would say also ransomware is another area where we have seen an evolution, a much more professionalization of ransomware that has affected not just governments, but obviously everyone that we all interact with on a daily basis. And we can get into those details in a little bit.

00:13:34.000 --> 00:13:38.000
More later on in the seminar.

00:13:38.000 --> 00:13:43.000
Absolutely. We will come back to both of those super clear. Jonathan, what about you?

00:13:43.000 --> 00:13:55.000
Yeah, definitely just adding to everything that Alana's already said i think it used to feel a bit different in government because you used to be worried about the foreign state actors and also something that is still around.

00:13:55.000 --> 00:14:16.000
The sort of unique regulatory environment that we find ourselves in now as Alana was explaining, there's been a massive proliferation in tooling that a multitude of actors can access. So it's no longer just the the state actors that have access to this really high-end capability, actually a lot of sort of smaller, lower end actors can access the same capability now so it's

00:14:16.000 --> 00:14:26.000
Really changed the landscape for us. We're having to base everything we do on risk, understanding where our highest value systems are and what we can do to protect those.

00:14:26.000 --> 00:14:33.000
As we have been doing for a long time. But things have changed massively in the last few years. It's kind of scary to be honest.

00:14:33.000 --> 00:14:39.000
Okay, well, there's a head of cybersecurity telling you that it's a bit scary out there. Francesco, what about you?

00:14:39.000 --> 00:15:09.000
I was about to say, what else can I say after this statement, right? So it's a little bit unfair coming after Ilana and Jonathan because they highlighted very well. I think that, I mean, to kind of like in a way complete and sum up in a way there is on one hand that the in a way the expansion, I would say, of their tax surface which is going hand in hand with the digitalization processes that we've seen as a society, but not

00:15:09.000 --> 00:15:29.000

In government organization. I think Ilana mentioned it very well and I mean, stated also by Jonathan in terms of like the type of actors. So state actors and non-state actors, but also kind of like what I call the democratization. Often we say that AI is democratizing tools and more.

00:15:29.000 --> 00:15:52.000
Kind of like participatory tools but then at the same time is also in a way democratizing the crime sphere because indeed you don't need to be a kind of like a super highly sophisticated criminal anymore. So the proliferation of ransomware, for example, as a service models that make it

00:15:52.000 --> 00:16:22.000
Kind of like made it in a way easier for less technical skilled actors to launch attacks, notably against critical infrastructure is increasing and incredibly worrying. Maybe just to add the one point, so there is the on one hand that the digitalization and the rapid pace of technology, including AI, I was surprised that in the In the first poll, when you asked about the, it's true that it was not, let's say, an open question related to AI, but in several conversations that we are having.

00:16:25.000 --> 00:16:45.000
With the state counterparts for example I mean, AI kind of like enable hampered supported cyber threats is kind of like a recurring. It's true that you can have ransomware powered by AI or you can have, for example, some other categories powered by AI. But I would say that

00:16:45.000 --> 00:16:58.000
Ai is indeed a sort of like a game changer when discussing with governments. Maybe one thing that was not necessarily mentioned, but it was in the poll.

00:16:58.000 --> 00:17:23.000
I would say is the blurring line between cybersecurity and information integrity, meaning that what I would say in a In addition to traditional, in a way, cyber threats, we are witnessing a convergence between security and information integrity, meaning that malicious actors are not only targeting, for example, IT systems, but also manipulating information flows through, for example, disinformation campaigns, influencing public opinion.

00:17:23.000 --> 00:17:36.000
And also creating confusion during rises, even more so if you couple it up with the what it was said before in terms of like the tension when it comes to the geopolitical situation.

00:17:36.000 --> 00:17:55.000
And again, here we go back to the AI again, because the rise of AI generated disinformation and deep fakes has made much more challenging to differentiate between, in a way, authentic and fabricated content, undermining trust in institutions, not only from a technical standpoint, but also from, let's say, from a thought.

00:17:55.000 --> 00:17:56.000

Leadership standpoint.

00:17:56.000 --> 00:18:01.000
Yeah, yeah. I mean, just such an interesting overlap there with the misinformation and disinformation.

00:18:01.000 --> 00:18:19.000
My next question is actually a follow-up for you there, Francesca. You said two things in there which kind of link to it. The one was about manipulating sort of responses during a crisis. For example, and the other is attacks on critical infrastructure, right? So we often talk about the financial and operational impact of cyber attacks, but

00:18:19.000 --> 00:18:29.000
Cyber threats, they have a really profound human impact. Could you share some insights and examples of how cyber attacks directly affect people's lives and essential services?

00:18:29.000 --> 00:18:45.000
So thank you so much for this question, because I think it's also it's very much at the core of why the Institute basically was created to expose the human harm of cyber threats. And this was just a very short context so the institute was launched at the end of 2019.

00:18:45.000 --> 00:18:52.000
Which means that we became operational at the beginning of 2020, right in time for when COVID hit.

00:18:52.000 --> 00:19:04.000
Which was not a great timing. But at the same time, we tried to never waste a good crisis. So we try to transform the expertise that we had in the institute in, okay, how we can help.

00:19:04.000 --> 00:19:29.000
And notably, as you all remember, there was also a sort of like hype in attacks against, for example, healthcare infrastructure and the healthcare supply chain, because before you mentioned the supply chain And with, I mean, with the many experts try to understand what was happening in terms of like the technical impact of the attack, as you very well said before, like the financial impact of the attack and so on and so forth.

00:19:29.000 --> 00:19:33.000
One question that we started asking ourselves was like, but what it means for society.

