#ITCon22

Security: Rolling with the Punches

August 2022

IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

Todays Presenter:

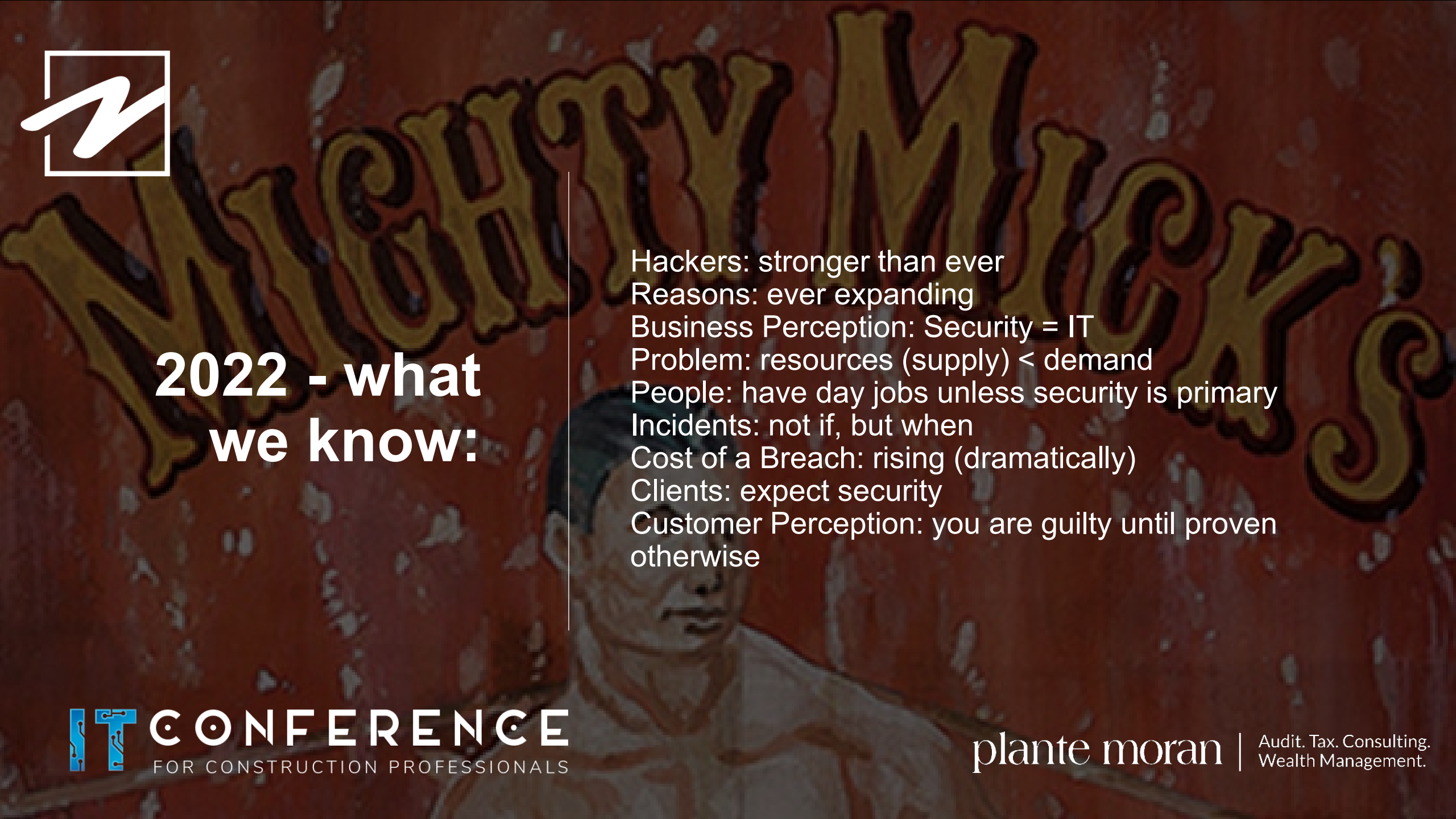
Joe Oleksak, CISSP, CRISC
Cybersecurity Partner
Plante Moran, PLLC
joe.oleksak@plantemoran.com
847-628-8860

IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

“Know thy enemy”

