THINK STACK

If your cybersecurity was a human, how would you describe it?

"It's a mid-career professional, ready to leap"

"1999 model in a 2021 world."

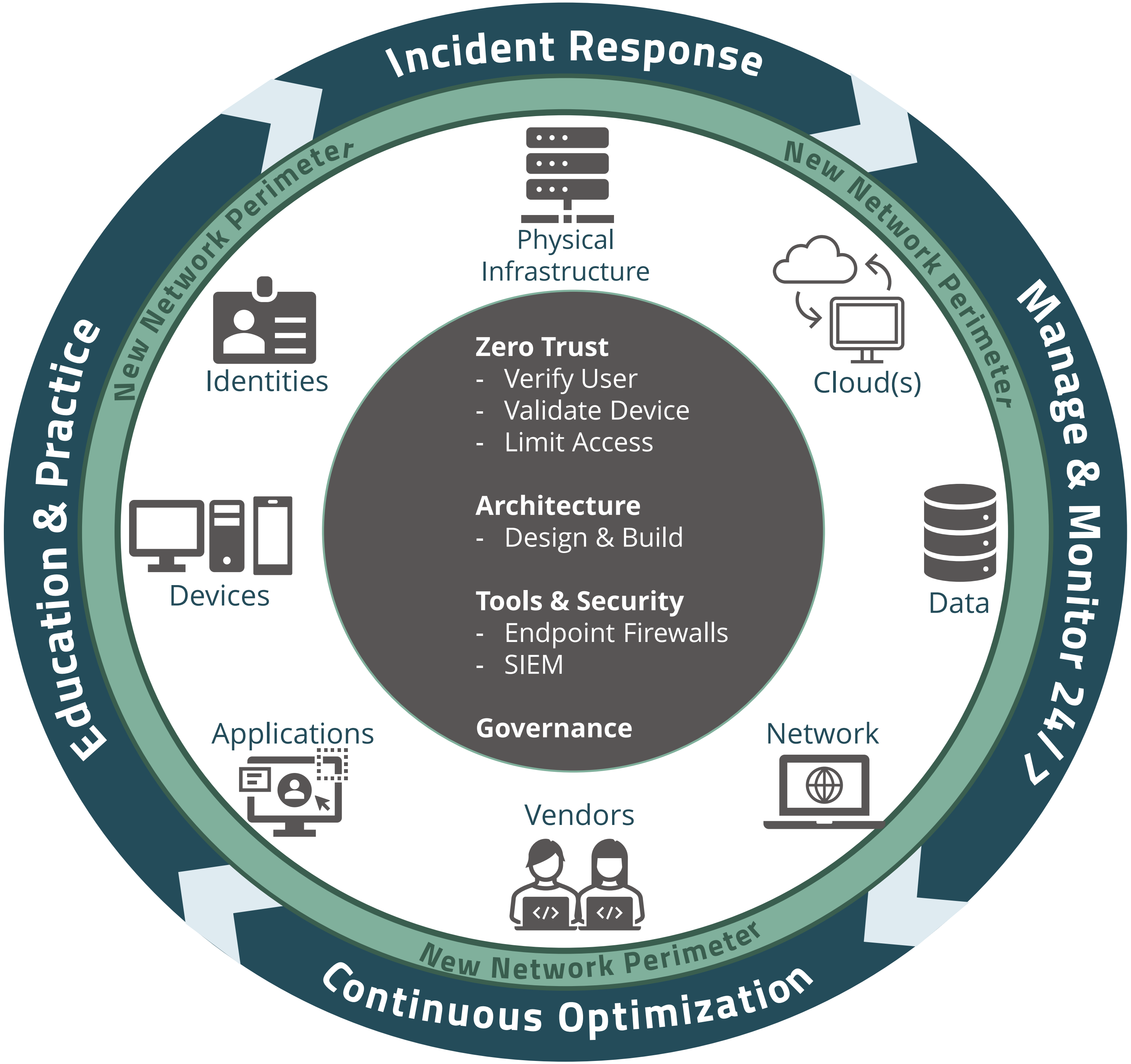
"It's a young adult with lots of education but little experience."