00:19:33.000 --> 00:20:02.000
What it means in terms of like how many people cannot get the vaccine because the hospital is blocked because of our ransomware. How many ambulances redirected? How many people could not get the surgery? How many people could not enter maybe certain medical facilities? Because I mean, mostly in our digitized society, everything is controlled by technology. So this is

why we produced, well, besides the report, but we also try to visualize this on a platform that is still available

00:20:02.000 --> 00:20:32.000
The data is a little bit outdated now, but it was specifically showing how basically for every cyber attack, specifically hitting healthcare infrastructure besides the i mean the the records that were leaked besides the disruption days and so on and so forth what it means in terms of actual human harm and societal impact. Similarly, we adopted the same approach when it comes to the, unfortunately, to the Ukraine conflict. So what happened was that

00:20:38.000 --> 00:21:02.000
Again, the kind of like the motivation was a little bit that there was a big hype in terms of like many experts are saying, well, there are no big cyber attacks happening in the context of the Ukraine conflict. And we were like, well, but there are the simple fact is that they are not, let's say, maybe reaching the threshold that, I mean, the whole world would stop. But for example.

00:21:02.000 --> 00:21:09.000
The attacks against the public administration entities, for example, in Ukraine.

00:21:09.000 --> 00:21:18.000
And also in other countries were constant, which means impacting the life of people because you cannot get access to your documents.

00:21:18.000 --> 00:21:26.000
Yeah. Yeah, yeah.

00:21:26.000 --> 00:21:27.000
The human.

00:21:27.000 --> 00:21:40.000
Understood your basic services and their comes exactly what you mentioned in terms of like the harm because the harm is not only again I mean, okay, the disruption days or the cost to recover a certain system, but it's also the psychological fatigue of people that are under attack let's say under

00:21:40.000 --> 00:21:41.000
And not able to sort of access their services. Absolutely, yeah.

00:21:41.000 --> 00:21:51.000
Yes, exactly. And so how we measured this and to measure this, we develop also a specific methodology is available on our website. I can also put it in the chat.

00:21:51.000 --> 00:22:01.000

Francesca, let's come back to that. That's fantastic. I want to make sure that we have a chance to sort of hear from Ilana and Jonathan as well. I think those examples of healthcare.

00:22:01.000 --> 00:22:08.000
What's happening in Ukraine, really bring home the reality of like actual citizens who are sort of being impacted by these events.

00:22:08.000 --> 00:22:15.000
And I see Doug has helpfully posted in the chat there a link to the Cyber Peace Institute. There's a lot going on there.

00:22:15.000 --> 00:22:27.000
Ilana, coming to you as well, I mean, when we sort of met before this call, you said in passing, you know, part of your job is like hacking the Pentagon, which I kind of love, right? And many people's jobs are hacking the Pentagon.

00:22:27.000 --> 00:22:43.000
You must have seen so many things during your career, had a lot of experience, but I'm wondering if there was a specific example that you wanted to share with the team. Could you tell us about a cyber attack or a security breach from your time working for the US government? What happened? How did you respond? What lessons did you draw?

00:22:43.000 --> 00:23:01.000
Sure. Yes. I mean, this section could be called Lessons Learned the Hard Way, right? And like learn from our mistakes. So I worked in the White House during the time that the White House or the US Office of Personnel Management was attacked by a nation state.

00:23:01.000 --> 00:23:20.000
They took the personnel records of 20 million civilian personnel And over a billion records. I remember being in the White House Situation Room where when they briefed us on the number of records that were exfiltrated. And I just remember writing like

00:23:20.000 --> 00:23:30.000
Oh shit and passing it back to my staff behind me. It was like, you know, one of those moments where you just realize like the gravity of what's at stake here.

00:23:30.000 --> 00:24:00.000
And the um The problem, the reason that they got in was essentially we had very, very old infrastructure. In fact, the actor had gotten in some time before, but actually didn't, there wasn't anybody that had the technology or the know-how to actually exfiltrate the documents because the system was so old. And so it didn't have the actual capability of monitoring it either. So I would say number one, spend the funds on modernization. Right. If you have vulnerable and outdated

00:24:04.000 --> 00:24:19.000
Components, you're not going to be able to track effectively what's going on on your system. And so that was a lesson learned the hard way. And especially in the government, it's hard to get those funds necessary to be able to provide those updates, but it's really essential.

00:24:19.000 --> 00:24:45.000
The other thing I would say is make sure you're investing in like constant diagnostics and monitoring. So, you know, one of the things that came out of the OPM breach was President Obama at the time pulled us all together and said, okay, you have a blue sky. What do you want to do on cyber? You tell me what we need to do to fix this. And we all got in a room together and kind of

00:24:45.000 --> 00:25:15.000
Came up with our list of best ideas. At the time, someone said, let's start a government bug bounty program. And I'll explain later what that is, but it's essentially a system in which you have constant monitoring of the systems because you have good faith or ethical researchers who are helping to make sure that your systems are secure. And so that is what ultimately became the hack the Pentagon program, we asked people to make sure that we were able to identify vulnerabilities and fix them

00:25:15.000 --> 00:25:34.000
Before they were exploited by cyber criminals. And now, 10 years later, since that incident, I think the Pentagon has identified almost 50,000 vulnerabilities that they've been able to actually action and prevent from being exploited. So I would say invest in that.

00:25:34.000 --> 00:25:39.000
And then the last thing I would say is think outside the box with respect to your cyber talent.

00:25:39.000 --> 00:26:04.000
You know, this is a government-wide problem. And we are too often focused on a particular like a particular type of cyber talent, which is often short, frankly, especially when it comes to recruiting them to the government. So really think outside the box. I think Jonathan could probably speak about how the UK digital service thinks about it and certainly how the US digital service

00:26:04.000 --> 00:26:16.000
Thought about what it took to actually get the right people into the US government or into the government in order to be able to attack this Huge problem. So those are the lessons I learned.

