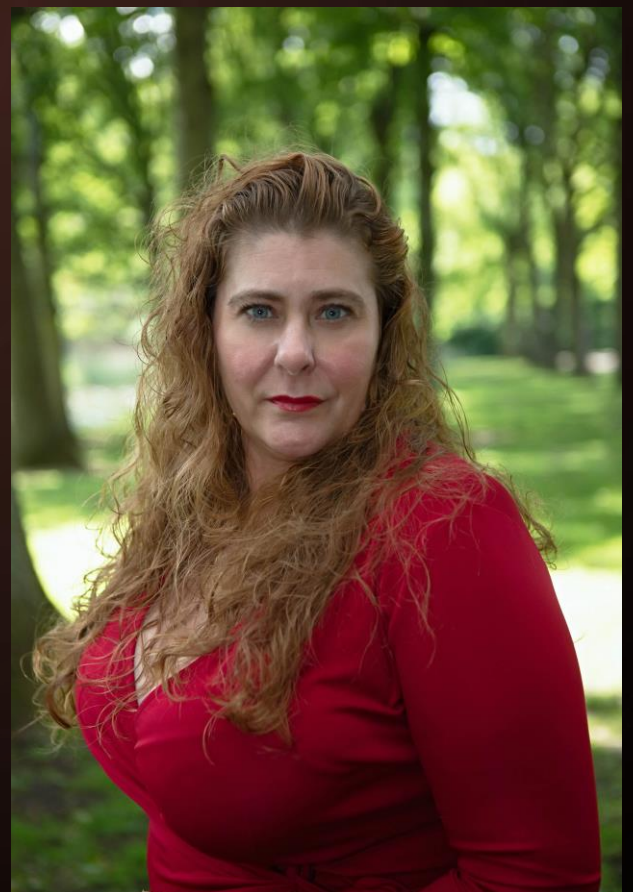
WHEN THEY ATTACKED THE SUPPLY CHAIN OF A NUCLEAR POWER PLANT

BSIDES NEWCASTLE 2021

CHRIS KUBECKA, CEO HYPASEC, MIDDLE EAST INSTITUTE DISTINGUISHED CHAIR

PRESENTER

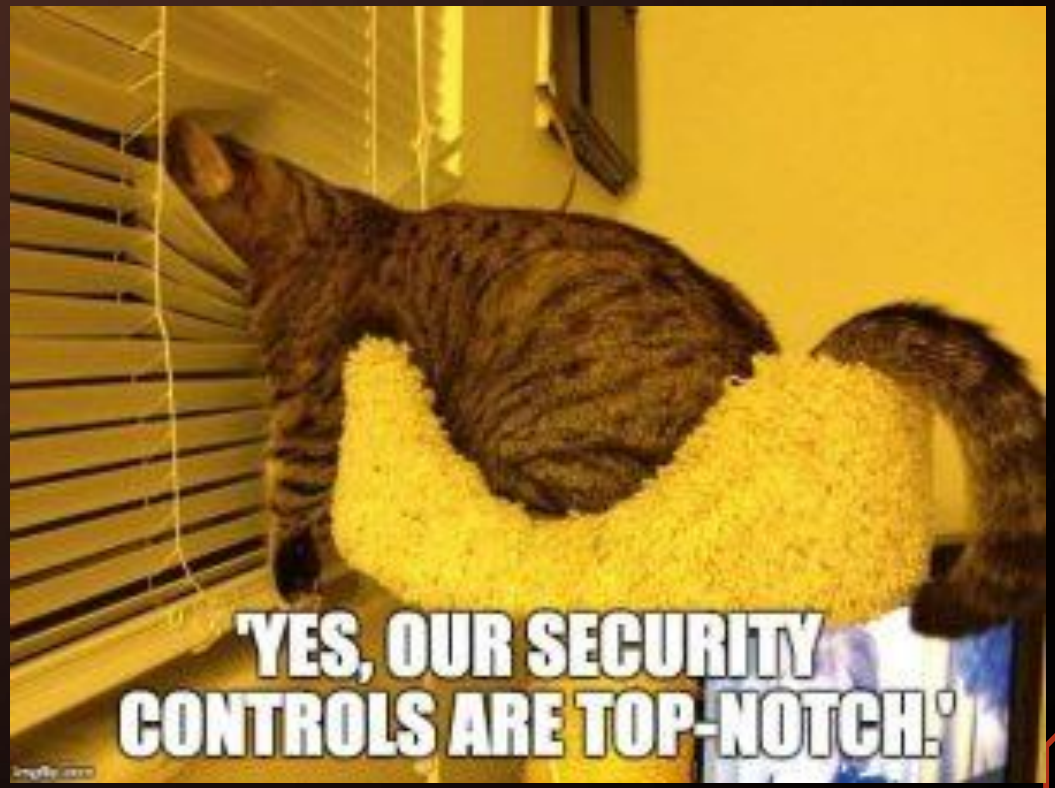
- Distinguished Chair of Cyber Middle East Institute
- Critical infrastructure security, ICS cyberwarfare
- Former Head of Aramco Information Protection
- Former U.S Air Force Aircrew & Space Command-Command & Control Systems