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

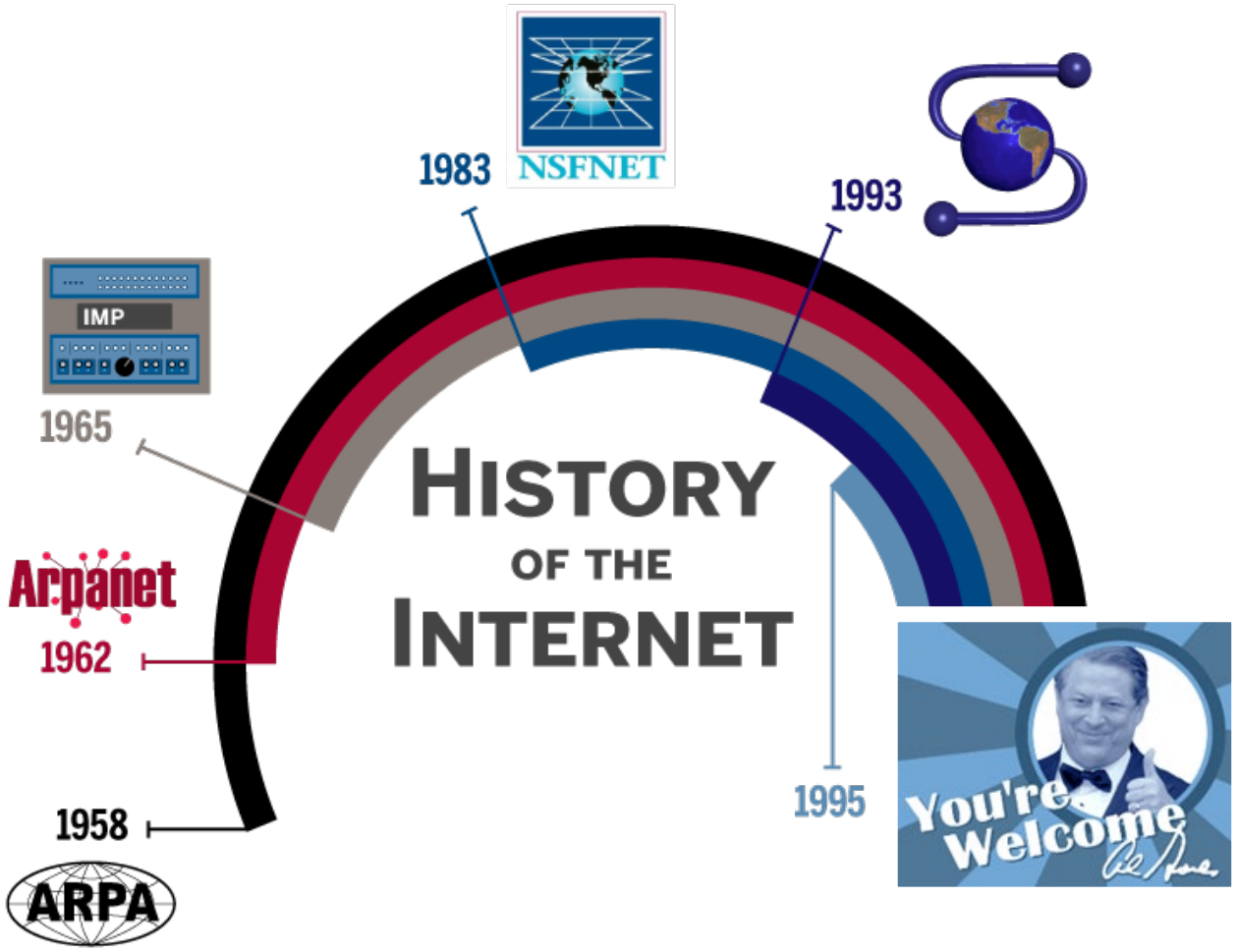


2022 - what we know:

Hackers: stronger than ever
Reasons: ever expanding
Business Perception: Security = IT
Problem: resources (supply) < demand
People: have day jobs unless security is primary
Incidents: not if, but when
Cost of a Breach: rising (dramatically)
Clients: expect security
Customer Perception: you are guilty until proven otherwise

How did we get “here”?

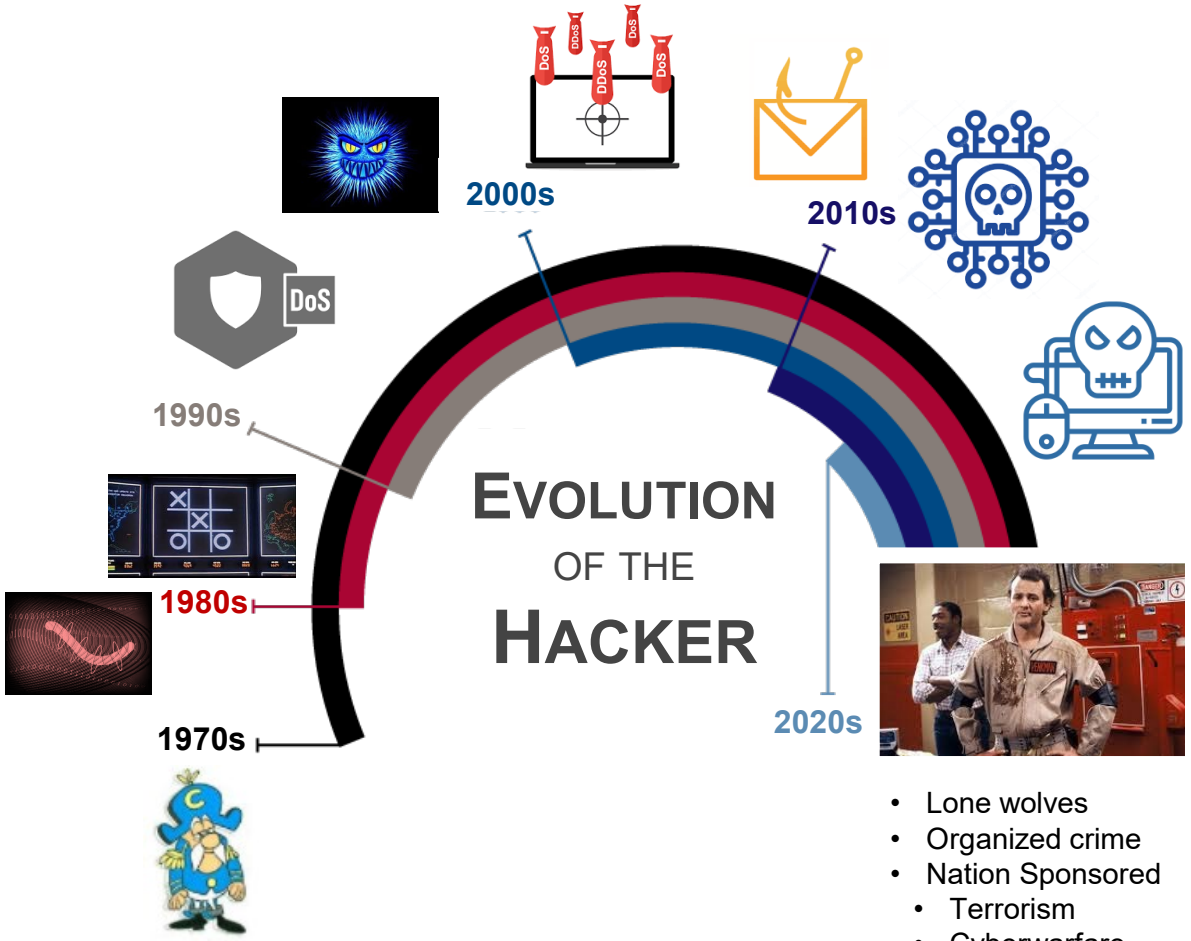
- The Internet was never designed with security in mind!
- Today, there are 22 billion connected devices
- By 2025 data from connected devices will go from 4 zettabytes (ZB) to 175 ZB



IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

How did they get “here”?