00:26:16.000 --> 00:26:17.000
Again, the hard way.

00:26:17.000 --> 00:26:25.000

Yeah, the hard way. I mean, and so everyone on this call, you don't have to go through a massive breach and hack to learn these things.

00:26:25.000 --> 00:26:33.000
Jonathan, you know, really happy if you want to respond to Ilana's sort of question around how the GDS is approaching this. I guess my broad question was.

00:26:33.000 --> 00:26:47.000
How can governments ensure that essential public services remain secure and resilient as well as accessible? I mean, is the balance between service security and usability a zero sum game? But we'd really love to hear from your perspective at GDS.

00:26:47.000 --> 00:26:51.000
Oh, yeah. There's kind of a few components to that question, I think.

00:26:51.000 --> 00:26:59.000
I think I'll start off with the fact that cyber is obviously like a really complicated area. It's really complex. There's lots of different things that you can do.

00:26:59.000 --> 00:27:15.000
And it's really hard to know which things that you should focus on because there's no silver bullet that will solve all of your problems. Save maybe like turning the systems off, but that's not really a viable option. Vendors will try and sell you things like zero trust and whatnot to try and get you uh

00:27:15.000 --> 00:27:29.000
To try and get you buying their stuff. But the reality is there's no one thing that you need to do to kind of fix all of the problems That's where I think a lot of the value that you can use in a practical sense is from the frameworks that exist for cybersecurity.

00:27:29.000 --> 00:27:48.000
Things like NIST, ISO 27001. We've got the cyber assessment framework here in the UK. So if you look up NCSC, have a look at their framework and it really helps you as an organization in the public sector to look at the different kind of areas where you need to have some competency and to kind of have some controls in place because

00:27:48.000 --> 00:27:53.000
I think cyber is increasingly about doing a lot of fairly basic things well.

00:27:53.000 --> 00:28:15.000
And being able to manage those things on a consistent basis as well. We see frequently attacks that are caused by You know, someone thinks, oh, I've got good protections in a number of areas, but they've kind of forgotten about managing this one thing that they needed to be doing

a bit better. So I think it really is about bringing together those different control sets and having that joined up viewers to

00:28:15.000 --> 00:28:20.000
How to protect the things that you care about and not just like picking one shiny thing and trying to jam it in.

00:28:20.000 --> 00:28:29.000
And hoping that it keeps things protected. Regarding the accessibility and usability stuff, I don't think it is zero sum.

00:28:29.000 --> 00:28:41.000
I do think there's often a right way to approach building services. And I don't think that so like kind of a more traditional view on security was perhaps that it was a blocker and that it could stop people from building good services.

00:28:41.000 --> 00:28:49.000
At GDS, we found that's not the case. You can bake security into how you approach things. We've got things like the secure by design framework, which is another framework I didn't mention before.

00:28:49.000 --> 00:28:58.000
That really helps consider how to design user-friendly useful services in a way that is actually secure.

00:28:58.000 --> 00:29:12.000
And when there are really difficult areas where you can't do that, we find other ways around. So like our digital identity identity service has like an in-person route that you can take if you can't for some reason access the digital routes that are available.

00:29:12.000 --> 00:29:22.000
Just to speak briefly to Alana's point as well on kind of bringing talent in, it is a really difficult thing. We rely heavily on apprenticeships training schemes.

00:29:22.000 --> 00:29:39.000
The UK government runs a number of initiatives around like what we call fast streamers which kind of like graduate entrance to the civil service who get trained up in various cyber kind of related competencies We also have an apprenticeship scheme. We've got a career changers

00:29:39.000 --> 00:29:51.000
Boot camp that the Department for Work and Pensions run So we're just about to have two excellent candidates join us who have come from quite disparate backgrounds, which I think is kind of what Alana was referring to when she talked about

00:29:51.000 --> 00:30:00.000
Looking at the kind of outside the usual suspects for where you might get cyber capability from. Not everybody needs to be an IT graduate to come and work in cybersecurity.

00:30:00.000 --> 00:30:05.000
In fact, my boss, our chief information security officer, used to be a music teacher and he's very, very good.

00:30:05.000 --> 00:30:17.000
Yeah, yeah. Yeah, I think it's such an interesting, as cybersecurity, like so many 21st century government challenges becomes a hall of government challenge.

00:30:17.000 --> 00:30:32.000
It's no longer the realm of just like experts with five advanced degrees. It's about a mindset and approach to problem solving and broadening that talent base. So I think that's really exciting that folks who can tackle this problem that that pool is starting to widen a little bit.

00:30:32.000 --> 00:30:47.000
Francesca, I wanted to come to you. So, I mean, let me put a similar version of what I put to Jonathan there. I mean, in your view and your experience, how can governments ensure that essential public services remain both secure but also resilient. What have you learned about that?

00:30:47.000 --> 00:31:17.000
So let me share maybe one thing, let's say one level up to what was said so far and going back to, let's say I spent more than 10 years at the more than 15 years at the UN. So working with the states as counterparts in a way. I would say prioritize the cybersecurity and national security frameworks. And I'm saying this again and again, because governments must recognize cybersecurity as a fundamental component of national security, so not an IT issue. I know that I'm sure most of the, let's say government representatives here in the chat

00:31:21.000 --> 00:31:51.000
In the webinar are well aware of this, but still, and I've seen this because I spent all my life in cybersecurity that has been, let's say, historically treated in a silo in a way approach whilst we need to, it's a key component of security frameworks. And then let me finish just maybe adding I mean, plus one to all what Elon and Jonathan mentioned. And I'm glad that the specific list was mentioned, the development of a skilled, let's say cybersecurity workforces specifically in government

00:31:59.000 --> 00:32:00.000
Hmm.

