OUTSIDE THE (BLACK) BOX: PROTECTING CORE OPERATIONS IN OIL & GAS

Video Transcript

74% of all oil and gas executives said their organization is confident that their cybersecurity measures will yield valuable results.

Over three quarters believe that their strategies can effectively protect their company's reputation and information as well as prevent disruptions in service.

However, oil and gas companies surveyed reported an average of 8 cyberattacks per month over a twelve month period of time for an average of 96 cyberattacks per year with one in three of these attacks resulting in security breaches.

More concerningly, half of the companies surveyed said it took months for them to actually detect the breach.

And finally, only 18 percent of the executives surveyed were confident in their abilities to identify the high-value assets and business processes needed to protect themselves from cyber attack. Now, when reviewing the survey results, a concerning 60 percent of those same leaders said cybersecurity is a bit of a black box.

So, what does this really mean?

Well, the big question is how can we help crack open that cybersecurity black box and really understand what's inside?

The answer:

- Better investments in cybersecurity
- Improved analytics on the process control network (PCN) and industrial control system (ICS) networks.

- Invest in incident management programs for both OT and IT networks
- And test their cybersecurity plans through things like tabletop exercises and ultimately red-teaming.

As this survey illustrates, cybersecurity doesn't end at the edge of the corporate network. It includes both operational technology and back-office systems.

Therefore, having a comprehensive cybersecurity program that includes all aspects across the entire organization will help that organization be better prepared when a cyber event occurs.