- Started with a toy in a cereal box!
- Seemed more a nuisance, but hey – we’re not a target
- “Cats and Dogs, living together… Mass hysteria!”



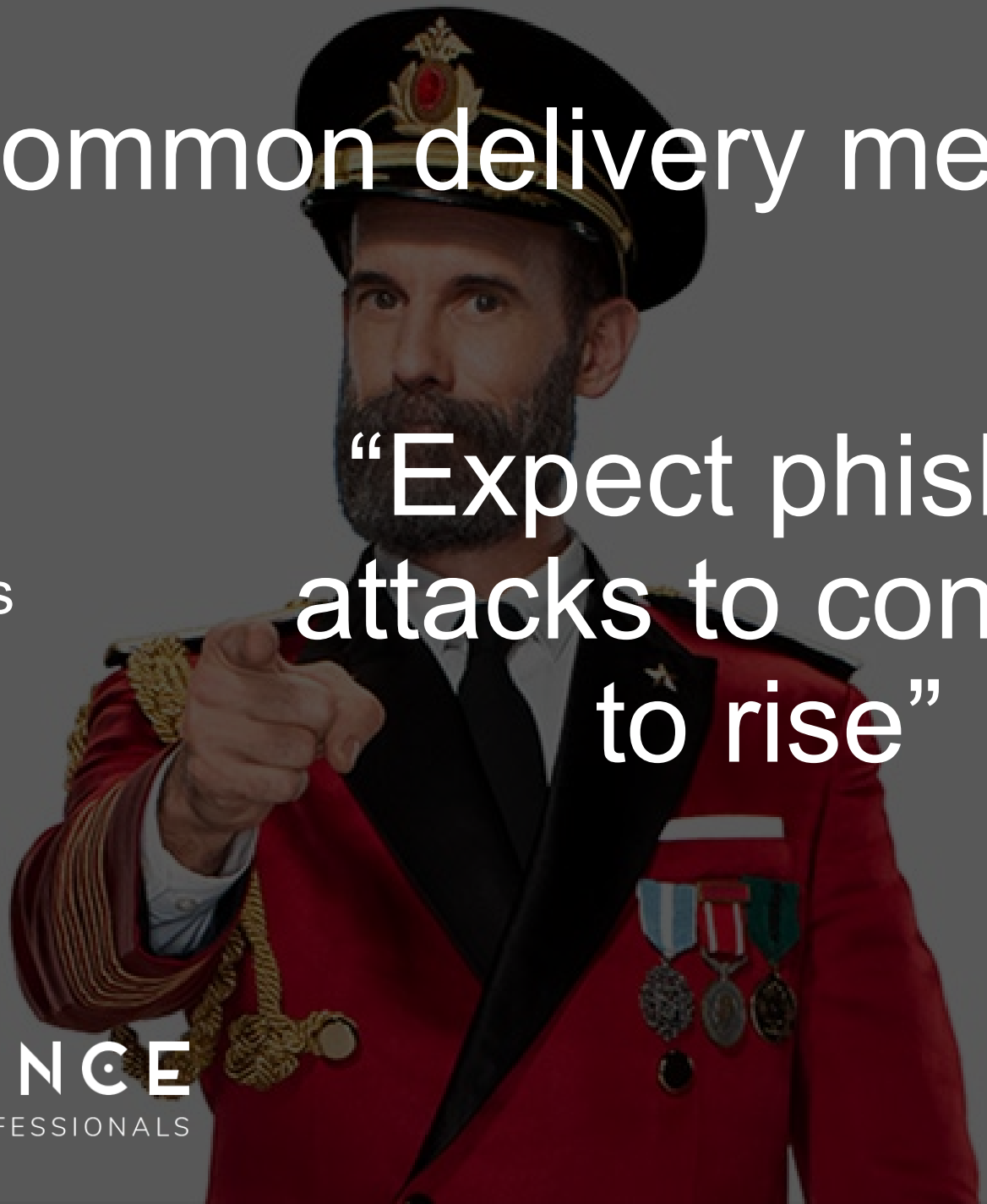
What is our current “reality”?

- Chances of getting struck by lightning: 1 in 1,000,000
- Chances of dating a millionaire: 1 in 250
- Chances of experiencing a data breach: 1 in 4

Depending on your source:

- The average time to intrusion discovery is upwards of 250 days
- The average cost of a data breach $800,000 – several million
- Spent another $900,000 – several million to restore normal business in the wake of successful attacks

Most common delivery method



"Expect phishing attacks to continue to rise"

- Captain Obvious

IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS


Three Most Likely Attack Strains
Ransomware
software designed to deny access to a computer system or data until a ransom is paid.
Malware
Software that is intended to damage, disable, or provide remote control over computer systems
Password Attacks
Easily guessed, cracked, or given away
IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

Did you see this one coming?

Did you know: Most of the vulnerabilities exploited throughout 2021 continued to be ones known by IT professionals at the time of the incident?

IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

Let’s “understand the ring”

What are you protecting?

Where are you protecting it?

How are you protecting it?

IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

Let's define "security"

- What is your organizations understanding of security?
  - Information Technology
  - Marketing, Sales, Client/Customer Service
  - Legal, Contracts, Vendor Management, Compliance
  - Physical Security, Worksite Security, Worksite Safety, Operations
  - Accounting, Finance…. Shall I go on?

Security maturity

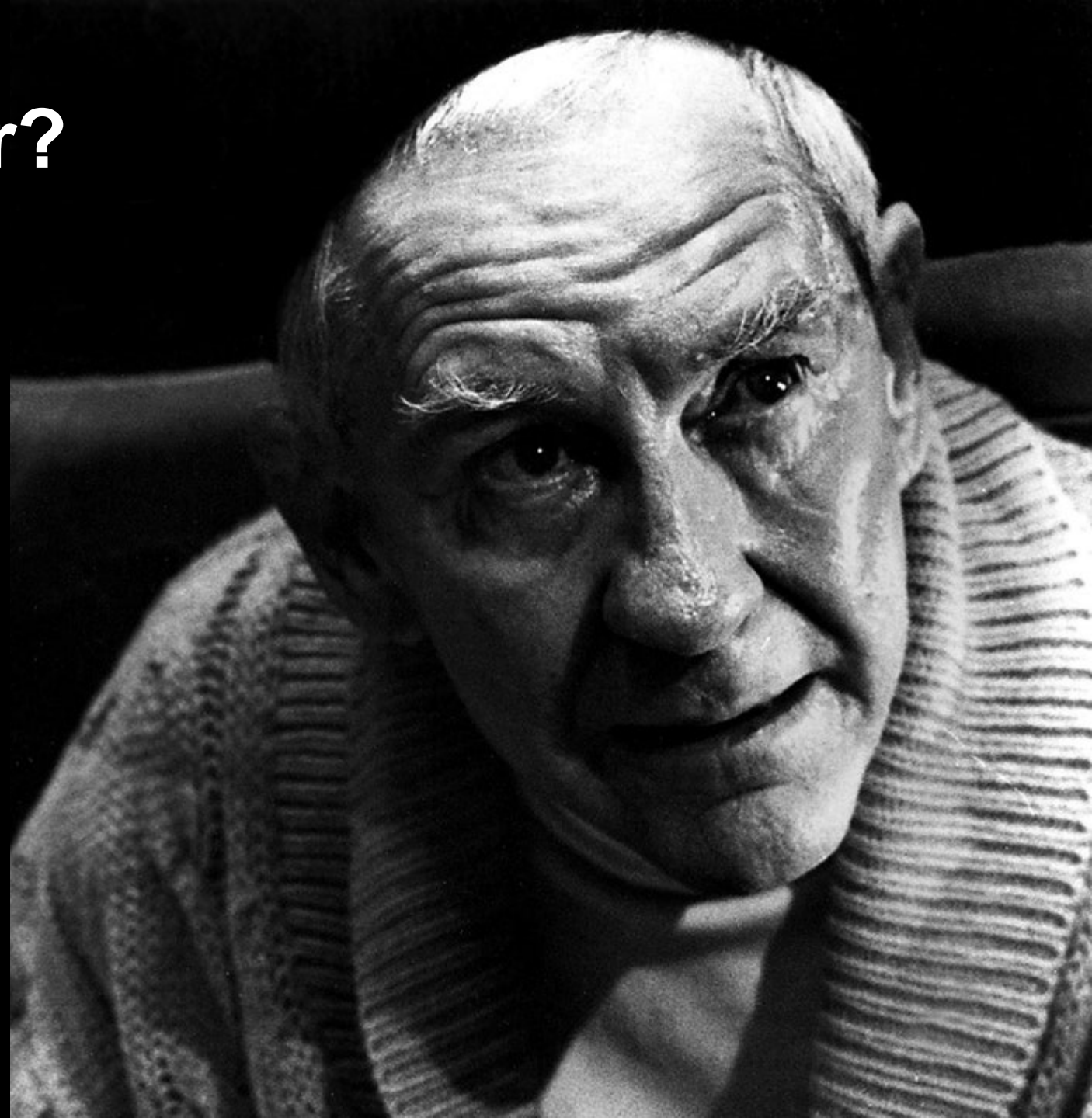
- What is the current maturity level of security within your organization?
  - Does the organization have an overall Security Strategy?
  - Is the responsibility for security a secondary function of a group(s)?
  - Does Security have its own “run budget”? What about “new asks”?
  - Do you have the programs necessary to stay ahead of security?
  - Do you have the tools necessary to make security visible?
  - What is your culture? Are your leadership and people buying into it?

A complete view

- Do you know what you are protecting?
  - Do you know where everything is?
  - Do you have all the tools you need to protect it?
  - Are people incentivized to protect it?
  - Do you understand the risks?
  - Do you monitor risk?
  - Do you adjust as risk changes?

Who’s in your corner?