00:32:00.000 --> 00:32:14.000

Also thinking about what I call the non-usual talent, let's say, with a career path. I would say also in terms of like mindset, and I loved what you mentioned in terms of like the culture of cybersecurity started with a resilience first approach. So always start the thinking.

00:32:14.000 --> 00:32:44.000
Before the next shiny object in what Jonathan was mentioning, ensured that public services can continue to function even if they are targeted. So which means implementing very let's say basic things like redundant systems, backup processes, the contingency plans, and so on and so forth. So also to what was mentioned before. And I would say just to add to what was already mentioned, always test a cyber emergency response plans regularly. Maybe just one last point would be

00:32:44.000 --> 00:33:02.000
In more regarding the multi-stakeholder collaboration, so public-private partnership but also working with different actors it's key nowadays because everything is interconnected Even more than before. So it's still one of the challenges that I still see there is threat intelligence.

00:33:02.000 --> 00:33:06.000
So threat intel mechanisms that are really working are very hard.

00:33:06.000 --> 00:33:11.000
To define.

00:33:11.000 --> 00:33:13.000
Oh, for me, Francesca, you've froze a little.

00:33:13.000 --> 00:33:21.000
But yeah. No, so just to mention threat intel it's definitely key, but still very challenging

00:33:21.000 --> 00:33:37.000
Thanks, Francesca. Thanks for repeating that. You just glitched a little at the end, but I think repeating it really helped. I mean, I'm heartened by this conversation and for everyone on this call because There's obviously the investment component, Ilana, that you spoke about. Governments need to invest in getting that infrastructure right.

00:33:37.000 --> 00:33:43.000
But there's also something about building a culture and having a conversation like the mindset as a team that's immediately implementable.

00:33:43.000 --> 00:33:51.000
That's something that everyone on this call in your teams and government, you could sit down and say as an organization, are we approaching this? Is this fed into our work every day?

00:33:51.000 --> 00:33:58.000

That can really help with not feeling that it's all the bar is so high to make a difference with cybersecurity that it's like almost unattainable.

00:33:58.000 --> 00:34:08.000
I want to double click on something which has come up in this call, but we've kind of glossed over it. And Ilana, you teased us on this, and that is AI, right? So AI is like supercharging cyber threats.

00:34:08.000 --> 00:34:15.000
What risks do they pose so AI sort of supercharged cyber threats to public sector digital services?

00:34:15.000 --> 00:34:19.000
And how should governments be thinking about this and prepare?

00:34:19.000 --> 00:34:49.000
Well, in a way, everything old is new again. And in that way, I mean, the AI driven cyber threats, as Francesca said, they've been democratized. I think it's as like lowering the bar to entry so many more participants who are able to use AI bots that are designed to impersonate trusted individuals with just alarming accuracy. So in a way, really, all we can really do with our core security practices is rely on trust, personal relationships in order to actually secure things.

00:34:53.000 --> 00:35:06.000
And so when Naditepid can mimic a writing style or a speech pattern or, you know, even like create some kind of emotional cue that can bypass some traditional security measure.

00:35:06.000 --> 00:35:11.000
Then we're going to have a hard time. Now there are, you know.

00:35:11.000 --> 00:35:23.000
There are systems that are also being developed that are able to identify when AI is being used, but they are frankly not being developed with the same pace.

00:35:23.000 --> 00:35:32.000
That the bots and other harmful uh AI tools are being developed.

00:35:32.000 --> 00:35:45.000
And then similarly, I would say folks can rely on AI to write malicious code, right? So that's another way in which we have a lower barrier to entry.

00:35:45.000 --> 00:35:55.000
And again, that's why you just need constant monitoring, constant supervision, constant attention in order to be able to address all of these different risks.

00:35:55.000 --> 00:36:10.000
But really, it's not a new, in some ways, it's not really a new tool or a new technique that people are using. It's just the means by which they actually deploy that technique in order to ultimately evade all of our traditional security methods.

00:36:10.000 --> 00:36:16.000
Yeah, and you almost have to sort of develop like a new literacy around it, right?

00:36:16.000 --> 00:36:21.000
We've just had a conversation in my family, which is spread all over the world about, you know.

00:36:21.000 --> 00:36:26.000
Should one of us be contacted by someone calling or sending an email?

00:36:26.000 --> 00:36:40.000
That we have some sort of code word as a family to just ensure that it's not a deep fake. And it's just amazing that we've kind of reached that stage where that's a concern. My elderly father, I'm constantly amazed with how many sort of

00:36:40.000 --> 00:36:49.000
Bonkers threats he sort of is sent, emailed, WhatsApped, et cetera. It really is like a staggeringly fast moving environment.

00:36:49.000 --> 00:37:06.000
Well, it's interesting. My parents or somebody will like with some of our elderly family members will pick up the phone and answer the answer a call to someone they don't know and sort of answer questions.

00:37:06.000 --> 00:37:07.000
Yeah.

00:37:07.000 --> 00:37:17.000
And I try to explain to them that that's like When I was little, they would say, don't open the door to strangers because it was like dangerous. And I'm like, you are, this is the same. This is the modern day equivalent. You are opening the door to strangers because they can then impersonate your voice. So I was like, don't answer the phone if you don't know.

00:37:17.000 --> 00:37:18.000
Yeah, yeah, yeah. Yeah, that's exactly right.

00:37:18.000 --> 00:37:24.000
Right. It's a whole new set of instructions.

00:37:24.000 --> 00:37:38.000

I want to zoom out a little bit and talk about sort of international cooperation, because one of the things about cyber threats as we started to cover here is that it knows no borders, right? It's just the whole world. And that's something that all three of you as experts and thinkers are working a lot on.

