Notes:

* Business email compromise
  + Uses social engineering
  + Uses victim account into adversary account
  + 10< a week in san deiega
  + First swift recall request from bank
  + Report incident to ic3.gov
  + Contact fbi office
    - Fbi has relationship with banks
    - Funds frozen b4 badguy can move funds offshore account

There will always be someone unauthorized in the network

How can we mitigate this access?

Encrypted traffic makes it harder on security professionals since we don’t know who or what is being done on a network(is it legitimate or malicious?)

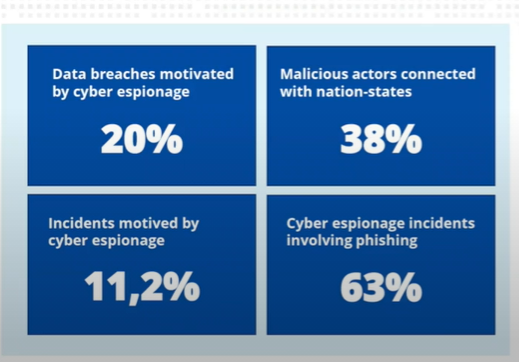
Looking at all endpoints (wfh, cloud, etc.)

Hackers worst is an out of ban looking at all their things

We are in a post compromised society

Patch patch patch

Session 3: Darktrace Presentation: Faking It - Stopping Impersonation Attacks with Cyber AI

* attackers have a lot on information through social media
* Workforce has adapted overnight
* A lot of critical information is curvilinear in these environments
* Unknown security backlash
* No longer a vault or perimeter and now the in is scattered and harder to keep outsiders out
* Legacy tools Miss novel threats bc they ask wrong questions
* Use a new approach using AI -does this belong?
* Enterprise immune system- what does it mean to be apart to be part ob the ecosystem
* Randsomeware
  + Target knowingly paying victims(hospitals, etc)
  + Steal the data before activating randsomeware to extort the information (double ectortion- becoming more common)
  + Happening usually at night
  + Immediate action if you see is disconnect from the network as soon as possible
  + Some can infect cloud based
  + Block system to system communication
  + Powerdown any system that have not been targeted yet
  + Through clicking on a link/attachments
  + Fbi does not recommend paying the randsome right- no guarantee
  + Secure offsite backups
* Espionage
  + Phishing -most common
  + 20% - data breach
  + Incident – 11.2% of all (incident = compromising cia)
  + 
  + Easiest is through email
* Remote workforce agreement
  + Privacy rights
    - Carbon block
      * Monitoring software
      * Let employees know what it does
  + Clear of deployment, reason, removing it
* Lines have been blurred between work and home life
  + Productivity vs security
* Insider threat = authorized user
  + Malicious
  + Acting from negligence