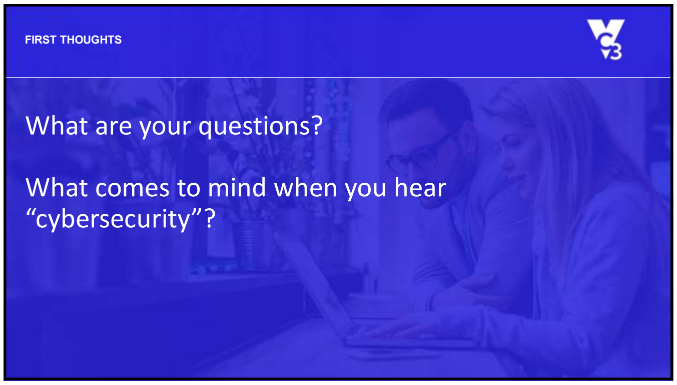
The information provided here is for informational and educational purposes and current as of the date of publication. The information is not a substitute for legal advice. Consult you attorney for advice concerning specific situations.

7 Mistakes You’re Making in Cybersecurity as a Non-Technical Leader

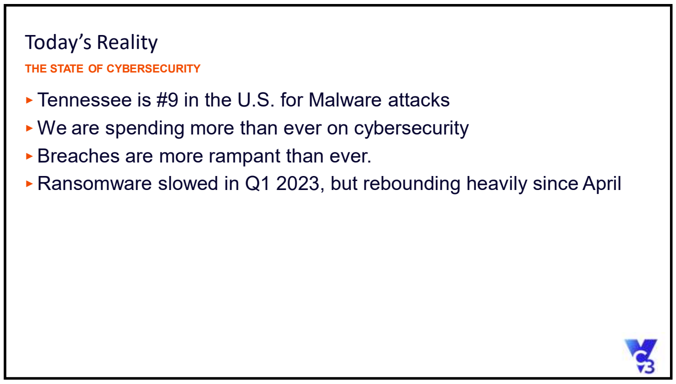
▸ STAY OUT OF THE HEADLINES



FIRST THOUGHTS

What are your questions?

What comes to mind when you hear “cybersecurity”?



Today’s Reality

THE STATE OF CYBERSECURITY

- Tennessee is #9 in the U.S. for Malware attacks
- We are spending more than ever on cybersecurity
- Breaches are more rampant than ever.
- Ransomware slowed in Q1 2023, but rebounding heavily since April

Today's Reality

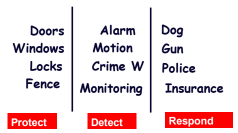
THE STATE OF CYBERSECURITY

- Traditional Network Security is Failing
- How did we get here?
- It's not your fault!

What is your cybersecurity strategy?

How does security actually WORK?

IT'S A SYSTEM, NOT JUST TOOLS



Doors
Windows
Locks
Fence

Alarm
Motion
Crime W
Monitoring

Dog
Gun
Police
Insurance

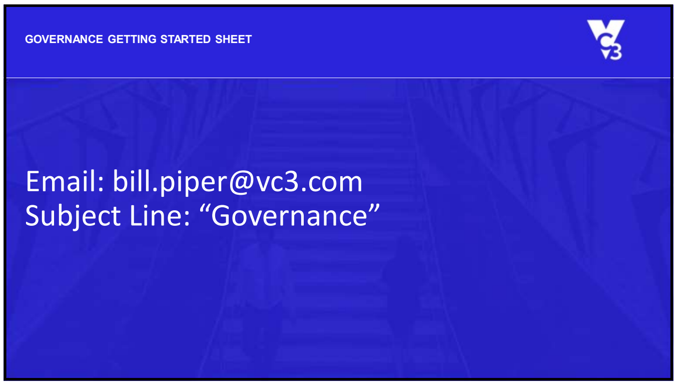
Protect
Detect
Respond

What does your city need from technology?