00:37:38.000 --> 00:37:45.000
Jonathan, developing cybersecurity norms at the international level, it's really crucial for stability.

00:37:45.000 --> 00:38:03.000
But so is the development of awareness internally. Before we get to the practical steps of public servants, it would be really useful just to have a bit of a chat about how does GDS think about relating to an organization like Ilana's or connecting with Francesca's, how are you approaching the sort of international cooperation side of things?

00:38:03.000 --> 00:38:08.000
And Francesca, I'm going to come to you afterwards because I know this is an area you work in a lot.

00:38:08.000 --> 00:38:31.000
Yeah, I mean, it's absolutely essential to our success to be able to rely on organizations like hacker one and like the Center for Internet Safety. I've forgotten the exact name of it sorry um But we heavily rely on our international partners. We actually really often go through our national agency of expertise, which is the National Cybersecurity Centre.

00:38:31.000 --> 00:38:40.000
They are handling a lot of our interrelationships with the intelligence community as well as other agencies around the world.

00:38:40.000 --> 00:38:49.000
To make sure that we have relevant threat information to help kind of inform the decisions we're making about controls we're implementing and how we're managing risk on a daily basis.

00:38:49.000 --> 00:39:00.000
And obviously organizations like Hacker One and some of the solutions that they offer are kind of one of the core controls that we rely on to make sure that our systems are Free of bugs through the bug bounty program.

00:39:00.000 --> 00:39:05.000
I will defer back to Alana and Francesca to add to that.

00:39:05.000 --> 00:39:20.000
Yeah, Francesca, you've worked so much in sort of international cooperation. Do you want to share a little bit about how you're thinking about how organizations should be talking to each

other, maybe governments should be connecting around a more joined up international framework for cybersecurity?

00:39:20.000 --> 00:39:40.000
Thanks for the question. So I would say, well. Couple of levels. One level is one level It's absolutely key, especially nowadays, I would say, especially for the geopolitical tension that we're seeing that governments, they need to participate. I see it as a

00:39:40.000 --> 00:40:10.000
As a sort of like moral obligation for governments to participate also to the international discussion. There are several avenues. Notably, when I'm thinking about cybersecurity, I would say the United Nations Open Ended Working Group. This cycle, because it's a five-year cycle, is coming to an end in July, but I'm mentioning this specifically because there will be most probably let's say a permanent body that will be created with the possibility for both member states but also non-state actors in terms of like, for example, other international organizations, academia, civil society to participate.

00:40:23.000 --> 00:40:53.000
To the discussion shaping basically cybersecurity at the international level. I mentioned in this specifically because in this framework, there was the establishment of norms of responsible state behavior, what it means specifically when it comes to attacks against the critical infrastructure and so on and so forth. So it's key to participate and also in a way to be able, thanks to the participation to this let's say to these processes to be able to work more with other states, for example, and also with the entities, as Jonathan was mentioning, that are not necessarily, let's say

00:40:58.000 --> 00:41:21.000
The immediate, I would say the immediate counterpart for a state. And maybe the second level is, okay, what we do concretely. And there are several avenues. On our side, and I mean, we can also talk later and I will put some some links in the chat, but very practically speaking. So one of the reasons why this was created was to provide the data.

00:41:21.000 --> 00:41:32.000
And evidence-driven knowledge to member states to then improve basically their policymaking when it comes to cyber. And then secondly, support those initiatives I'm mentioning specifically one, Common Good Cyber.

00:41:32.000 --> 00:41:46.000
That aims basically to foster cybersecurity as a global public good. So working with nonprofit and research institution to develop and support open source public entrance of cybersecurity tools.

00:41:46.000 --> 00:42:04.000

That's really exciting. Please do pass those links into the chat. Just, you know, really interesting to see that sort of cooperation happening. Ilana, coming to you. So there's, I'm sure there's burgeoning legislative frameworks in countries all around the world. We've got folks on this call. They will all have their own national country's legislative framework around cyber attack.

00:42:04.000 --> 00:42:15.000
But there are also a whole lot of voluntary standards, a whole lot of sort of international cooperation. I mean, how are you thinking about this in your work? How does HackerOne contributing to the international conversation?

00:42:15.000 --> 00:42:26.000
Sure. Yeah. Well, thank you for that question. So we at HackerOne do a variety of different things. We do a bug bounty program, a vulnerability disclosure, and we do AI red teaming and I'll explain what all of that is.

00:42:26.000 --> 00:42:40.000
And actually, one of the things that drew me to this company is the work that we do for governments. As a former government employee myself, it's very important to me to be able to protect government systems and data. I think it's just essential.

00:42:40.000 --> 00:42:41.000
Yeah.

00:42:41.000 --> 00:42:57.000
In the US and the UK, we've over a decade of experience helping to run programs that are essentially What we do is we marry up good faith researchers with these government programs in order to allow them to report vulnerabilities

00:42:57.000 --> 00:43:22.000
Before the malicious actors can exploit them. And that is a best practice. It's something that is actually that the US government has said is one of the most cost effective cybersecurity programs that you can have. It's a requirement in the US for all of the government agencies to run those types of programs. And it's increasingly becoming a requirement across the globe.

00:43:22.000 --> 00:43:28.000
So we have what's called a vulnerability disclosure policy map on our website. I don't know if you can pull that up.

00:43:28.000 --> 00:43:34.000
Yes, I'll ask our tech support if they can share it. Sorry, Alana, please carry on.

