CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

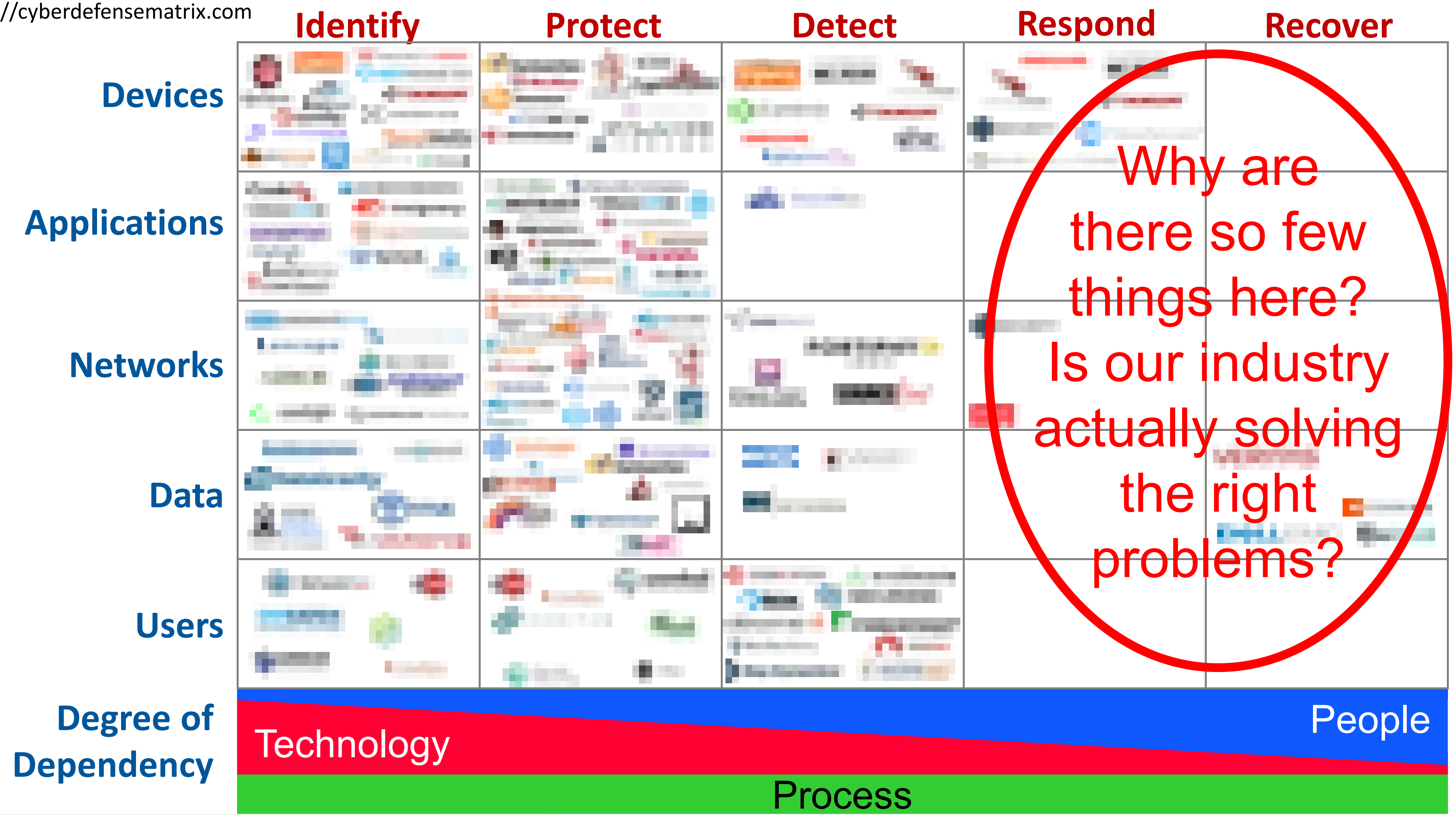
3RD ANNUAL NATIONAL CYBERSECURITY SUMMIT

Day 2: Opening Keynote
New Paradigms for the Next Era of Security

Sounil Yu

Cyber Defense Matrix

https://cyberdefensematrix.com



Identify | Protect | Detect | Respond | Recover

Devices

Applications

Networks

Data

Users

Why are there so few things here? Is our industry actually solving the right problems?