Staff	**Support**
Security	**Strategy**

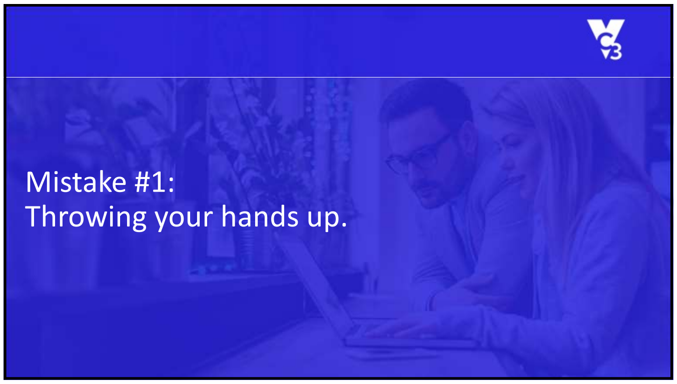
IT Governance:

How you manage the business of IT within your city.



GOVERNANCE GETTING STARTED SHEET

Email: bill.piper@vc3.com
Subject Line: “Governance”



Mistake #1:
Throwing your hands up.

Mistake #1: Throwing Your Hands Up

You might be a non-technical municipal leader if…

WE'RE ALL FRIENDS HERE.

- You say "I know enough to be dangerous."
- You use the word "guru" to describe an IT person.
- You still use the word "mainframe."

You:

Run organizations with complex processes.

Solve complex problems for a living.

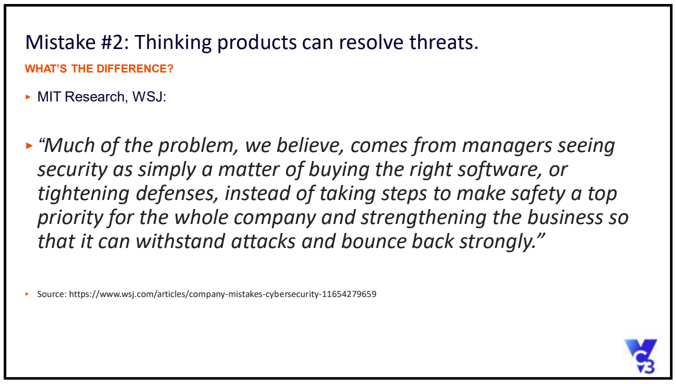
Are capable of setting objectives for technology.

Know your risks:

HOW DO YOU LOSE?

- Safety
- Operational
- Financial
- Reputational

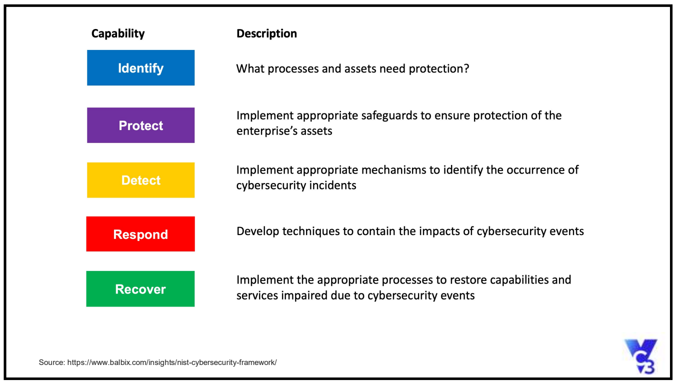
Mistake #2:
Thinking products can resolve threats - (a.k.a. no strategy)



Mistake #2: Thinking products can resolve threats.

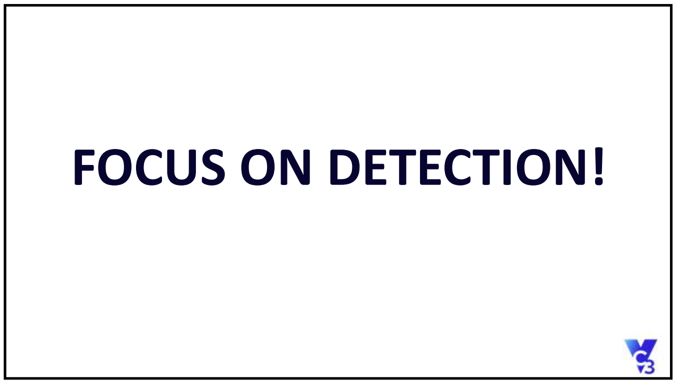
WHAT'S THE DIFFERENCE?