How A 10-Year-Old War Dialer Became A Top Cybersecurity Expert

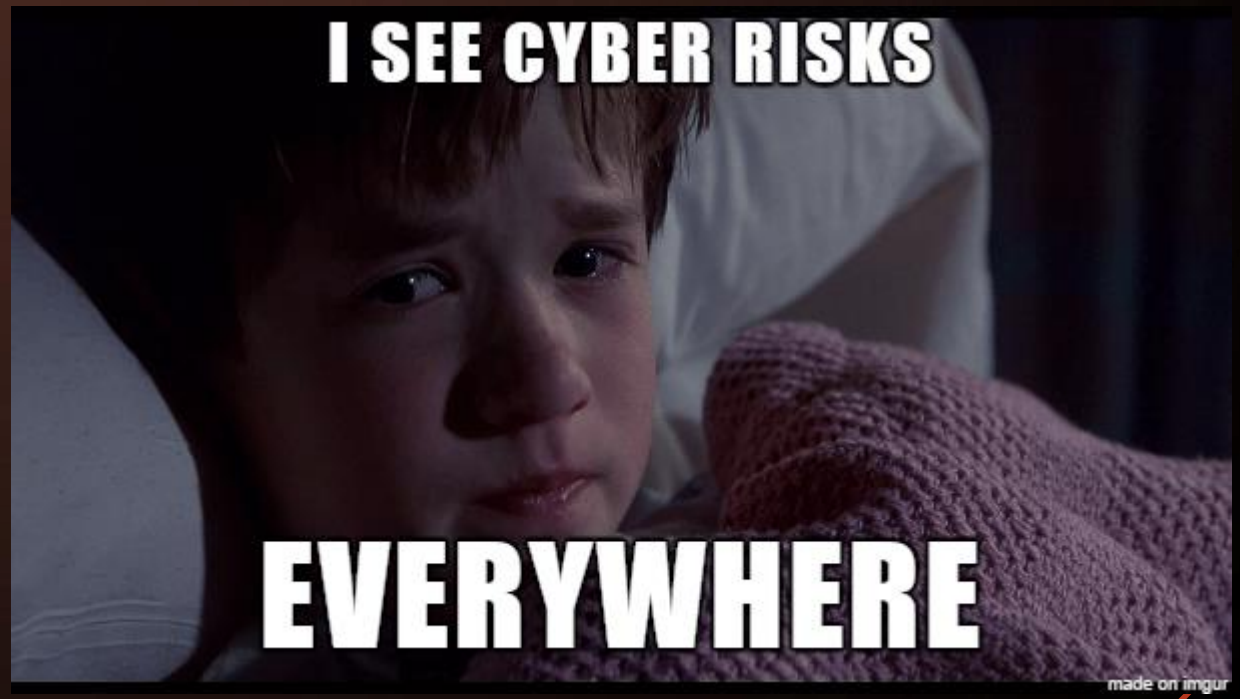
SUPPLY CHAIN CHALLENGES

- Trust
- Contracts
- Procurement
- Financial Penalties



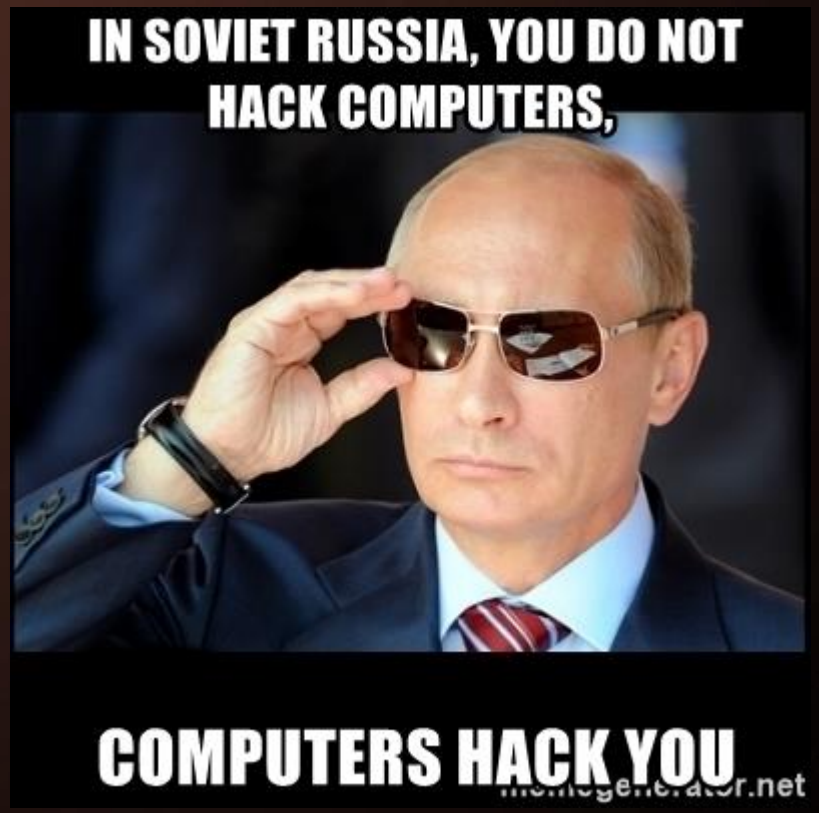
LACK OF CYBER SECURITY IN SUPPLY CHAIN

- Do they security test
- Do they care about privacy
- Have you tested for DR
- Can you be used as a pivot