Degree of Dependency

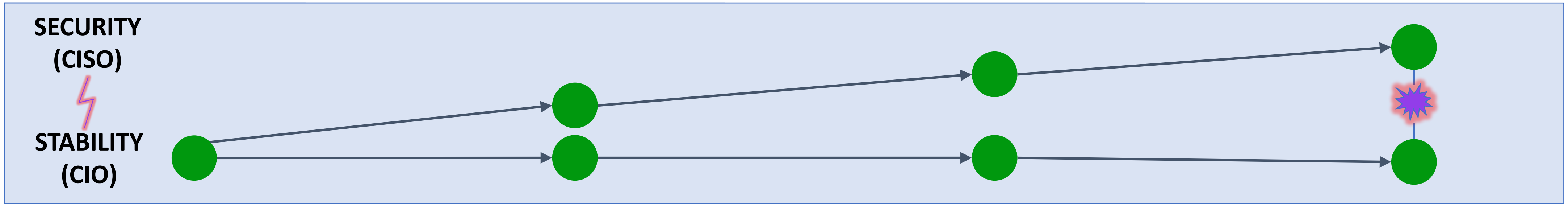
Technology

People

Process

Disclaimer: Vendor logos fuzzily shown are representative only. No endorsement should be construed because they are shown here.

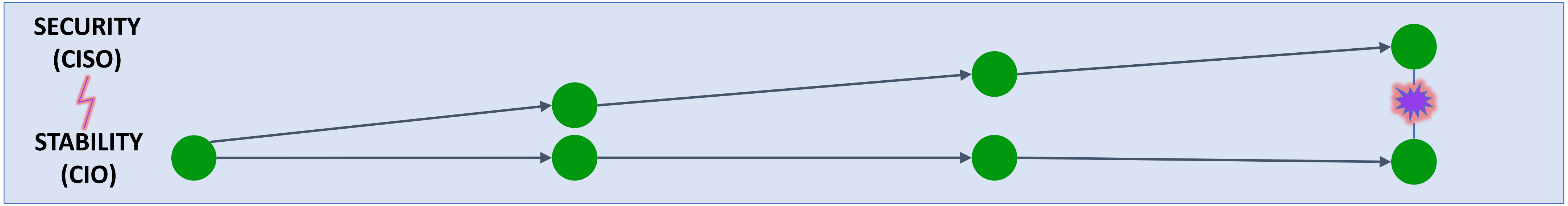
A Quick History of IT and Security

Era	1980s	1990s	2000s	2010s
Core Challenges	What did we buy and how does it support the biz?	Viruses, Server-side Attacks, Insecure Configs	Too many logs and alerts, Client-side attacks	Assume Breach, Raging Fires, Too Many Privileges
Solutions	Asset Mgt, Systems Mgt Tools	Anti-Virus, Firewalls, Secure Configs	IDS, SIEM	Incident Responders & IR Tools (EDR, SOAR)
IT / Security Tension				
Security Team Composition & Focus	None	Hobby Shop / Vulnerability Mgt	Sec Ops Center / Threat Mgt	Dedicated Biz Unit / Risk Mgt

Mapping to the NIST Cybersecurity Framework

Era	1980s IDENTIFY	1990s PROTECT	2000s DETECT	2010s RESPOND
Core Challenges	What did we buy and how does it support the biz?	Viruses, Server-side Attacks, Insecure Configs	Too many logs and alerts, Client-side attacks	Assume Breach, Raging Fires, Too Many Privileges
Solutions	Asset Mgt, Systems Mgt Tools	Anti-Virus, Firewalls, Secure Configs	IDS, SIEM	Incident Responders & IR Tools (EDR, SOAR)
Security Team Composition & Focus	None	Hobby Shop / Vulnerability Mgt	Sec Ops Center / Threat Mgt	Dedicated Biz Unit / Risk Mgt

IT / Security Tension



2020s: Age of Recovery (or Resiliency)

What kind of attacks should we see in the 2020s that would challenge to our ability to RECOVER or cause irreversible harm?