"Woefully end of life."

"It's TSA, you see them you know they are doing something but you have no idea how effective they are"

PEOPLE BEFORE TECH

What does an ideal Modern Network Security look like?



Zero Trust
- Verify User
- Validate Device
- Limit Access

Architecture
- Design & Build

Tools & Security
- Endpoint Firewalls
- SIEM

Governance

Cybercrime Up 600% Due To COVID-19 Pandemic

It takes organizations an average of 191 days to identify data breaches.

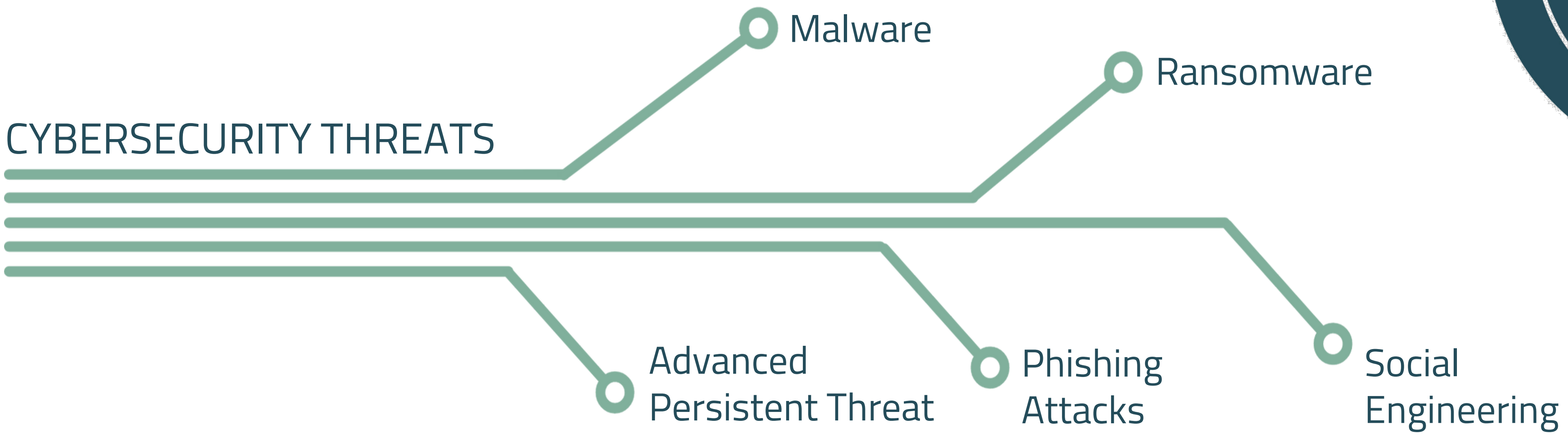
70% of small businesses are unprepared to deal with a cyber attack.

3 out of 4 small businesses say they don't have sufficient personnel to address IT security.

Ransomware damage costs alone are on track to hit $11.5 billion in 2019, at which point it's estimated that small businesses will fall victim to a ransomware attack every 14 seconds.

60% of small companies go out of business within six months of a cyber attack.

TRANSFORM PROTECT



CYBERSECURITY THREATS

Malware

Ransomware

Advanced Persistent Threat

Phishing Attacks

Social Engineering

What is your current confidence level?

