THINK STACK

Tales from the Cybersecurity Darkside

People Before Tech

to Transform and Protect

We Are Think|Stack

Founded in 2011, we are an innovative Managed Service Provider, focused on cybersecurity and cloud solutions that support organizational growth.

We believe technology should be used to create organizational transformation and should support a well-designed user experience.

Our core methodologies blend Design Thinking, Human and Experience-centered Design, and Systems Thinking with expertise across leading tech platforms to help organizations transform how they do business.

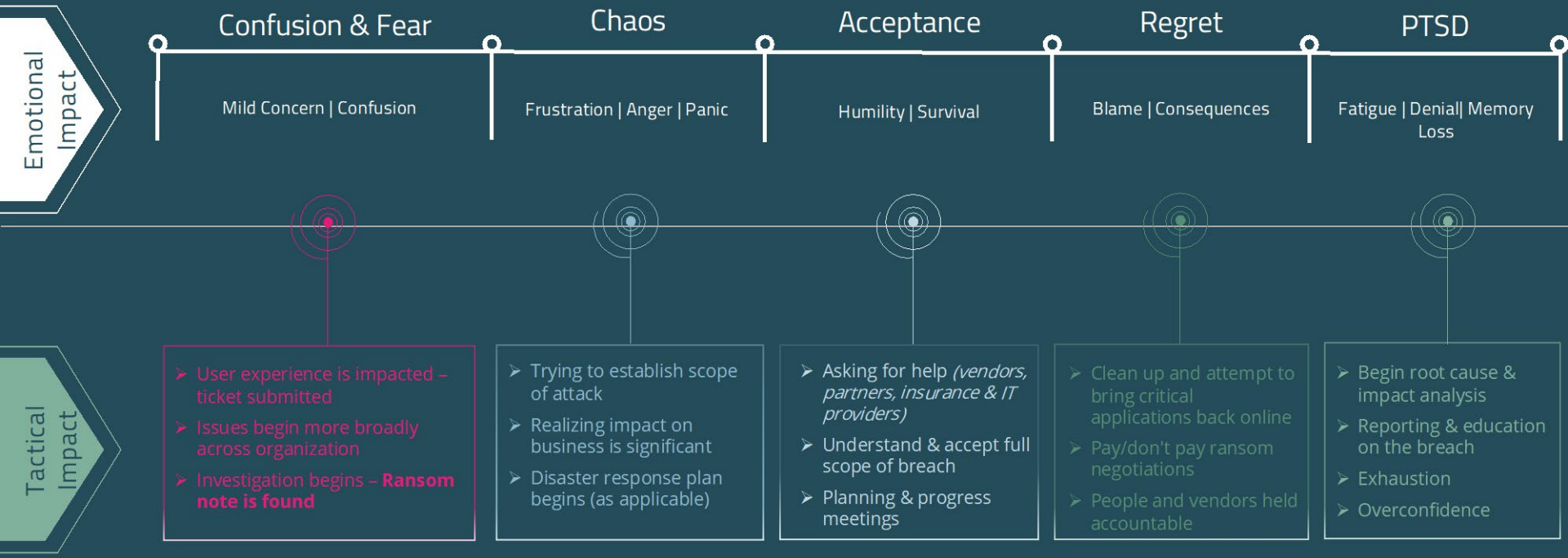
Jen Anthony

- Vice President of Cybersecurity at Think|Stack
- Served 20 years on Active Duty as part of Air Force Cyber Command
- Led offensive cyber operations against well-known nation-state actors
- Passionate about protecting the critical infrastructure of the US through education & and development
- Believes Cybersecurity is a team sport
- Serves as Executive & Human Performance Coach

Tales From the Cybersecurity Darkside

- Cyber Attack – What Really Happens?
- Holy Risk Management!
- Incident Planning & Response
- Why the Zero Trust Approach?
- Summary

THE RANSOMWARE ROLLERCOASTER



GAO Study

- Review Critical Technology
- Annual $90B tech spend
- 10% - Critical Infrastructure – outdated by 55 years or more
- US Treasury
  - 51 years old
  - Highest criticality level