00:43:34.000 --> 00:44:02.000
No, no, no, that's great. And so that's one of the things actually that we do is we help to monitor this practice across the world. So it's sometimes required for the US government, but other

times it's a requirement just for a particular industry within a country or it's a requirement for the EU member states. So we have, if you go to the website and you go to this policy map, you can You know, either scroll over the country or the region that you're looking at or scroll over your specific country or region

00:44:02.000 --> 00:44:22.000
To try to determine what is actually required and then use that in order to advocate for implementing it within your own you know department because again it is the most cost effective way that you can reduce vulnerabilities is to catch them in advance. Another thing that we often talk about for some of our

00:44:22.000 --> 00:44:35.000
In government programs, you don't always have to pay. Frankly, people really love hacking the Pentagon, even if they don't get a bounty for it, even if they don't get paid for it. It's just like a cachet associated with saying like, I have into the Pentagon?

00:44:35.000 --> 00:44:58.000
But for those of our customers that do pay, the average bounty or payment for a vulnerability is about $1,000, whereas the average cost of a breach in the US is about four and a half million dollars. So there's an obvious incentive to trying to get these things done and addressed in advance.

00:44:58.000 --> 00:45:10.000
That's a super useful resource. I'm going to ask Doug, who's our tech support, if there's an opportunity to just sort of pull up the map that Ilana was referring to. It would be really useful to just show folks because it's a practical resource.

00:45:10.000 --> 00:45:19.000
Where you can just kind of scan over it and have a look at what your country is doing. I'm sure there are lots of people on this call from different backgrounds who want to have a look at it.

00:45:19.000 --> 00:45:27.000
So let us know, Doug, if you're able to share that. If not, I'm going to move on with another question.

00:45:27.000 --> 00:45:31.000
Silence from Doug. Okay, so we'll carry on. That's really useful. So we've sort of looking at Oh, there it is. He's there. Right.

00:45:31.000 --> 00:45:46.000
Oh, there it is. Yeah. Right. Yeah. So all you have to do is just, you know, put in your country, you can scroll down, select the country that you want, and then it will pull up like you can put the UK as a number of different standards.

00:45:46.000 --> 00:46:01.000
For example, or whatever you choose. And then it will identify all the different requirements, whether it's a recommendation or a requirement, anything that you want that you can and where the where the the authority is that drives the requirement.

00:46:01.000 --> 00:46:09.000
Sort of a shared resource there for that global vulnerability disclosure policy map. Really, really useful. We'll share the link there as well.

00:46:09.000 --> 00:46:14.000
Yeah, really fantastic to see. You can find your country if you're there as well.

00:46:14.000 --> 00:46:30.000
Yeah, I think thinking about that international piece is so important because there's got to be that cooperation, maybe even finding sort of organizations and our communities are a great place to sort of chat to other departments or organizations battling with some of those challenges. How are you approaching it?

00:46:30.000 --> 00:46:49.000
We've got a couple of questions. And then I want to bring it back to sort of practical steps that everyone on this call could take, because I think that's really useful as we close off just to bring it back to like practical things that everyone can do. But we have a great question in the chat on monitoring. And you've mentioned this a couple of times, Ilana, like the need for constantly monitoring.

00:46:49.000 --> 00:47:01.000
But Jonathan, I'm going to throw it to you first. Deshawn asked, what type of monitoring system would you recommend to monitor our networks? Like when we talk about monitoring, what are the different kinds of monitoring? What does that look like?

00:47:01.000 --> 00:47:08.000
Yeah, I mean, principally, we're looking at technical monitoring of the different components of the services that we offer.

00:47:08.000 --> 00:47:32.000
There are a number of proprietary tools, but there's things like Splunk and other security incident event management system so seams which gather together all of the data that you're relevant bits of system that relevant devices are kind of continuously logging, capturing that information. And you want to be able to bring that all together in a way that helps you manage and assess whether anything unusual is going on.

00:47:32.000 --> 00:47:46.000
Often with these tool sets, you can bring together a big picture of all this data and set alerts on what looks like suspicious behavior, what looks like things that might be getting and set alerts

that then trigger and let people go away and investigate those things a little bit more. So for example.

00:47:46.000 --> 00:47:56.000
If I tried to log into my laptop multiple times. It might trigger an alert somewhere in our monitoring center that says, hey, Jonathan's failed to log into his laptop.

00:47:56.000 --> 00:48:05.000
10 times in a row. This is a bit weird. Maybe something's happening. And then you go on and look at it and go, hey, actually, he's trying to log in from the other side of the world. He's not supposed to be over there.

00:48:05.000 --> 00:48:10.000
And that will give you a good idea as to like, you know, when strange things are happening.

00:48:10.000 --> 00:48:17.000
But having that coverage and that continuous view of the sort of the health of your system through those monitoring technologies is really important.

00:48:17.000 --> 00:48:31.000
Being able to identify when something is going on is kind of the first step in responding to an incident. It's like figuring out that you have something going on as Alana mentioned, but the opm breach The actor was actually there for a while before they were able to pick up.

00:48:31.000 --> 00:48:32.000
Quite a while, yeah.

00:48:32.000 --> 00:48:48.000
Really important. Yeah, so it's kind of there's a lot of proprietary technologies and a lot of approaches to it but that is the the fundamental approach. So I think There's a number of tools that you could use. I'm not going to recommend any specific one, trying to be impartial but um

00:48:48.000 --> 00:48:52.000
Yeah, there's lots of ways to do it. I don't know if my colleagues would add to that all.

00:48:52.000 --> 00:49:02.000
Can I just add one thing, which is that it's true, all of those practices are super essential. We all have policies that we put in place that are considered, you know.

00:49:02.000 --> 00:49:27.000
Effective at preventing breaches. But as a government official, as a former government official, I'll tell you, oftentimes the actor who exploits finds the one person who has not followed the policy, right? So the person who has not somehow disabled multi-factor authentication or the person who has, you know, essentially evaded whatever control you've put in place.