- MIT Research, WSJ:
- *"Much of the problem, we believe, comes from managers seeing security as simply a matter of buying the right software, or tightening defenses, instead of taking steps to make safety a top priority for the whole company and strengthening the business so that it can withstand attacks and bounce back strongly."*
- Source: https://www.wsj.com/articles/company-mistakes-cybersecurity-11654279659

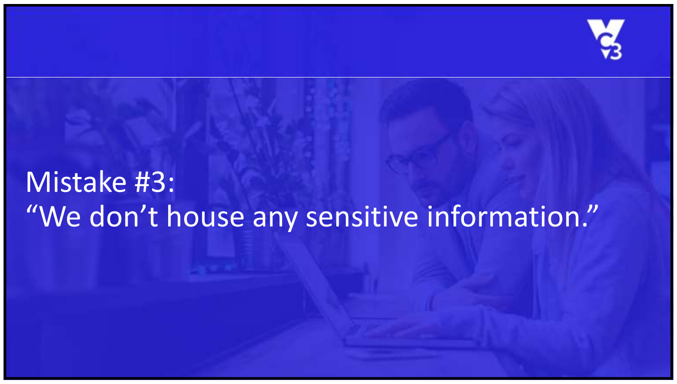


Capability	Description
🟦 Identify	What processes and assets need protection?
🟪 Protect	Implement appropriate safeguards to ensure protection of the enterprise's assets
🟨 Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
🟥 Respond	Develop techniques to contain the impacts of cybersecurity events
🟩 Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

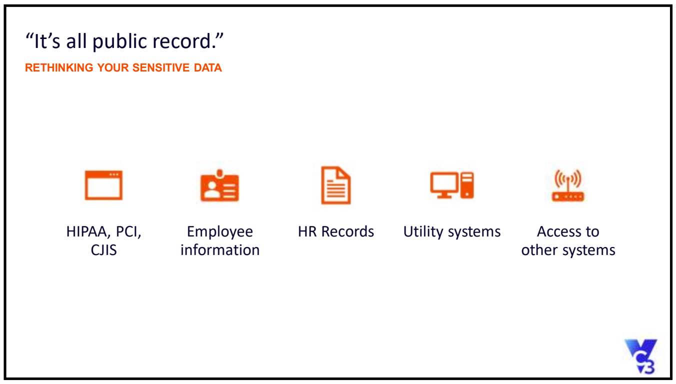
Source: https://www.balbix.com/insights/nist-cybersecurity-framework/



FOCUS ON DETECTION!



Mistake #3:
"We don't house any sensitive information."



"It's all public record."

RETHINKING YOUR SENSITIVE DATA

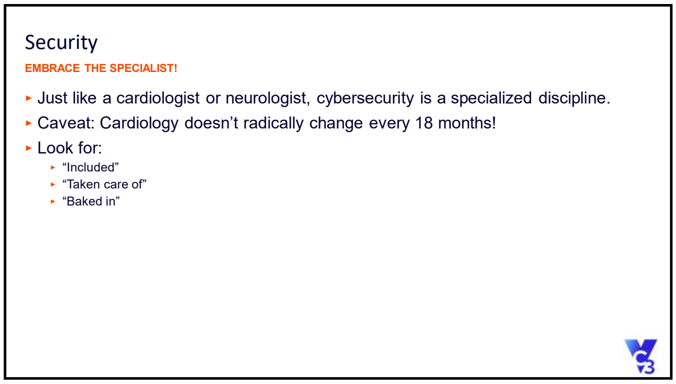
- HIPAA, PCI, CJIS
- Employee information
- HR Records
- Utility systems
- Access to other systems

Mistake #4: Assuming IT is "handling" security.