1

Our organization is 100% secure and monitored,
I sleep soundly at night

2

I feel pretty good about our security but, I'm a little restless at night

3

I honestly don't know how secure we are, and that fear keeps me up at night

Cyber Regualtions

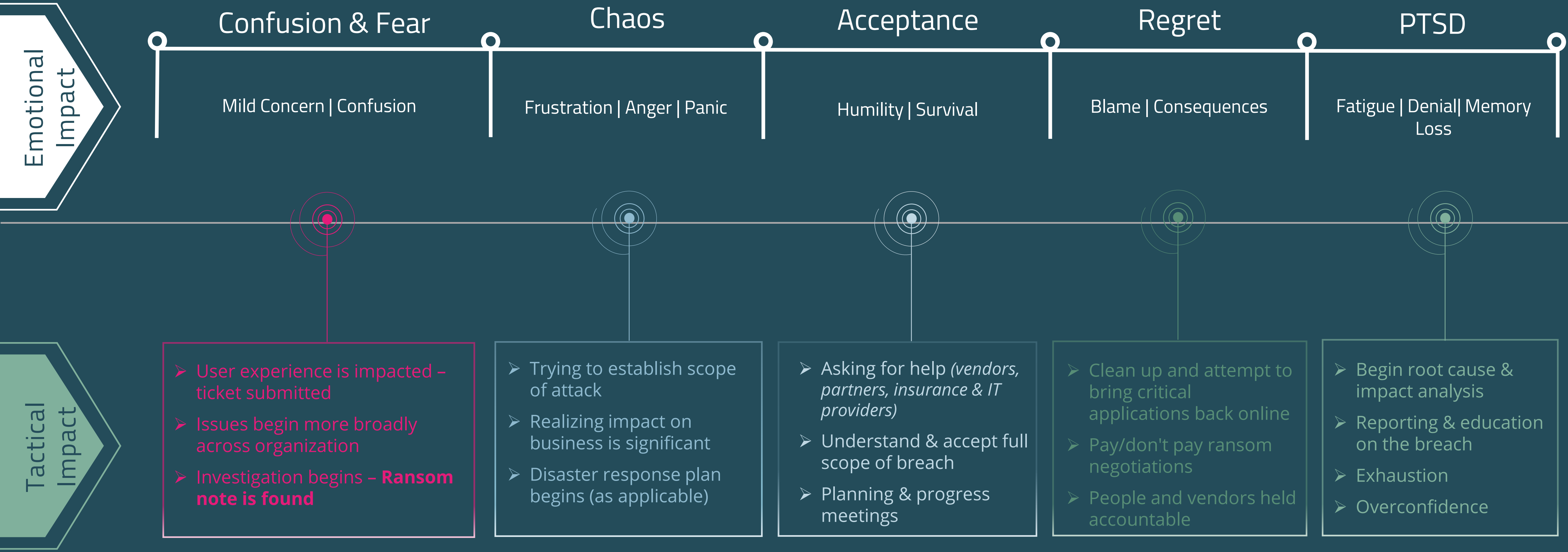
Good frameworks to guide best practices

Checklists are not unified, coordinated plans

Not all examiners are not cyber experts

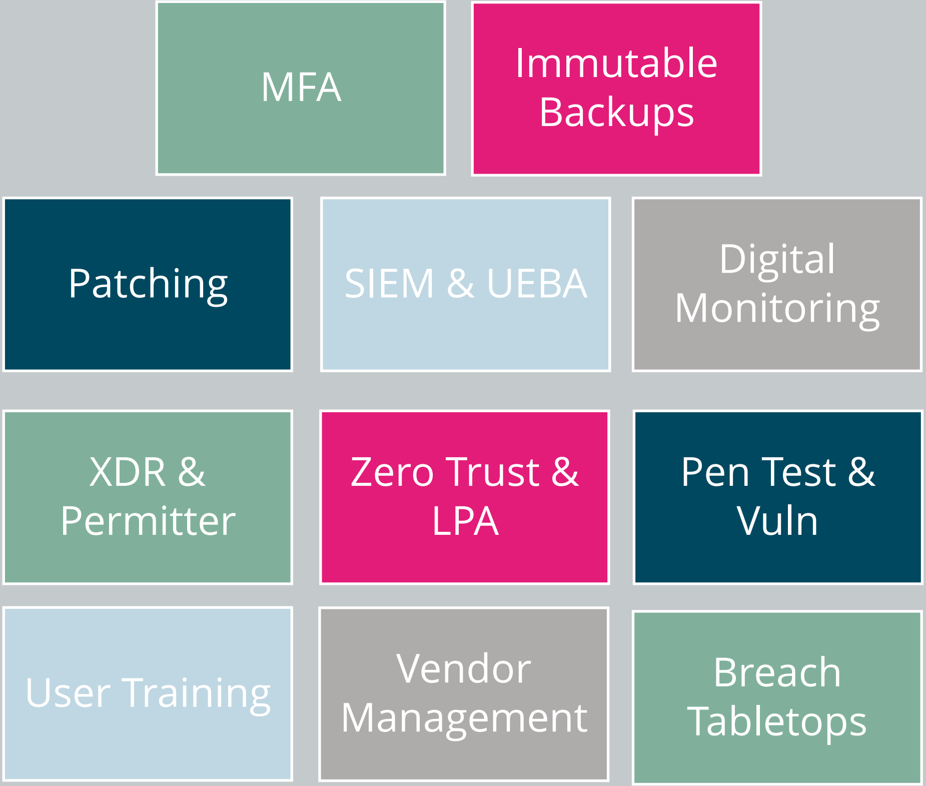
False confidence can be dangerous

THE RANSOMWARE ROLLERCOASTER



	Confusion & Fear	Chaos	Acceptance	Regret	PTSD
Emotional Impact	Mild Concern | Confusion	Frustration | Anger | Panic	Humility | Survival	Blame | Consequences	Fatigue | Denial| Memory Loss