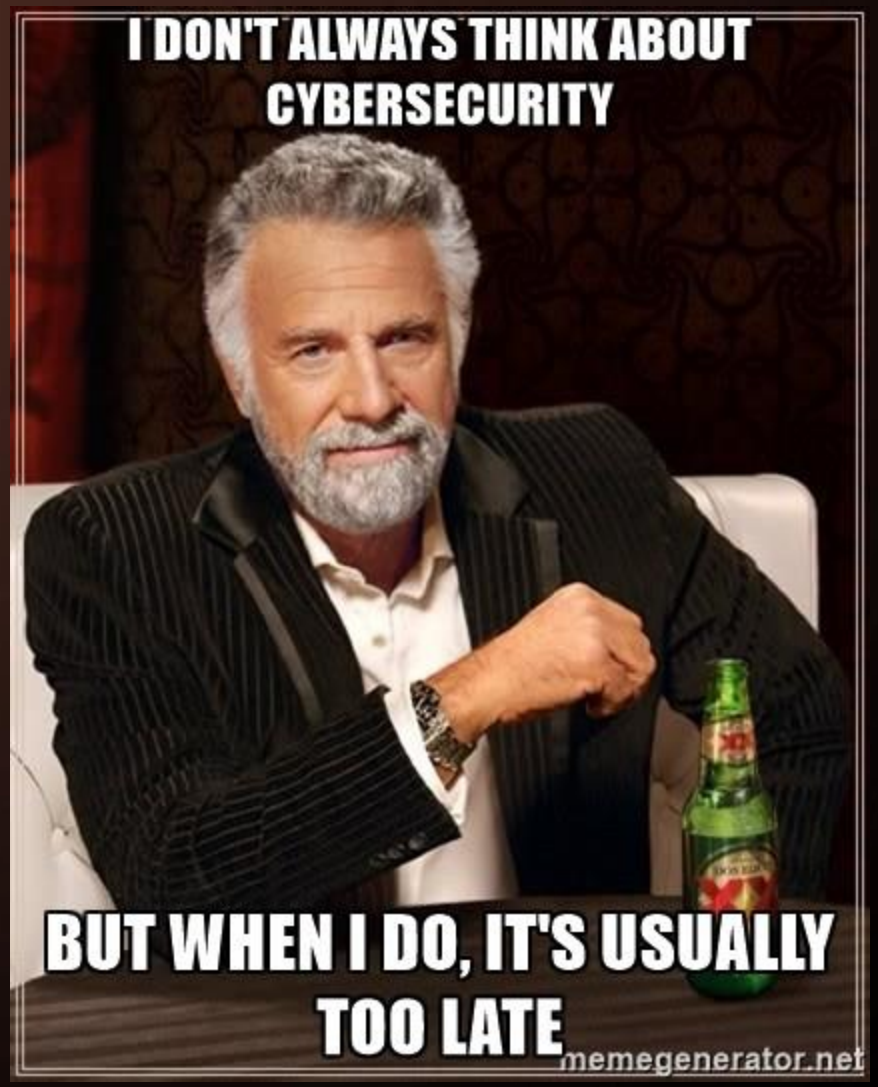
CENTRAL ANTI-VIRUS SYSTEM

- Many big orgs have them
- Alerts for potential problems
- Connects to every computer with admin privileges