Confidentiality

Wikileaks
Doxxing

Integrity

Ransomware
#fakenews

Availability

PDoS, MBR Wiper,
Bricking Firmware

2020s: Age of Recovery (or Resiliency)

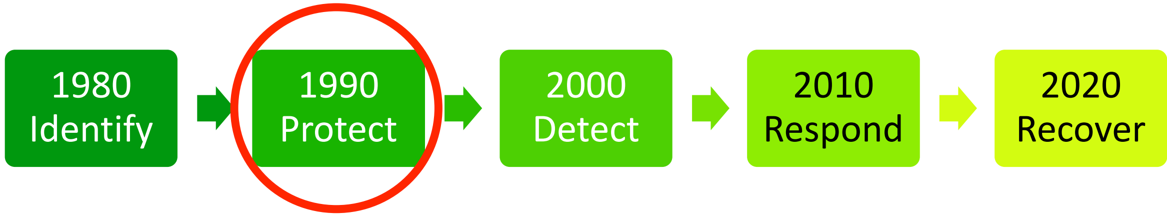
What kind of solutions directly support our ability to RECOVER or be RESILIENT?

Forging ahead or regressing back?

Recent advertising campaign from major vendor

DINOSAURS REACT.
PROFESSIONALS
PREVENT.
JOIN THE PREVENTION AGE
STOP CYBER BREACHES

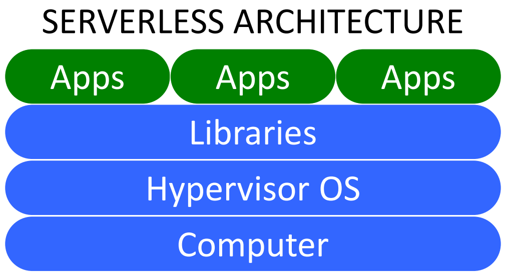
- A call to go back to the 1990s?


1980 Identify → 1990 Protect → 2000 Detect → 2010 Respond → 2020 Recover

- How will prevention mitigate the impact of ransomware?
  - Remember, we learned “assume breach” in the 2010s
  - Prevention minimizes the occurrences, **but does not address the impact or ability to recover**

2020s: Age of Recovery (or Resiliency)

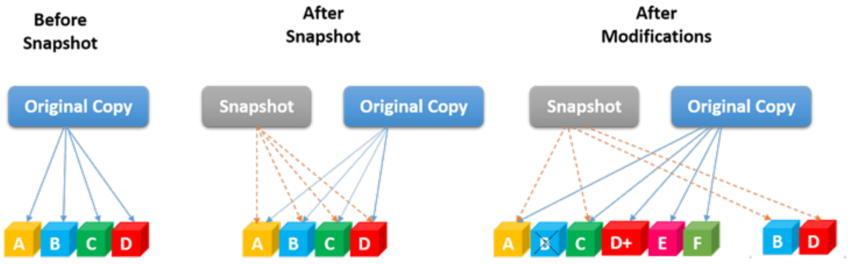
What kind of solutions directly support our ability to RECOVER or be RESILIENT?


