Hello, welcome, and thank you for joining us at the Cybersecurity in Healthcare and Pharma Summit.

I am Dr. Alon Ben-Ari I am the Chief Medical Information Officer of the Northern California VA healthcare system, one of several healthcare systems within the Veterans Health Administration. One of the nation's largest healthcare systems in the US providing integrated healthcare services to over 8M Veterans across the continental US and also out of it. I am also a clinically active physician actively taking care of our Veterans.

Slide 1:

Much has happened in the past year in cyber security and in healthcare and I wish to review some of the trends and events that have taken place this year. We will start by reviewing the HHS breaches in the cybersecurity tracker. We will add a review of IBMs Cost of Data Breach Report. Something that is of interest to me personally is ‘how does cyber security register in the clinical literature. I found this quite surprising. We cannot leave the major event of the year: Chage Healthcare. The fallout of which is only starting with recent congressional hearings. Lastly, I am sure many of you are part of efforts in digital transformation. Cybersecurity is a large topic to consider, not to call it a significant enabler of these technologies. I wish to share with you some real number about the VA’s own secure messaging system and the challenges we have with multi-factor authentication.

Slide 2

Data from the HHS cyber breaches of healthcare systems. I wish to start by highlighting the daily rate of breaches in healthcare plans, insurers etc. We are seeing an average of 2.24 event a day with STD of 1.6, the box plot on the left allows to visually appreciate the IQR of daily breaches. Roughly 1-3 breaches a day.

Slide 3

This one highlights the entities being Hacked leading the charts are the Healthcare providers, but take notice of the Healthcare Clearing Houses. We will revisit this point shortly.

Slide 4

Here we detail the Breach type, Still leading are an IT incident, but unauthorized access/disclosure are high up there as well. To my understanding this is where Phishing/Vishing comes into play.

Slide 5:

This one details the breach location. This is particularly interesting. What is known as surface attack has grown significantly in the past few years in healthcare and in other industries. Notice the ‘Network Server’ as a target for breaching, followed by emails. Typically by following an authorized link and in-advertently compromising one’s credentials. Keep that in mind for whats coming in the next few minutes.

Slide 6- 7:

IBM reports annually some statistics on the cost of breaches. Sampling 553 companies world wide on majore leading industries, healthcare included. As the landscape of scalable computing changes, its impact on cyber is also detailed. Its an interesting report that is current and responds to current technologies. I don’t know how to relate to the fact that 51% of organizations are planning to increase cyber security investments… does that mean the rest do not.? This is not entirely un heard of. Cyber ranks low in the corporate board rooms. However in light of these figures , clearly a cyber event is costly. Cyber security teams, can mitigate some of the costs and contain the damages.