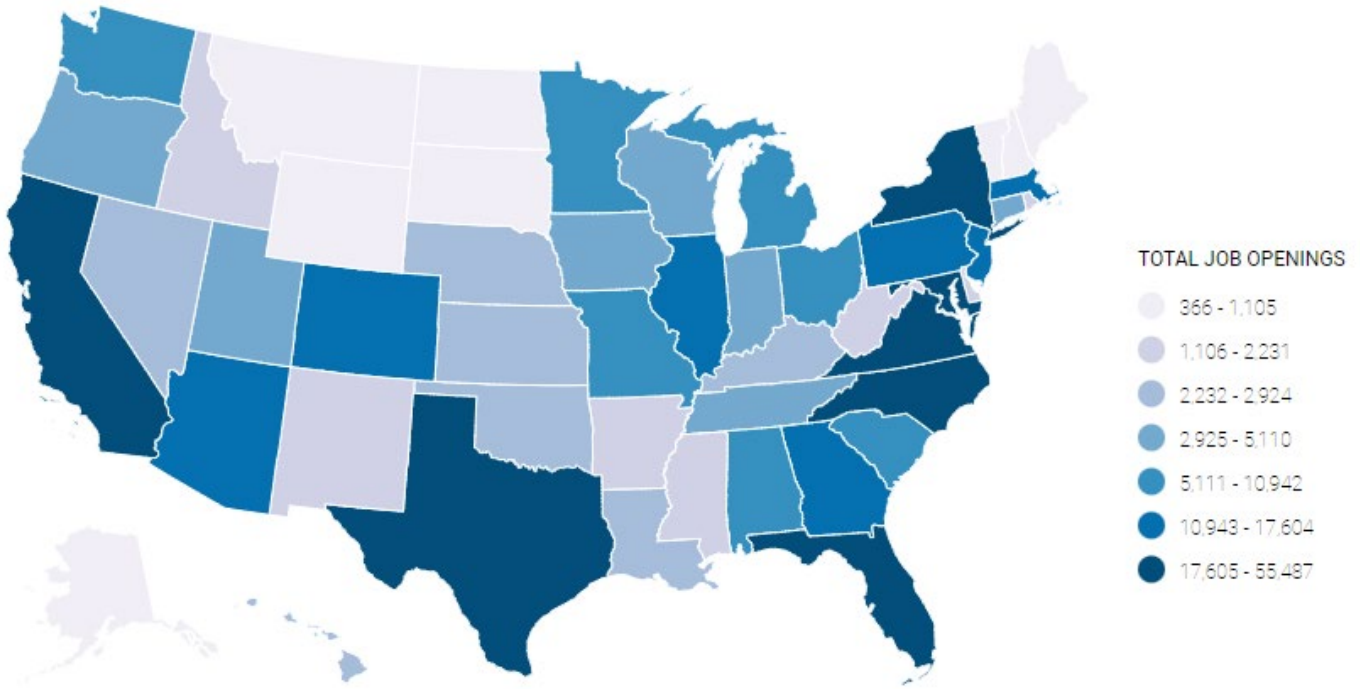
“The world ain’t all sunshine and rainbows. It’s a very mean and nasty place and I don’t care how tough you are it will beat you to your knees and keep you there permanently if you let it.”



IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

Where is the help?

- 464,420 open cybersecurity positions currently unfilled in the United States alone
- 2.93 million open cybersecurity positions currently unfilled world-wide
- Biggest complaints from those leaving Cybersecurity: limited budgets, limited training, always on the clock



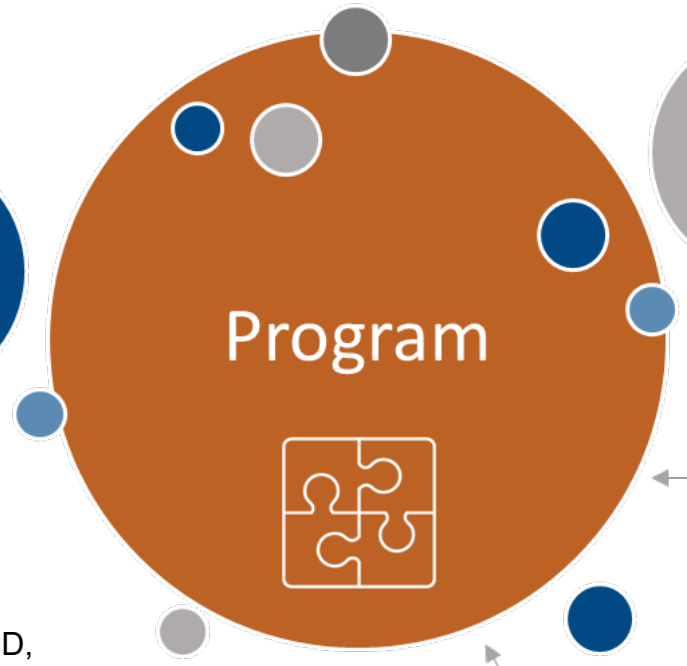
IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

“Know thyself”

How prepared are you for this fight?

IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

Asset Management: what we see



Ad Hoc: replaced after an issue, not planned on a schedule

Overlooked: overly reliant on automated solutions (even after known issues)

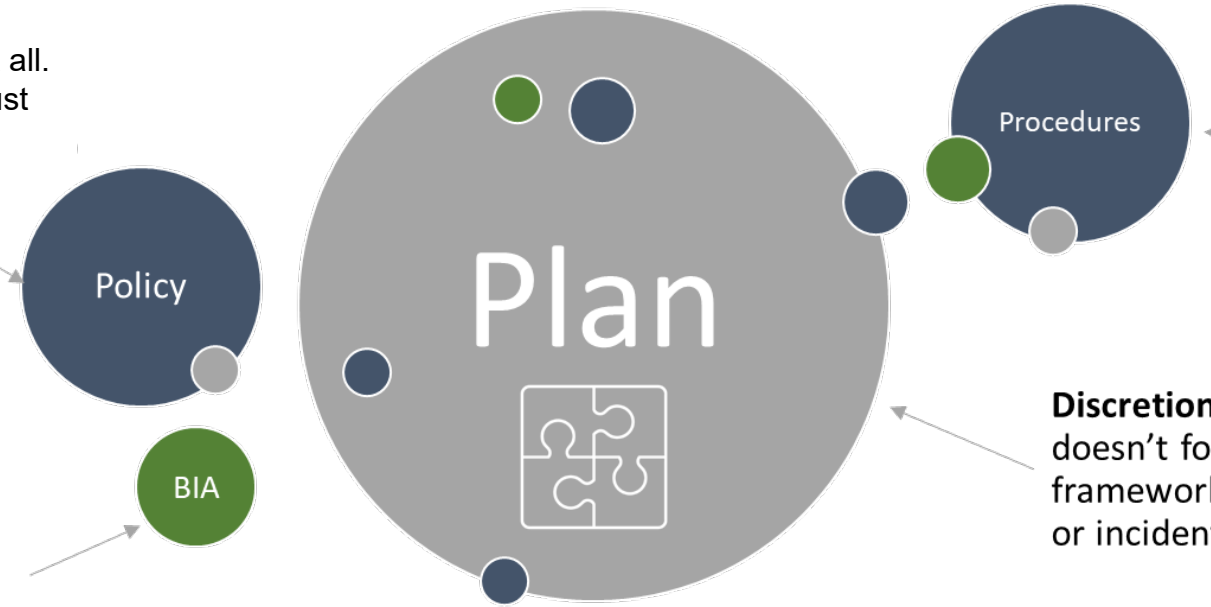
Outdated: Controls in place not focused on risks of remote workforce and ransomware threats of 2022