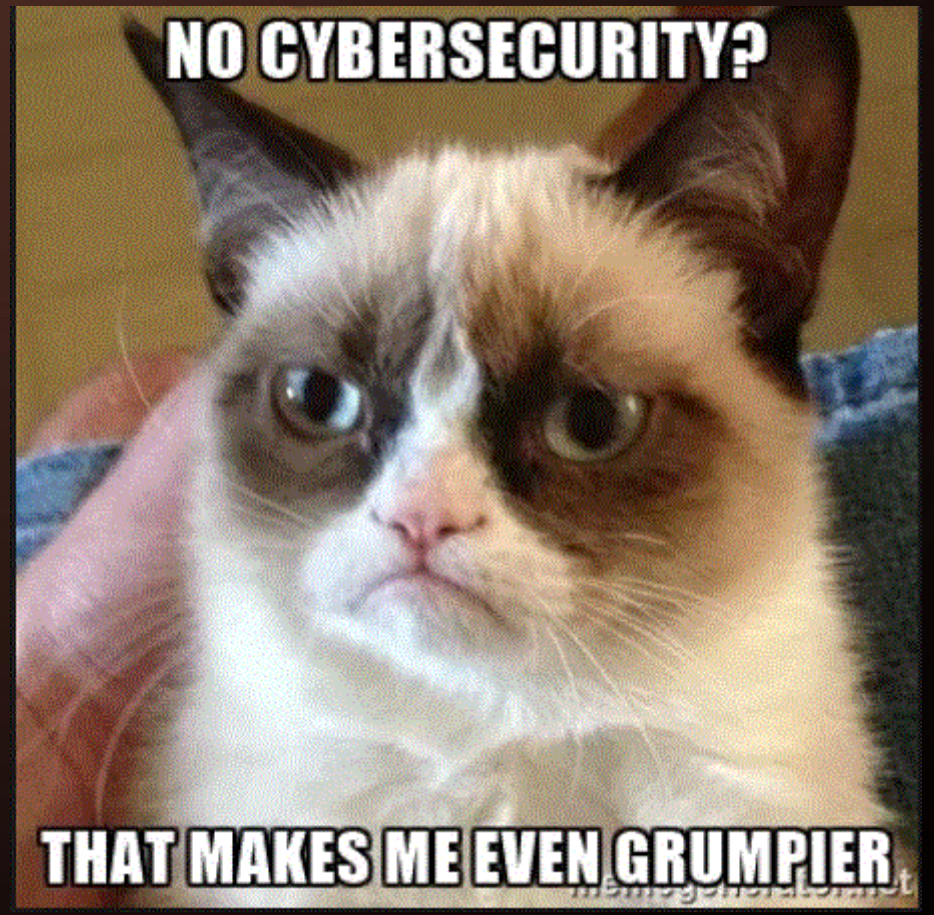
AV SECURITY ISSUES

- Super-dat files
- No authentication
- Not security tested
- Our own tool used against us



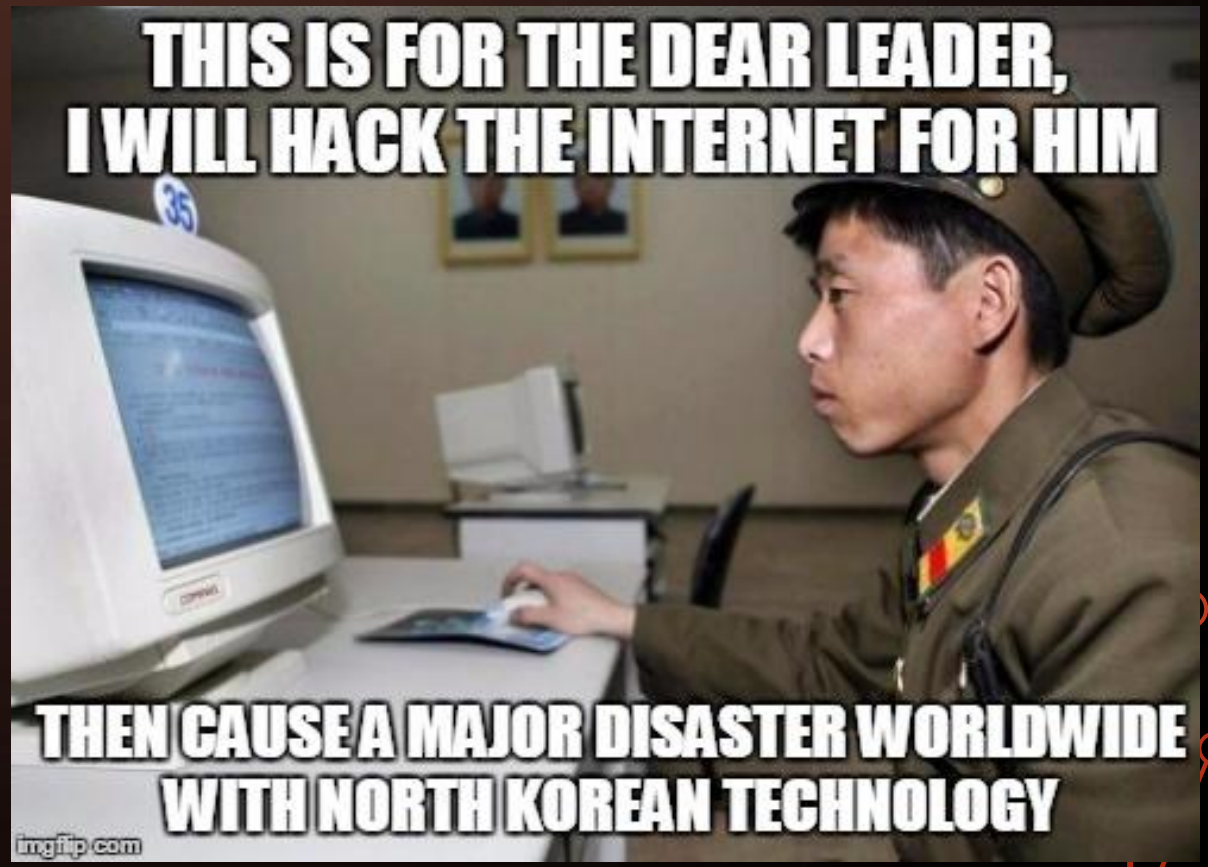
INITIAL ATTACK

- Attacker sent super-dat file
- Update service insecure
- Our AV system accepted
- Neutered our alerts
- Attack and tools successful
- Platinum support