SERVERLESS ARCHITECTURE

Apps	Apps	Apps
Libraries		
Hypervisor OS		
Computer		

docker

Content Delivery Network

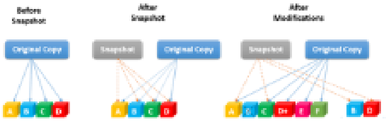


Copy on Write

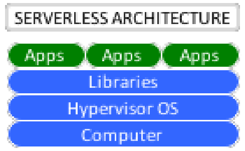
BLOCKCHAIN

The DIE Triad

BLOCKCHAIN



docker



Distributed

DDoS Resistant

The best solution against a distributed attack is a distributed service

Availability

Immutable

Changes Easier to Detect and Reverse

Unauthorized changes stand out and can be reverted to known good

Integrity

Ephemeral

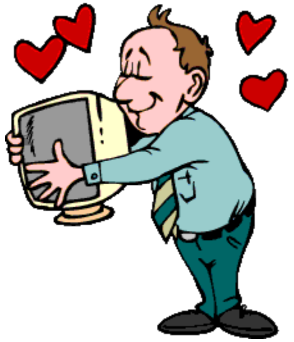
Drives Value of Assets Closer to Zero

Makes attacker persistence hard and reduces concern for assets at risk

Confidentiality

Pets vs Cattle

- Given a familiar name
- Taken to the vet when sick
- Hugged



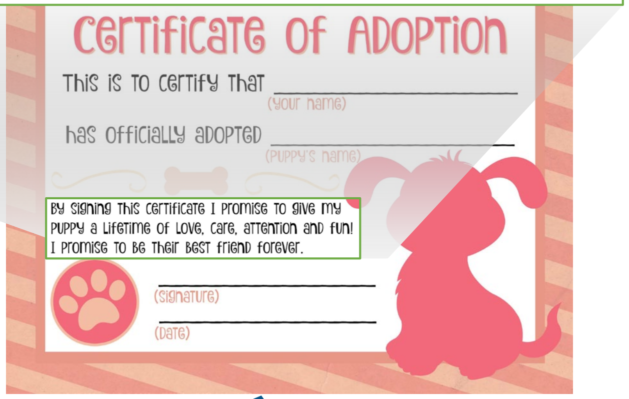
C.I.A.

- Branded with an obscure, unpronounceable name
- Culled from herd

D.I.E.

Pets vs Cattle Controls

By signing this certificate I promise to give my puppy a lifetime of love, care, attention and fun! I promise to be their best friend forever.



Certificate of Adoption

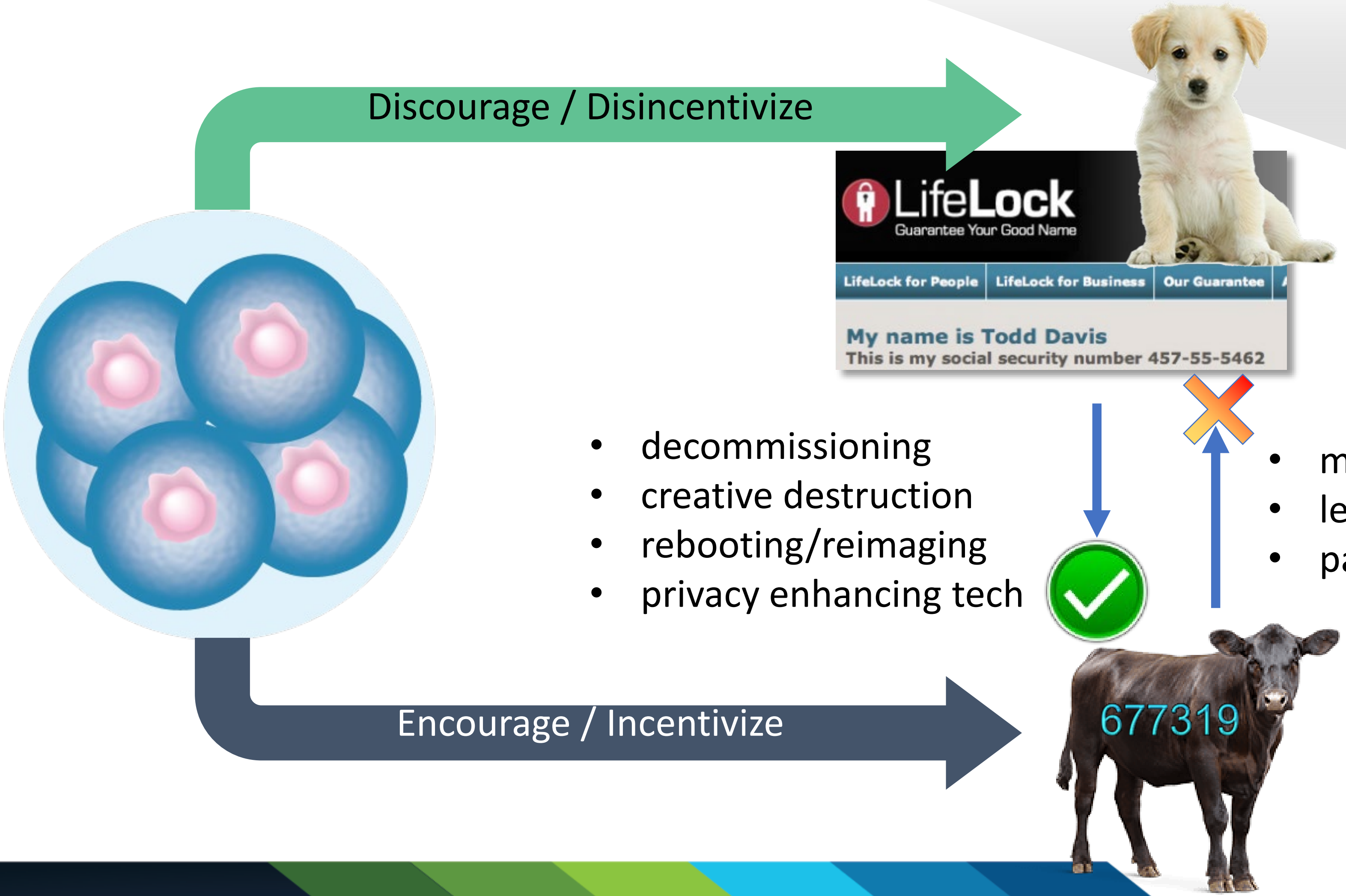
This is to certify that ______________________
(your name)