Blind Spots: Mobile Devices, BYOD, IOT, "exceptions to the rule" are not tracked and therefore not secured to company standards (if those standards exist)

Decentralized: owners don't always consider all business, cloud or vendor systems (aren't aware of)

Business Continuity: what we see

Vanilla: If they exit at all. Gathering dust as we speak



Subjective: indiscriminate inclusion/exclusion of certain procedures

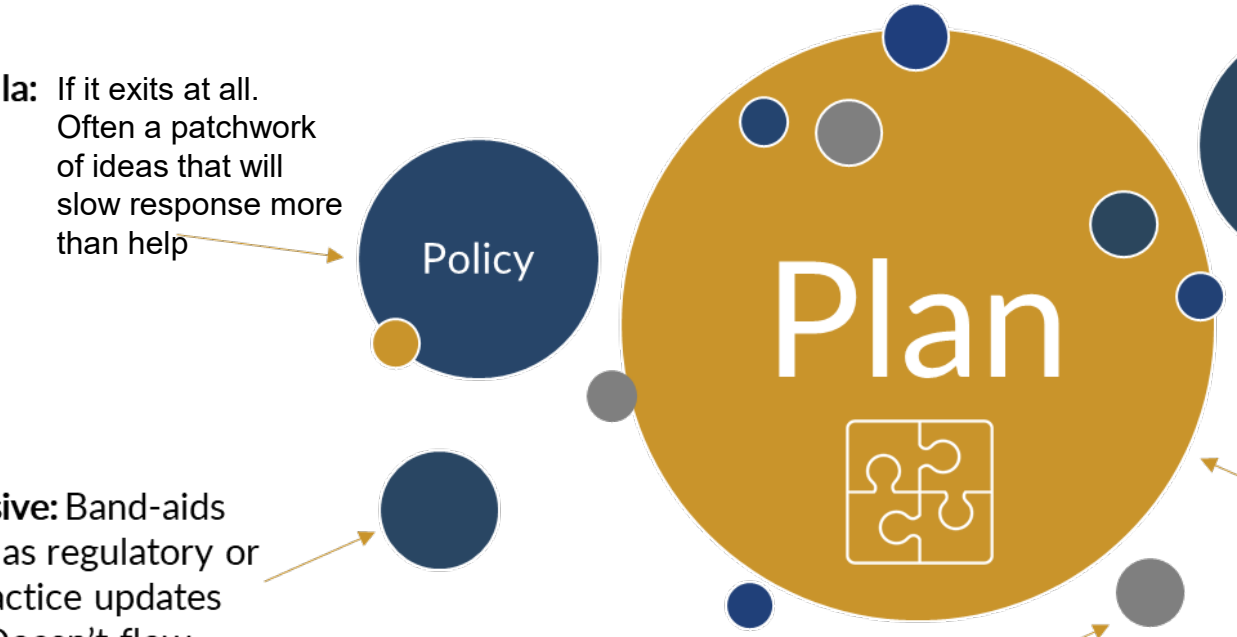
Discretionary: Generally doesn't follow a defined framework for all events or incidents to follow

IT Centric : Heavy on opinion from IT, the user is an afterthought. Not cohesively integrated in the overall program

Incohesive: Band-aids applied as regulatory or best practice updates occur. Doesn't flow.

Inconclusive: Specific business unit continuity testing either untested or testing undocumented.

Incident Response: what we see



Vanilla: If it exits at all. Often a patchwork of ideas that will slow response more than help

Subjective: indiscriminant inclusion/exclusion of certain procedures

Incohesive: Band-aids applied as regulatory or best practice updates occur. Doesn't flow.

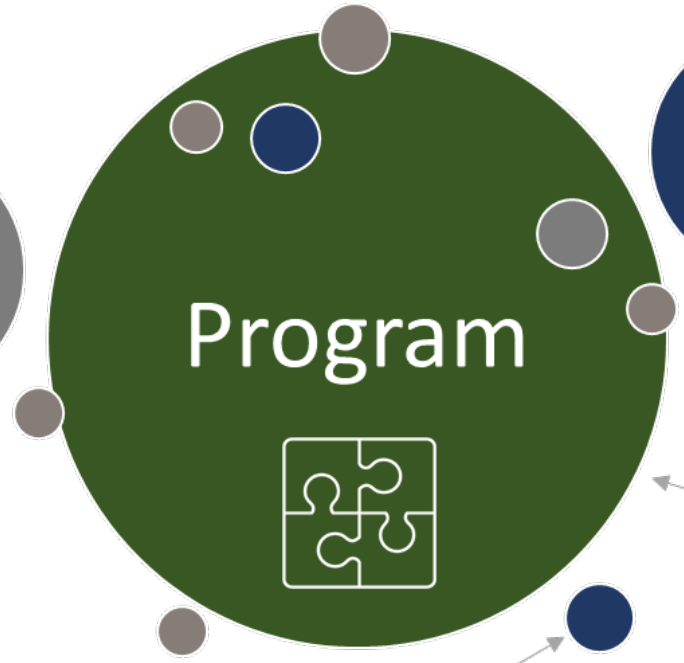
Discretionary: Generally doesn't follow a defined framework for all events, incidents and breaches to follow