00:49:27.000 --> 00:49:49.000
So as important as putting those policies in place is a constant vigilance to making sure that everyone is following them. I know that's stating the obvious, but it is really important to actually pay close attention to that. And a lot of times we just focus on, okay, we've implemented this. Everyone should be following it, but we're not paying enough attention to like who is not following those protocols. And that's where

00:49:49.000 --> 00:49:50.000
You get in trouble.

00:49:50.000 --> 00:50:09.000
Yeah. Yeah. It's about that whole ecosystem kind of approach We were talking about AI and we've got such an interesting question from Jacqueline here, which I want to share. She's got a slightly different question around AI. So going back to AI-driven cyber threats, how do you see the future of cybersecurity roles within organizations?

00:50:09.000 --> 00:50:26.000
Which roles are likely to be replaced by AI in incident management, for instance, and what new roles might emerge. Francesca, do you want to have a first go at that? What does a government team look like in five years time that works on cybersecurity?

00:50:26.000 --> 00:50:28.000
Oh, you're on mute, I think, Frances. Yeah.

00:50:28.000 --> 00:50:58.000
I'm on mute. Yes, obviously it should happen. So I was about to say that that's interesting because to me, the first things that comes to mind is even when you apply basically AI nowadays in an organization do it in a responsible way which means, again, and I mentioned this specifically thinking about, let's say, adopting responsible AI when it comes to the workplace. It involves also the workplace ethic.

00:51:02.000 --> 00:51:29.000
And in terms of like which are the, let's say the roles that you want to keep in a way and having it in a sort of like intentional way. So don't adopt, let's say tools and services, but I guess that micro working in government would agree with that simply because again is the is the next um uh let's say ai driven uh marketing uh tool

00:51:29.000 --> 00:51:49.000
I would say that most probably the most, I would say administrative back off office functions the data processing and analysis. And also, I would say the basic IT support we've seen already. I mean, this happening when it comes to the

00:51:49.000 --> 00:52:06.000

I mean, to governments that we've been discussing with. I would say that some roles might be augmented. I mean, not necessarily replaced. And where I see the superpower in a way might be, for example, for cybersecurity experts or policy analysts, for example.

00:52:06.000 --> 00:52:36.000
Within cybersecurity teams. And why not? I mean, I know I'm trying to see the glass half a full maybe here, but there are also some roles that might be created And I'm thinking, for example, about all those officers that you might need specifically to look of how AI is implemented. I'm thinking about some emerging roles that we've seen across different geographies like the AI ethics ones, the cyber resilience engineers, for example, specific disinformation analyst in the team, prompt engineers.

00:52:43.000 --> 00:52:58.000
I think we should rethink, let's say, the workplace functions But not necessarily just in a sort of like a negative way.

00:52:58.000 --> 00:52:59.000
No need to raise. Jump in, Jonathan, by all means.

00:52:59.000 --> 00:53:10.000
I was trying to figure out how to raise my hand and add to what Francesca was So yeah, I think Francesca's spot on that AI is really likely to augment capabilities that we already have in cyber teams. I don't think they're going to be replacing anybody in the short term.

00:53:10.000 --> 00:53:17.000
But in the same way that we were talking earlier about how AI tools have kind of democratized access to enhance capabilities.

00:53:17.000 --> 00:53:27.000
That goes the other way too, right? The bad guys can use AI tools to figure out how to do things. We can use AI tools to enhance how we do lots of things as well on the good guy side. Well, I think I'm a good guy because I'm trying to protect stuff. But anyway.

00:53:27.000 --> 00:53:29.000
Be the bad guys. Yeah, it's pretty good.

00:53:29.000 --> 00:53:43.000
It'll be a bug guidance. Let's not talk about that. So, yeah, we could use AI tooling to really enhance some of our static and dynamic application security testing that we do to like pick up some of those bugs that might otherwise have kind of made it out the door.

00:53:43.000 --> 00:53:51.000
We know that hostile actors are using it to pick up zero day vulnerabilities through means like that. So maybe we can start stopping more of those things.

00:53:51.000 --> 00:54:00.000
So I think it's really going to be a part of like the cat and mouse experience that we often have in security of trying to kind of keep pace with what the bad guys are doing.

00:54:00.000 --> 00:54:15.000
And AI is definitely just another tool for doing that. In terms of new roles and things like that, I don't foresee any right now, but as things are progressing very rapidly, perhaps there will be some in the near future.

00:54:15.000 --> 00:54:16.000
Yeah, go for it.

00:54:16.000 --> 00:54:31.000
Yeah, I just can I, I know. It's another person saying the same thing, but in a different way. So I'll make it quick. But like the best security is really, you know, a combination of human ingenuity with the best automation possible and available. And so AI is just a new version of that, right? It's just the next step in that iteration.

00:54:31.000 --> 00:54:38.000
There's a lot of times where folks are using AI just to automate repetitive tasks or scan a vast amount of data or, you know.

00:54:38.000 --> 00:54:56.000
Identify in our case, you know, potential vulnerabilities, but you really need to have that human in the loop In order to be able to ultimately make it useful and productive. So I don't see it as replacing, but just making us all much more efficient, effective and quicker at being able to identify the things that we have to

00:54:56.000 --> 00:54:58.000
Identified fix.

00:54:58.000 --> 00:55:08.000
Yeah, so Jacqueline, I hope the answer from our experts sort of is heartening that it's more likely to sort of augment, be a companion that kind of works with you to be more effective.

00:55:08.000 --> 00:55:19.000
We're coming up for time. So we have a final question here and I'm going to ask each of our experts to sort of answer it in quite a sort of lightning mode. But I think it really comes back to the like practical steps here, right?