Tactical Impact	➢ User experience is impacted – ticket submitted ➢ Issues begin more broadly across organization ➢ Investigation begins – **Ransom note is found**	➢ Trying to establish scope of attack ➢ Realizing impact on business is significant ➢ Disaster response plan begins (as applicable)	➢ Asking for help *(vendors, partners, insurance & IT providers)* ➢ Understand & accept full scope of breach ➢ Planning & progress meetings	➢ Clean up and attempt to bring critical applications back online ➢ Pay/don't pay ransom negotiations ➢ People and vendors held accountable	➢ Begin root cause & impact analysis ➢ Reporting & education on the breach ➢ Exhaustion ➢ Overconfidence

TECH | MAP



Start with a Plan

Build a comprehensive plan for cybersecurity.

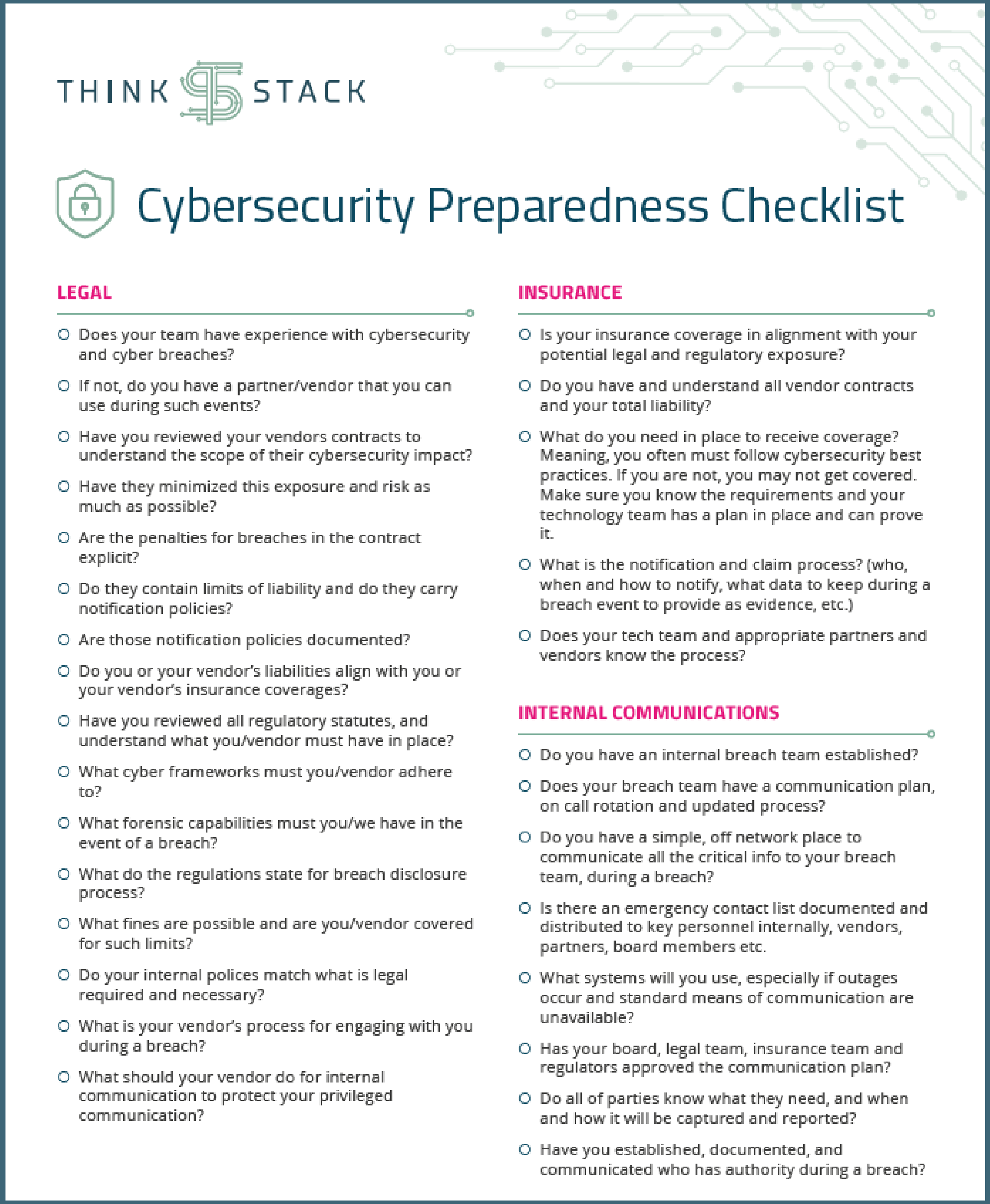
Change the culture and you will be more secure.