MIA: Incorporation of information sharing, threat intelligence, and vulnerability management

Missed Opportunities: Results rarely incorporate back into the User Awareness Program

Vendor Management: what we see

Boilerplate: often not reviewed by security and key departments to ensure appropriate responsibilities are included



Point-in-time: not updated as relationship expands and reliance on vendor grows

No Teeth: Risk concerns and exceptions do not impact actual vendor relationships

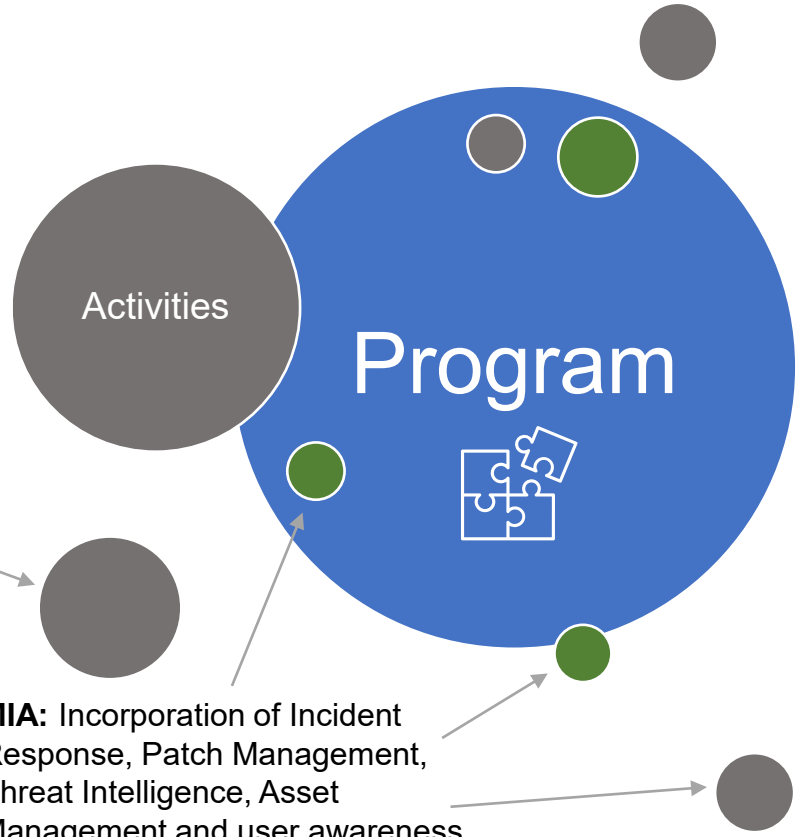
Inefficient: Annual reviews of information that does not tie to actual business risks

Lost in translation: "User Controls" are informally considered (at best) and are not incorporated into risk assessment or practice

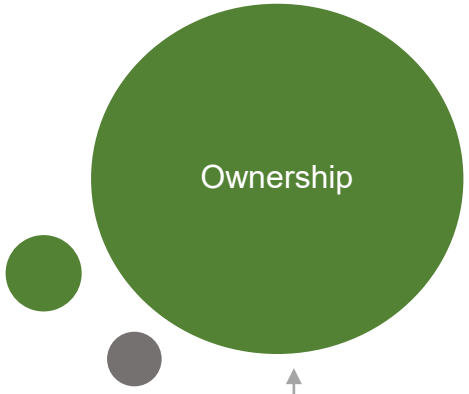
Vulnerability Management: what we see

What's the goal: Activities are undefined and inconsistently executed. Historical comparisons often unavailable due to inconsistencies

Who's on first: Output acted upon inconsistently, and progress is rarely monitored or enforced. IT has day jobs!



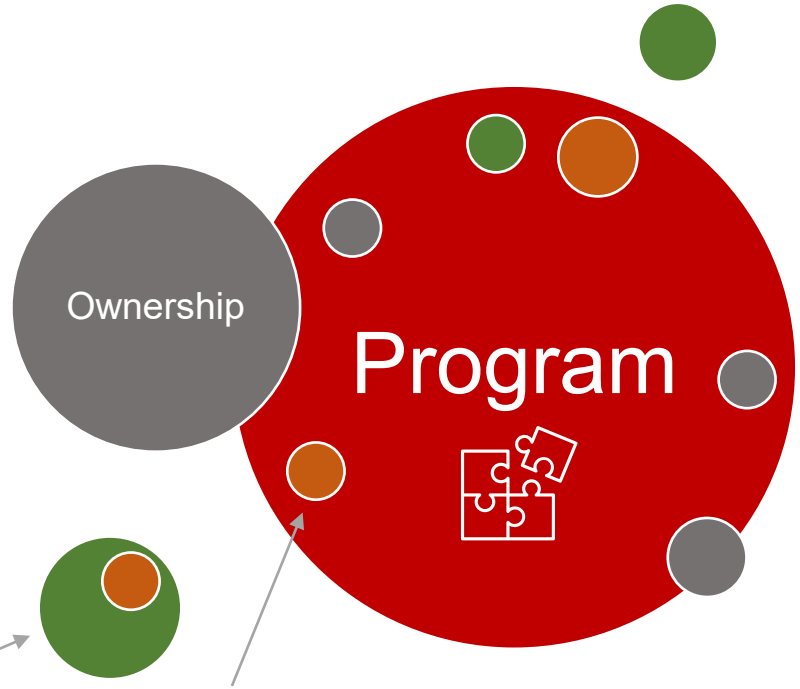
MIA: Incorporation of Incident Response, Patch Management, Threat Intelligence, Asset Management and user awareness