What things need support?

SKILLS, STAFF, SECURITY, STRATEGY

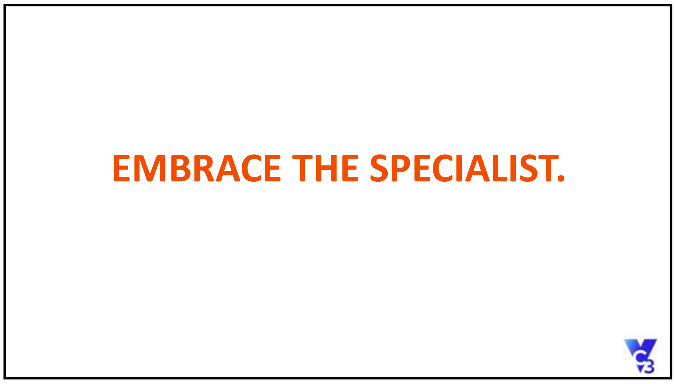
- Technical
  - Users
  - Servers
  - Switches
  - Backup
  - Firewalls/Switches/Routers
  - On-prem Assets
  - Cloud Services
  - Apps
  - PCs
  - Mesh
  - Software & Applications
  - Security Tools, Monitoring, Management
  - Patching & Maintenance
  - IT Hygiene
- Administrative
  - Warranties
  - Licensing
  - Security Strategy
  - After-hours Support
  - Finding new software and applications
  - Hardware Refreshes
  - System/Software Upgrades
  - Reporting and Analysis
  - Vendor Management
  - Adopting new technologies



Security

EMBRACE THE SPECIALIST!

- Just like a cardiologist or neurologist, cybersecurity is a specialized discipline.
- Caveat: Cardiology doesn’t radically change every 18 months!
- Look for:
  - “Included”
  - “Taken care of”
  - “Baked in”



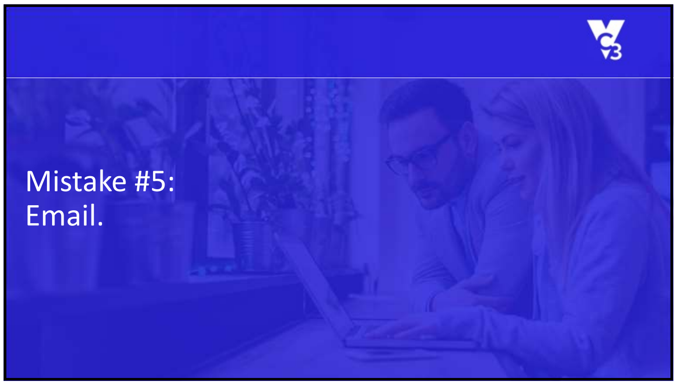
EMBRACE THE SPECIALIST.

Levels of Protection/Detection You Need:

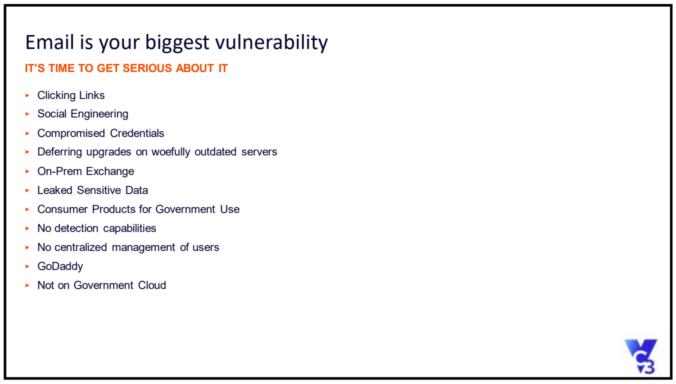
NOT JUST A PIECE OF SOFTWARE:

- Workstation
- Email
- Cloud Applications (i.e. Microsoft 365)
- Web Protection (Content, HTTPS Attacks)
- Network Layer
- Backups
- Policies and Procedures
- Dark Web Monitoring

"Trust but verify."