You need to understand what you do to build a protection plan.

Cybersecurity Basics

What do I know?

Get the Checklist here



THINK STACK

Cybersecurity Preparedness Checklist

LEGAL

○ Does your team have experience with cybersecurity and cyber breaches?

○ If not, do you have a partner/vendor that you can use during such events?

○ Have you reviewed your vendors contracts to understand the scope of their cybersecurity impact?

○ Have they minimized this exposure and risk as much as possible?

○ Are the penalties for breaches in the contract explicit?

○ Do they contain limits of liability and do they carry notification policies?

○ Are those notification policies documented?

○ Do you or your vendor's liabilities align with you or your vendor's insurance coverages?

○ Have you reviewed all regulatory statutes, and understand what you/vendor must have in place?

○ What cyber frameworks must you/vendor adhere to?

○ What forensic capabilities must you/we have in the event of a breach?

○ What do the regulations state for breach disclosure process?

○ What fines are possible and are you/vendor covered for such limits?

○ Do your internal polices match what is legal required and necessary?

○ What is your vendor's process for engaging with you during a breach?

○ What should your vendor do for internal communication to protect your privileged communication?

INSURANCE

○ Is your insurance coverage in alignment with your potential legal and regulatory exposure?

○ Do you have and understand all vendor contracts and your total liability?

○ What do you need in place to receive coverage? Meaning, you often must follow cybersecurity best practices. If you are not, you may not get covered. Make sure you know the requirements and your technology team has a plan in place and can prove it.

○ What is the notification and claim process? (who, when and how to notify, what data to keep during a breach event to provide as evidence, etc.)

○ Does your tech team and appropriate partners and vendors know the process?

INTERNAL COMMUNICATIONS

○ Do you have an internal breach team established?

○ Does your breach team have a communication plan, on call rotation and updated process?

○ Do you have a simple, off network place to communicate all the critical info to your breach team, during a breach?

○ Is there an emergency contact list documented and distributed to key personnel internally, vendors, partners, board members etc.

○ What systems will you use, especially if outages occur and standard means of communication are unavailable?

○ Has your board, legal team, insurance team and regulators approved the communication plan?

○ Do all of parties know what they need, and when and how it will be captured and reported?

○ Have you established, documented, and communicated who has authority during a breach?