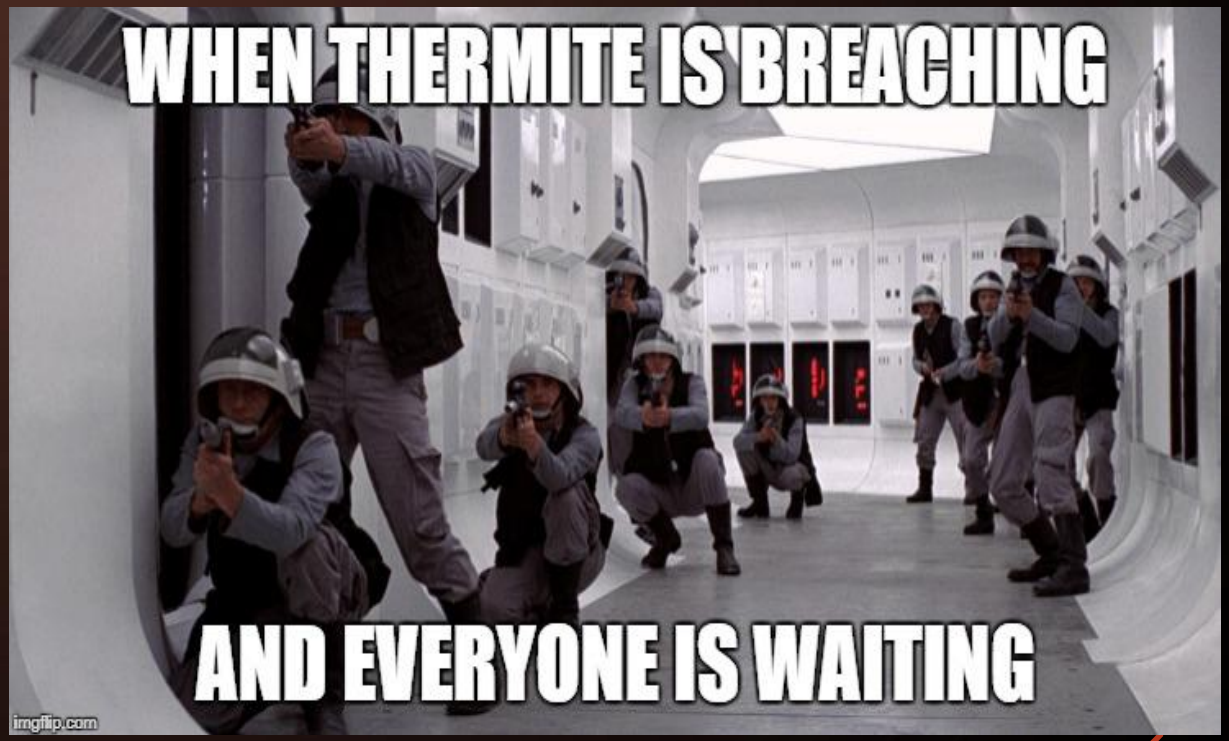
NORTH KOREAN CYBER AGGRESSION

- Small acts of terrorism
- Risk to telecom
- Employee safety
- Intellectual property
- Evacuation



THERMITE?

