

AUGUST 3, 2021

Technology Can't Be Retrograde in Protecting Critical Infrastructure

FEATURING:

Michael Brown, Rear Admiral, USN (Retired), Eclypses Board Advisor

Critical infrastructure in the United States - pipelines, electrical grids, election systems, among others - are at constant risk from hackers all over the world. It is crucial to meet technological threats with technological security advances.

In this webinar, speakers include former national security leaders who have protected national secrets, individuals on foreign assignments, and domestic infrastructure from national state attacks.

They discuss the optimal approach to staying ahead of hackers and ransomware attacks. Is our fear of and response to attacks equal to the threats that exist?

Are the crown jewels for a lot of people, the data?

"Absolutely, and that's one of the things that perhaps is missing in the discussion right now with respect to zero trust architecture. When thinking about zero trust architecture, there's an enormous amount of work being done to help define the reference architecture in the things that I mentioned in the past, but the crown jewel, as you've said, is the data - and not all data is the same priority or risk when it comes to exposure."

So knowing "where, what, how" to protect that data, I think, is critically important. Thinking about the mobile environment or, as we've been talking about with 5G and OT (Operational Technology) and so on, data is going to be pervasive. It already is, but it will become more pervasive. So what are the standards and best practices to protect that data throughout that the potential journey that they'll be on?"

Continuing on cyber security...

"In today's environment - going back to the application of technology - mobile is extremely important. It's in everybody's daily routine, so having mobile security as part of the strategy is really, critically important. We've got to be able to battle the vulnerabilities, whether they're inside the TLS protocols or otherwise. It really is important to recognize, as we both have stated, that there is no edge. Therefore, we have to prioritize and understand the uses of the technology and how it is applied and ensure that there's the appropriate security wrapped around those elements."

"Too many people ignore the cyber security, national security, and business security threats on the public safety until it is too late."

- Michael Brown, Rear Admiral, USN (Retired)