U.S. Government Accountability Office
GAO

Traditional Security Approaches

Fake accounts, sites and mobile apps

Data breaches and credential compromise

Most Threats Are Out Here

Unknown and vulnerable IT assets and servers

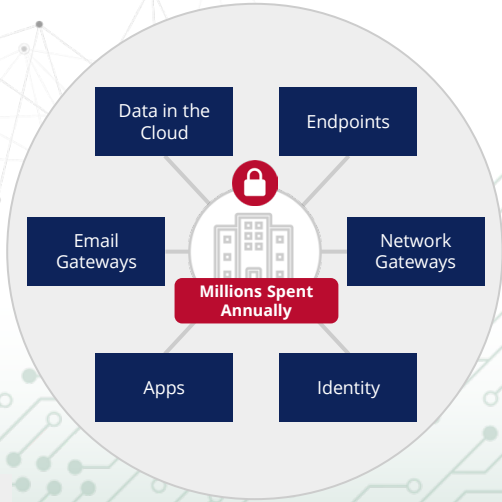
Physical threats to locations and people

Phishing sites and spoofed domains

Scams and fraud on social media and web

Dark web chatter and data leaks

#USERS



72% of cyber spending

18% of cyber spending

Incident Response & Planning Recommendations

THIS

- Follow Incident Response Framework
- Incident Response Plan
- Cyber Insurance
- Identify key players
- Establish relationships
- Practice, practice, practice
- Identify your “Break glass” option

NOT THAT

- Ignore
- Panic
- Shut Systems Down
- Box check your tabletop exercise

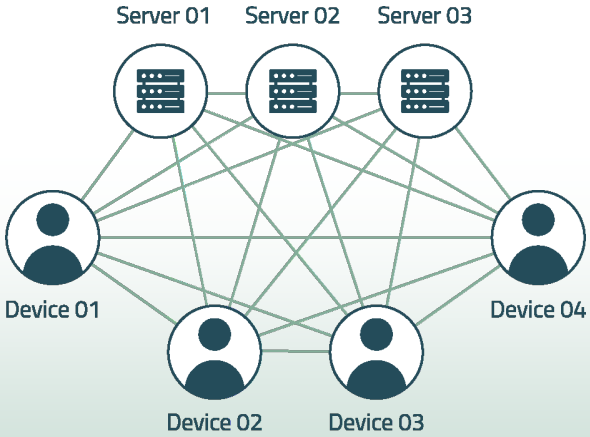
What is Zero Trust?

- A framework and architecture that treats every aspect, device, service and user of a network, as continuously exposed and potentially compromised.

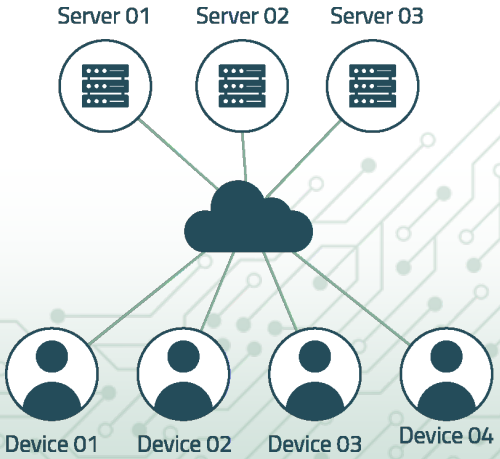
- Zero Trust Architecture or ZTA is intentional and customized, built to support your cyber risk appetite and your Confidentiality, Integrity and Availability (CIA) requirements using the zero trust philosophies and frameworks.

Access Control Example

Transition from an environment where each device can exchange data directly with every other device..



...to a ZTNA environment where identity is verified and every access is mediated, logged, and analyzed



Almost done…

- Threats will continue
- Use of technology in the banking process is rapidly increasing
- Member experience can be impacted by cybersecurity
- Consumers are more aware of technology than ever before
- We prepare for cyber threats in a reactionary mode

Summary

- Cyber Attack – What Really Happens?
- Holy Risk Management!
- Incident Planning & Response
- Why the Zero Trust Approach?
- Summary

Questions?

*"It's not a faith in technology. **It's faith in people**."*

-Steve Jobs