- US Military friend
- Dropped Satellite phones
- DBAN
- Readied aircraft
- $h*tshow

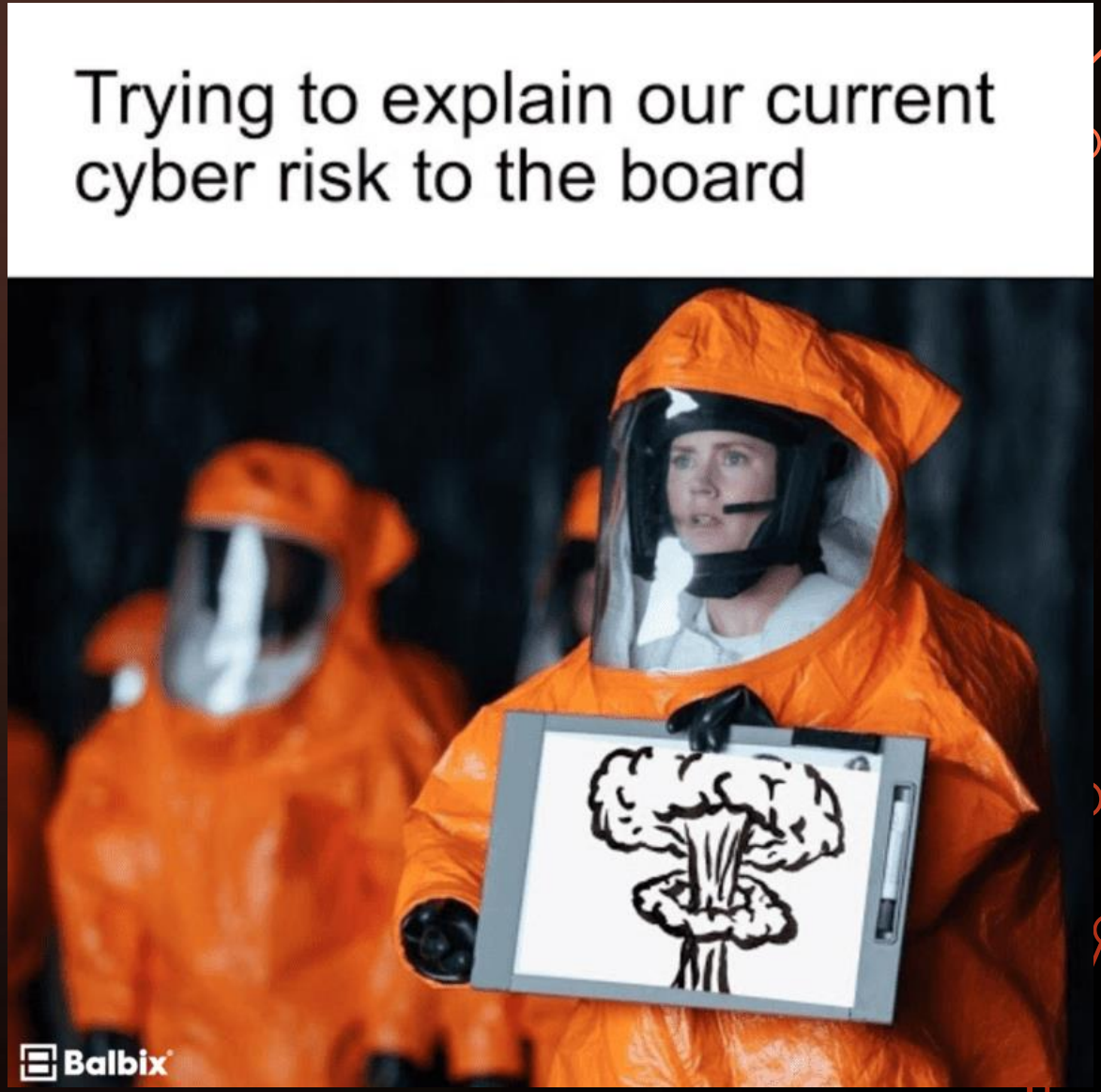


PIVOT ATTACK

- Pivot from network
- Joint venture network
- Partner systems were unsegmented
- Connected to nuclear facility

RECOMMENDATIONS

- Talk to the board in their language
- Adjust legal contracts
- Adjust procurement
- Buy iodine



THANK YOU

- Hacking the World with OSINT & Censys
- Down the Rabbit Hole an OSINT Journey
- https://mei.edu/profile/chris-kubecka