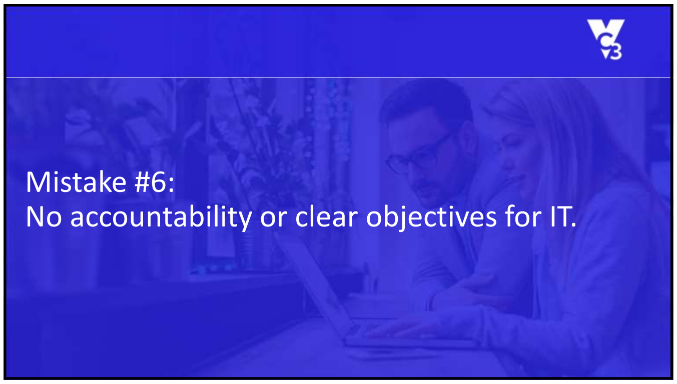
Mistake #5:
Email.



Email is your biggest vulnerability

IT'S TIME TO GET SERIOUS ABOUT IT

- Clicking Links
- Social Engineering
- Compromised Credentials
- Deferring upgrades on woefully outdated servers
- On-Prem Exchange
- Leaked Sensitive Data
- Consumer Products for Government Use
- No detection capabilities
- No centralized management of users
- GoDaddy
- Not on Government Cloud

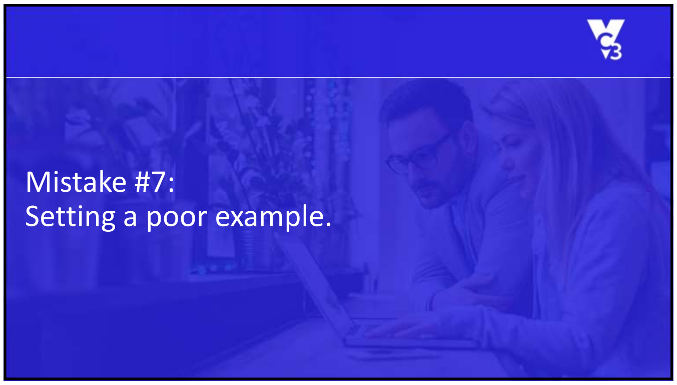


Mistake #6:
No accountability or clear objectives for IT.

What does “GOOD” look like?

PROVIDE HELPFUL ACCOUNTABILITY

- Step 1: Adopt a Framework
- Step 2: Know your risks
- Step 3: Build a strategy
- Step 4: Adopt a “risk-based approach” to IT Budget planning
- Step 5: Provide accountability and optimize

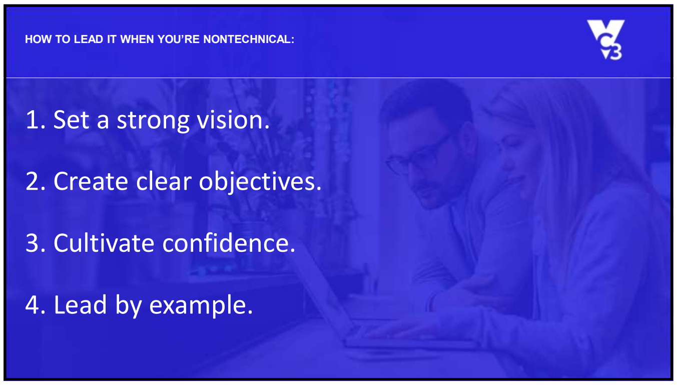


Mistake #7:
Setting a poor example.

Lead By Example

SET A STRONG VISION

- Do you defer maintenance?
- Do you treat IT as an asset?
- Is “good enough” good enough?



HOW TO LEAD IT WHEN YOU'RE NONTECHNICAL:

1. Set a strong vision.
2. Create clear objectives.
3. Cultivate confidence.
4. Lead by example.