1. In the govtech article, the Lear CISO discussed how traditional approaches to security training has been informational. How has he tried to change the culture at Lear to get away from this approach?

* The cybersecurity when Duby joined was infancy and was in need of some improvement.
* The Intranet with the companies has an active page which holds the articles related to Cyber Security.
* It Lacks in Global incident response capability and gathering insightful and meaningful data was a challenge.
* The process has been streamlined for reporting simple suspicions and concerns, making it easier and more intuitive.
* He has designed the security awareness training program and focused on training employees to be extensions of our security team( crowdsourcing security).
* He modified the conventional corporate training model going beyond the normal posters and email approach to awareness.

1. How has the Lear CISO changed his approach to communicating to security to employees (e.g., do the focus on broad messages to every employee?)?

* Yammer Which is internal Social media where the Security awareness programs are conducted and the voluntary groups which grew enormously from 100 to 1000 over a year.
* The Intranet with the companies has an active page which holds the articles related to Cyber Security.
* The suspicious reports which are recorded as incidents from the employees have been increased which means people are proactively aware of what they are doing and what needs to be done as a part of security.
* The phishing tests have got good results and have seen a drastic decrement in falling trap to those emails.
* The Challenge coin has made employees participate enthusiastically and be aware of security
* Incentivized learning, gamified training modules, podcasts, animations, onsite events which are implemented as a part of the information security aspect.

1. Both articles discuss similar approaches on how to get employees more engaged. What have they suggested linking risks to besides the organization?

* The Main Risk that both the papers have noted are human errors which are specifically targeted by hackers and are being utilized as great tools to intrude the system.
* The approach both papers make is employee engagement through various streamlines to make the cybersecurity issues more familiar to employees and make sure they are well educated to deal with them
* The Real world connection and helping to combine the security issue with the day to day life even personally can make a large difference