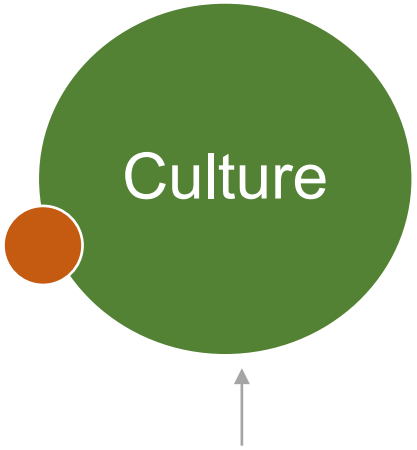
Dead on the vine: Consumed by IT, but rarely (never) summarized and reported to business leaders in a nontechnical/digestible way. Often resulting in reactive funding for security projects

Compliance Management: what we see

What's the goal:
Management expects IT to drive compliance without considering the cost (cultural, $, and time.) IT aren't compliance experts often biting off more than they can chew.



Pushing Paper: Development of Policy and Procedure is driven by governing body, often templates are used with the goal of checking a box. Culturally integration fails.

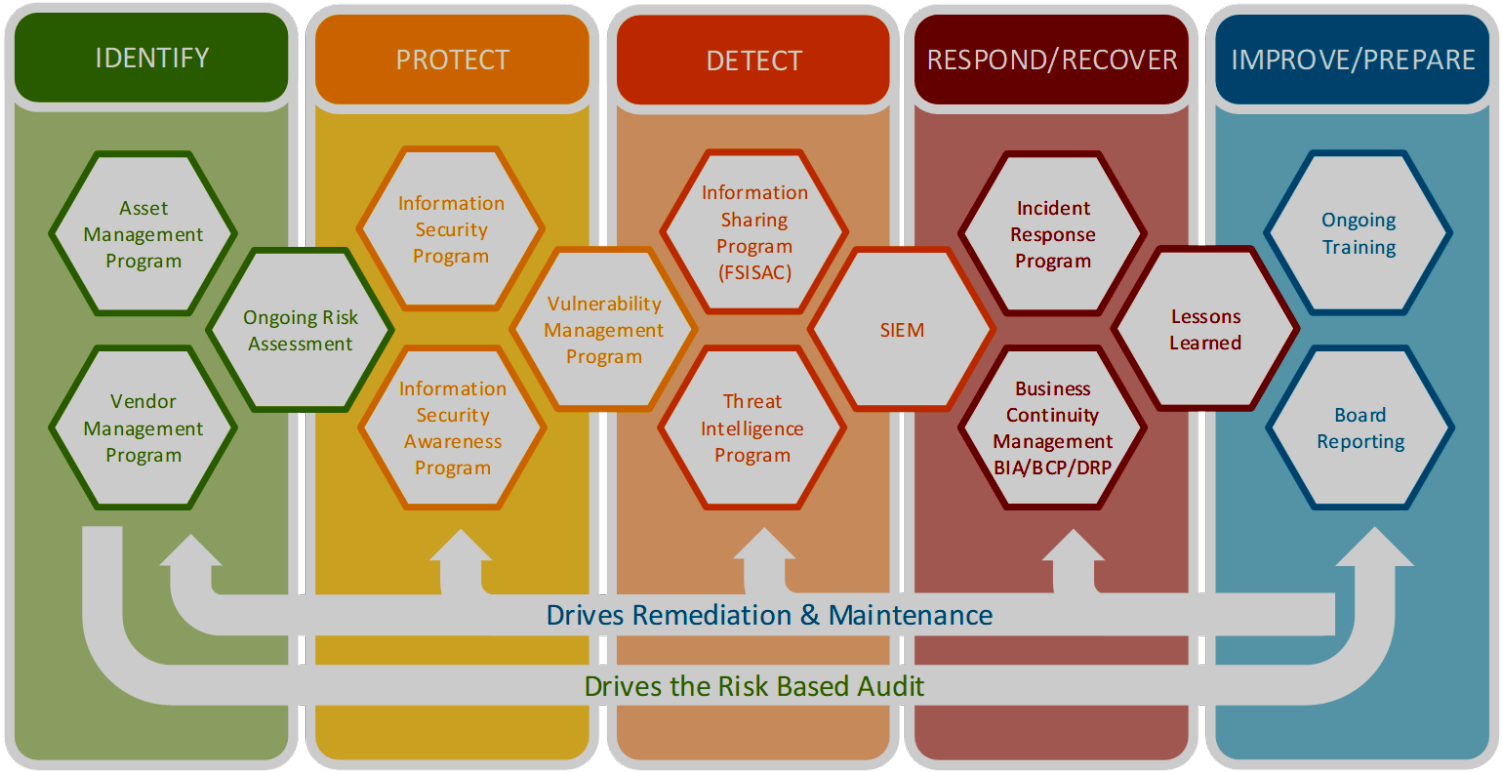


Belief: Compliance equals effort. Shortcuts are identified and compliance becomes a façade. The house of cards crumbles when an incident is severe.


Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat
IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

What's your strategy?

Let's learn from a highly regulated industry:



“The controls you’ve implemented today won’t necessarily address the risks of tomorrow.”

- Understand the ring
- Cybersecurity Strategy& Resource Planning
- Incident Response Planning
- Vulnerability Management Program
- Vendor Management
- Annual Assessments
- Strong Partnerships
- Know thyself

What does the future hold?

"The secret to your future is hidden in your daily routine."

IT CONFERENCE
FOR CONSTRUCTION PROFESSIONALS

#ITCon22

Questions?