00:55:19.000 --> 00:55:30.000

Someone says, I'm a systems manager for the UK government working in counter fraud, bribery and corruption. I have no formal IT digital or data training. However, I build and debug dashboards and spreadsheets daily.

00:55:30.000 --> 00:55:37.000
What formal training or other ways of entering the cybersecurity area of work would you suggest for me and others like me?

00:55:37.000 --> 00:55:59.000
I'm going to actually broaden this question a little bit and just say, what would your top tip top takeaway tip B, Jonathan, Ilana, Francesco, for those watching today, how can they increase their cyber awareness How can they improve their cyber literacy and what's a practical thing they could do taking away from today? I'll go Jonathan, Francesca, Elana.

00:55:59.000 --> 00:56:06.000
Sure, okay. Yeah, I think there are so many resources out there that you can access for free today. We were talking about YouTube earlier. We've talked about other things.

00:56:06.000 --> 00:56:12.000
There are a ton of things that you can access for free. There are free courses available online from recognized institutions.

00:56:12.000 --> 00:56:19.000
To really upskill yourself in terms of cybersecurity capabilities for the person that asked the question specifically on the chart.

00:56:19.000 --> 00:56:24.000
You've clearly got some digital skills which are highly relevant to what we do in cyber a lot of the time.

00:56:24.000 --> 00:56:31.000
So I would start to look at some of the vast training materials available out there.

00:56:31.000 --> 00:56:33.000
There are a bunch of entry-level courses as well that you can get access to.

00:56:33.000 --> 00:56:51.000
But I also mentioned earlier on, we've got a, in the UK, we've got the DWP security academy um and basically that's for like career changes so that's exactly the kind of thing that we're looking to bring people like yourself in through. And obviously there's nothing stopping you from applying like i think

00:56:51.000 --> 00:57:01.000

We recognized as a panel We're kind of moving away from that traditional we need people that are IT graduates to come and work in cybersecurity. We're looking for the people with the right behaviors, the right attitudes.

00:57:01.000 --> 00:57:11.000
And we can train skills. And I think the skill shortage has really highlighted the fact that we need to be able to do that and we need to be able to bring people in with those behaviors and attitudes that we want.

00:57:11.000 --> 00:57:14.000
I'll leave it there.

00:57:14.000 --> 00:57:15.000
Francesca.

00:57:15.000 --> 00:57:33.000
Thank you so much. And I mean, I cannot agree more. I would say a couple of things. So first of all, thanks for mentioning the fact that there are tons of like free resources out there. So definitely start there. There are also some international organizations that are

00:57:33.000 --> 00:58:03.000
Publishing kind of like very basic and hands-on kind of like a toolkit. When I'm saying international organization, I'm thinking, I mean, both big organization like Aniza and so on and so forth, but also like civil society organization also our peers let's say also share some some links in the chat. So start with that. Also, as much as possible, my suggestion would be to try also to get into any kind of like cyber drills competition scenario based type of training because these are extremely helpful because you learn by doing basically and also by interacting with people. I mean, for example, I'm judging in a couple of like cyber competition and I'm mentoring

00:58:17.000 --> 00:58:42.000
In this case, specifically Women for Cyber program But the width, I mean, the person that have no, let's say formal let's say IT or engineering background that wants to pivot into cyber. And the first thing that I'm saying is be curious, always, let's say, try to educate yourself with the free resources, but also try to get your hands dirty in a way.

00:58:42.000 --> 00:58:47.000
With this sort of like more kind of like exercises scenarios, simulation because they are extremely helpful

00:58:47.000 --> 00:58:55.000
Practical Fantastic. Okay, with one minute to go before we wrap up, Ilana, what is your tip for everyone?

00:58:55.000 --> 00:59:10.000

Well, I agree with everyone on the panel so far. And I would just like to say, if you are a woman who is interested in learning more about cybersecurity and specifically bug bounty, this is something that at HackerOne, we are really focused on.

00:59:10.000 --> 00:59:37.000
Female community of hackers is too small. So with Capital One and GitHub, we sponsor an annual conference for free that teaches women specifically how about cybersecurity and then also about how to hack, how to be an ethical researcher. But it's not just us. Obviously, there's a multitude of these programs. And, you know, I think we could probably put our heads together and come up with a resource list for everyone who's

00:59:37.000 --> 00:59:42.000
Who's participating here so that they can decide that they want to get involved.

00:59:42.000 --> 00:59:56.000
We'd love to do that. It just gives you a sense of how broad the topic is. We have come to the end of today. There is so much still to cover. I wish you would just join me in a huge round of applause for our three amazing speakers, Francesca, Ilana, Jonathan. Thank you so much on this amazing topic.

00:59:56.000 --> 01:00:03.000
We are going to thank you all and let you carry on with your day. But before we do that, our team is going to pull up a quick poll.

01:00:03.000 --> 01:00:17.000
Just to help us improve our event in future, please rank your agreement with the statement This event was a good use of my time, a valuable use of your time, one meaning you completely disagree and 10 meaning you completely agree.

01:00:17.000 --> 01:00:26.000
That is all we have time for today. I hope you found it helpful. We have a lot of resources. Our speakers just have so much inside their heads, which we will make sure that we share with you afterwards.

01:00:26.000 --> 01:00:32.000
Thank you for taking time out of your busy days. Keep an eye out for the email coming your way with the recording and the resources.

01:00:32.000 --> 01:00:37.000
And we hope to see you at another apolitical event soon.

01:00:37.000 --> 01:00:43.000
Thank you again to our three speakers and have a great day, everyone. It was such a fantastic conversation. Thanks, everyone.