has officially adopted ______________________
(puppy's name)

By signing this certificate I promise to give my puppy a lifetime of love, care, attention and fun! I promise to be their best friend forever.

____
(signature)

____
(date)



My name is Todd Davis
This is my social security number 457-55-5462

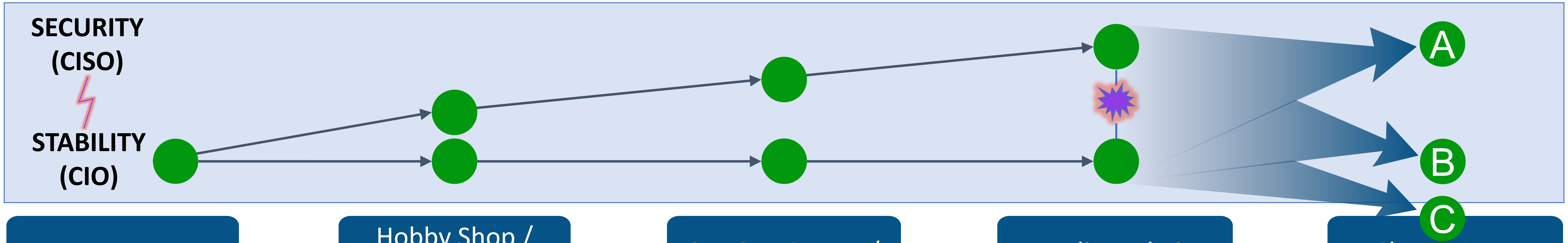
- decommissioning
- creative destruction
- rebooting/reimaging
- privacy enhancing tech

- modifying an immutable container
- letting an asset live longer than needed
- patching in place

Completing the NIST CSF

Era	1980 Identify	1990 Protect	2000 Detect	2010 Respond	2020 Recover
Core Challenges	What did we buy and how does it support the biz?	Viruses, Server-side Attacks, Insecure Configs	Too many logs and alerts, Client-side attacks	Assume Breach, Raging Fires, Too Many Privileges	Ransomware, MBR Wiper, DDoS, Firmware Bricking
Solutions	Asset Mgt, Systems Mgt Tools	Anti-Virus, Firewalls, Secure Configs	IDS, SIEM	Incident Responders & IR Tools (EDR, SOAR)	Distributed, Immutable, Ephemeral (DIE!!!) Systems

IT / Security Tension



Security Team Composition & Focus	None	Hobby Shop / Vulnerability Mgt	Sec Ops Center / Threat Mgt	Dedicated Biz Unit / Risk Mgt	Choose Your Own Destiny

Fragility vs Resiliency vs Antifragility

Destiny A

(C.I.A)

Harm mitigated through bolt-ons and workarounds that create instability

Destiny B

(D.I.E.)

Harm results in destruction but no change in configuration

Destiny C

(DIE + Creative Destruction)

Harm drives change that removes "pets" and makes the system even more DIE-like

Creative Destruction Redefined:
Intentional discovery and removal of unnecessary pets that exacerbate fragility

Icons made by Nhor Phai and FreePik

Summary

- The next era in IT and Security will manifest **more irreversible attacks** that challenge and undermine our ability to RECOVER
- Better PROTECT, DETECT, and RESPOND capabilities may reduce occurrences of malicious events but are **insufficient against well-executed destructive/irreversible scenarios**
- Our best countermeasure is to **avoid pet creation** (that requires CIA) and **promote cattle creation** (built to DIE)

3RD ANNUAL NATIONAL

CYBERSECURITY SUMMIT

For more information:

@sounilyu

https://cyberdefensematrix.com

https://www.linkedin.com/in/sounil

https://www.slideshare.net/sounilyu/presentations

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA