# Cybersecurity Build-a-Plan Workshop

## Strategizing Cyber Resilience: Aligning with BEAD and Enhanced ACAM for a Secure Future

*WTA's Spring Educational Forum*

James Taylor
Sr. IT Security Consultant

VantagePoint
EMPLOYEE OWNED

# About the Presenter

James Taylor –

Sr. IT Security Consultant

Vantage Point Solutions, started 2016

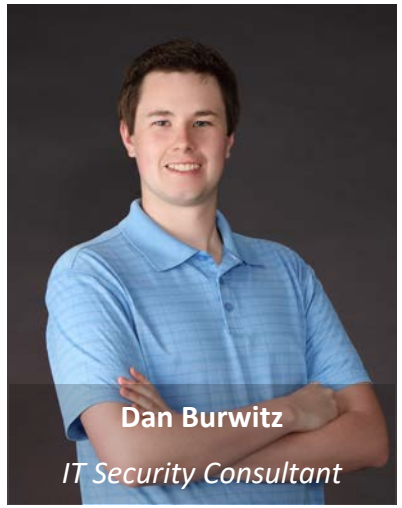
Background:

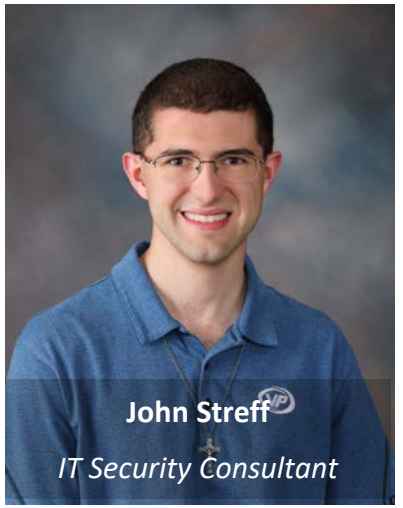
- Dakota State University with B.S., Computer Science (Information Security)
- Colorado University with A.S., Criminal Justice

Father of 3 boys (22,21,19, my wife is a saint) and 2 dogs

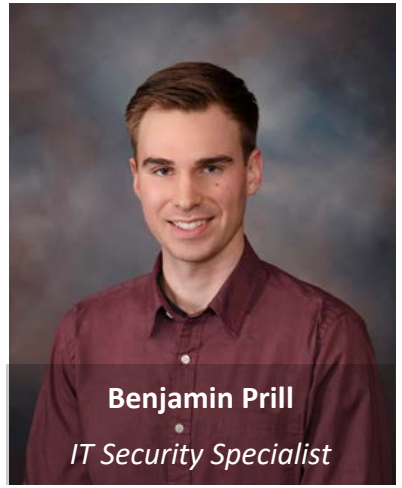
Fan of Capture the Flag Contests (CTF is like a scavenger hunt with computers) competitions, gaming, and training/teaching

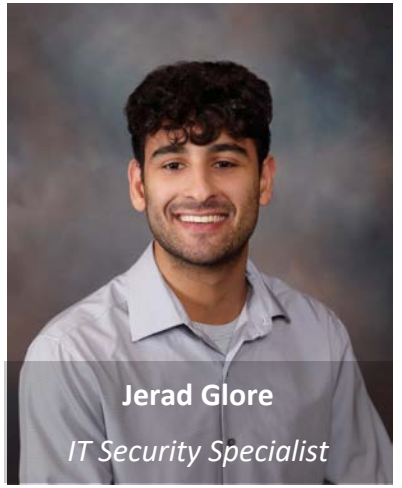
James.Taylor@vantagepnt.com







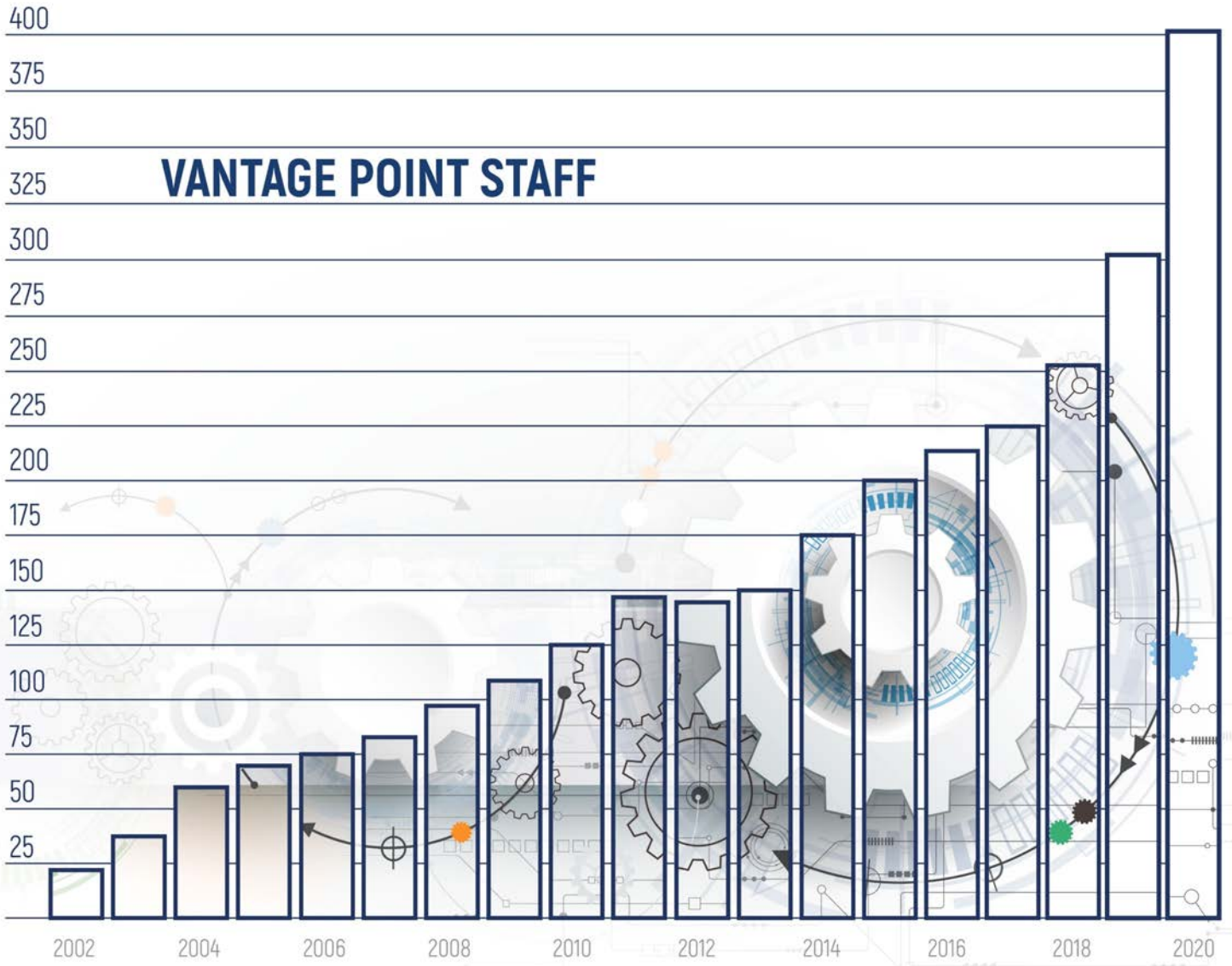
# Meet the Security Team

- James.Taylor@vantagepnt.com
- Dan.Burwitz@vantagepnt.com
- John.Streff@vantagepnt.com
- William.Gonzalez@vantagepnt.com
- Jerad.Glore@vantagepnt.com
- Benjamin.Prill@vantagepnt.com
- Justin.jaunay@vantagepnt.com

VantagePoint
EMPLOYEE OWNED

# **Vantage Point Solutions**, Mitchell, SD.

www.vantagepnt.com




With over 400 employees, VPS has the vast experience necessary to provide the best solution for any company. **Including yours.**

VPS serves **hundreds of clients**, large and small, across the country and internationally.

# Here for all your questions

- Enterprise Risk Management
- Audit
- Regulatory Compliance
- Independent Credit Review
- Cybersecurity
- Network Monitoring
- Server Virtualization
- Data Networking

# Todays Objectives

- Discuss and Define cybersecurity planning mechanisms
- Guidance of critical steps of a cybersecurity program
- Define the needs for compliance adherence
- Cybersecurity concerns overview

# What Does a Cybersecurity Plan Provide You

- Protecting data and infrastructure by creating a blueprint
- Prioritize risk/threats and create strategic plans
- Create controls and technical safeguards
- Create a culture around cybersecurity
- Incident Response (IR) Disaster Recover (DR) and Business Continuity (BC)

# Why build a cybersecurity program

- Protect yourself and your subscribers
- Backbone of the internet
- Prime targets for malicious actors
- Regulatory commitments and funding opportunities

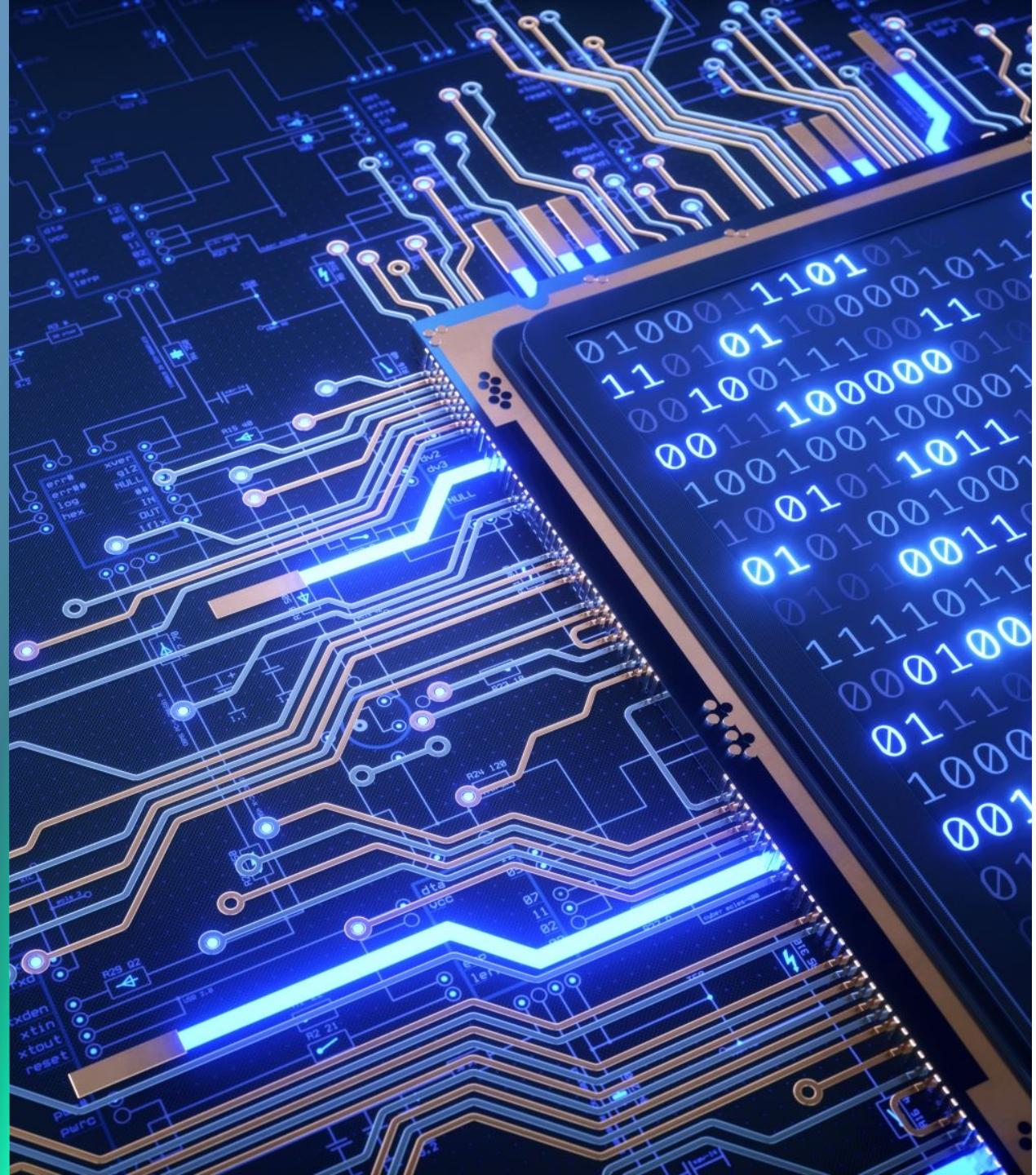
# Regulatory Bodies

National Institute of Standards and Technology (NIST) – Creates standards and measure, key cybersecurity frameworks.

Cybersecurity and Infrastructure Security Agency (CISA) - Responsible for cybersecurity and infrastructure protection.

Federal Communications Commission (FCC) – Create initiatives that influence ISP and TELCO cybersecurity approaches.

Some local Public Utilities Commission (PUC) – Depending on state.

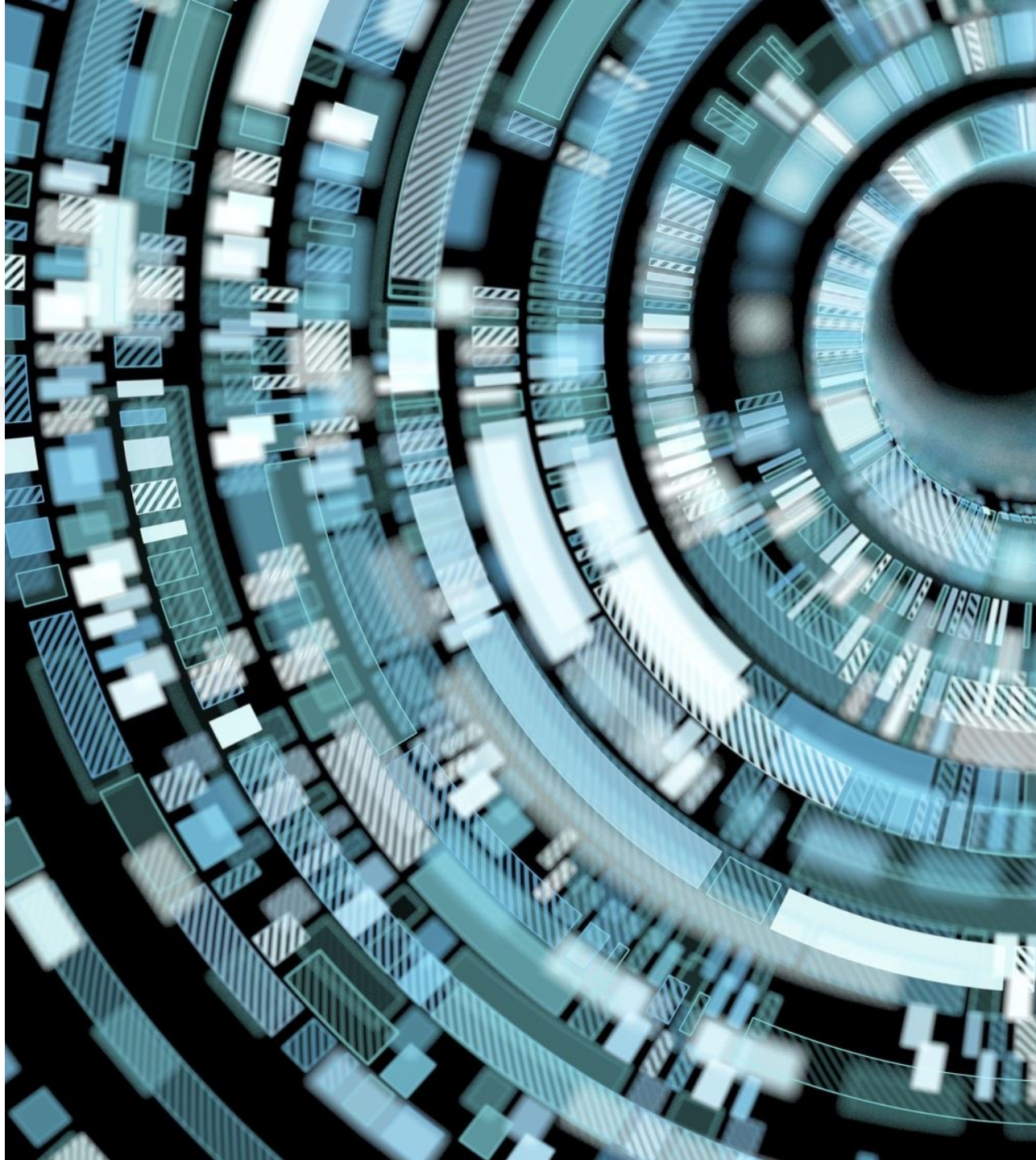


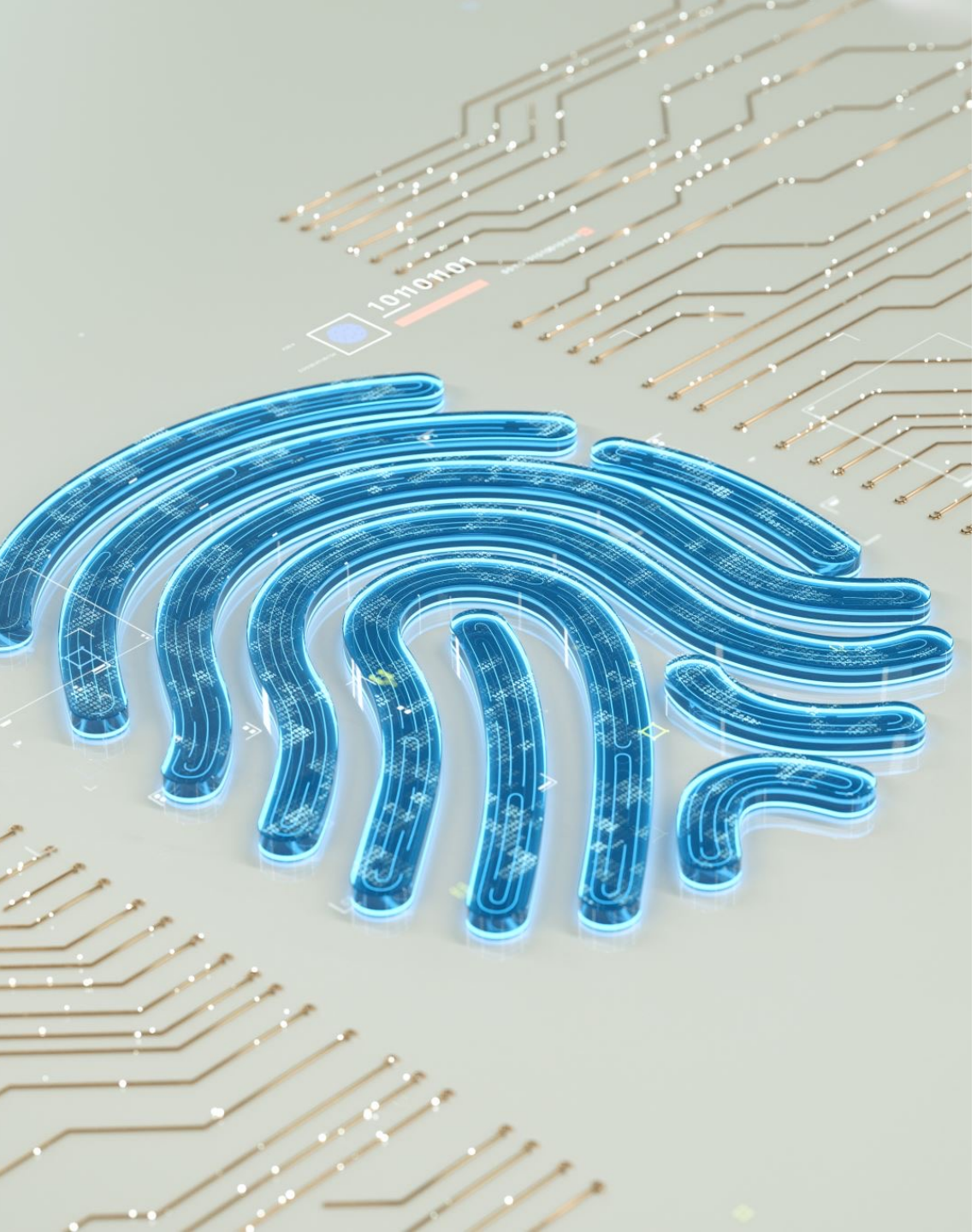
# NIST

- Created special publication 800-161 – Defines supply chain risk management
- NIST Cybersecurity Framework (CSF) - Guidelines for managing cybersecurity risks. Contain sections consisting of; Identify, Protect, Detect, Respond, and Recover.
- NIST 2.0 - Standards and guidelines

# CISA

- Part of the Department of Homeland Security (DHS)
- Analyzes and communicates cybersecurity risks
- Collaborates between private and public sectors
- Critical and essential infrastructure security





# FCC

- Cybersecurity labeling for IoT devices – can earn label “U.S. Cyber Trust Mark”
- Cybersecurity and Communications Reliability Division (CCR) works to ensure the reliability and security of communication networks
- The FCC collaborates with other government agencies like CISA to address cybersecurity issues

# Center for Internet Security (CIS)

- Non-profit organization established 2000
- Develop best practices, controls and benchmarks for a wide range of industries, devices and software
- Global collaboration among IT professionals

# Parts of a cybersecurity plan

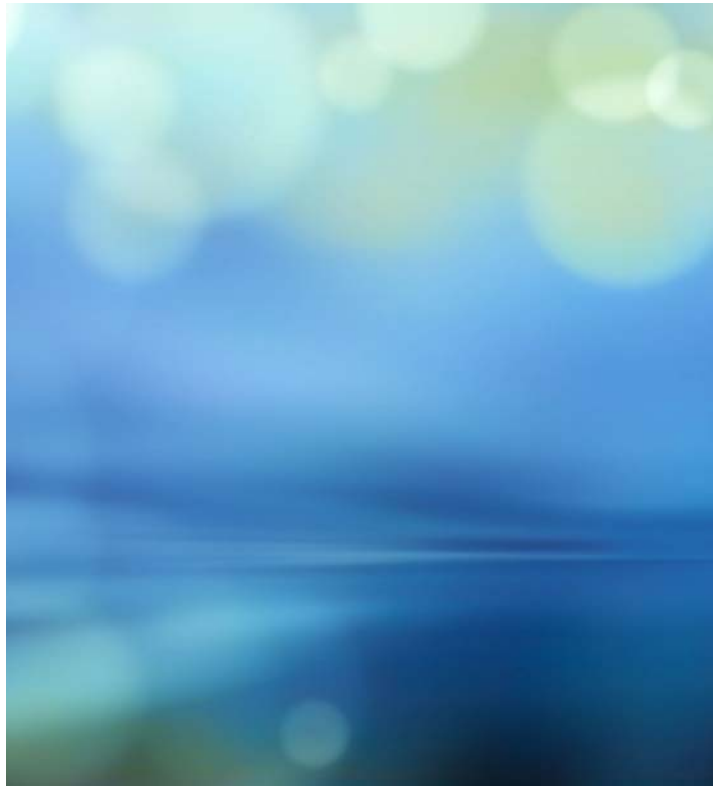
- Program guidelines and policies
- Risk Assessments (IT and supply chain/third party)
- Monitoring Systems
- Event and Metrics Logging Capabilities
- Data Backups - Testing
- Asset and Device Management
- Incident response and disaster recovery
- Physical security
- Vulnerability management
- Testing and Training
- Strategic Planning and Improvements

# Program guidelines and policies

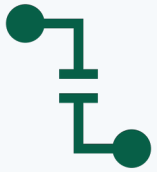
- Outlining  acceptable behavior and security measures for everyone
- Strong cybersecurity practices significantly reduces the risk of incidents
- Policies ensure adherence to specific data security standards
- Clearly define roles and responsibilities
- Raises awareness  among employees about threats and provides best practices
- Streamline decision making
- IR planning and recovery

# Risk Assessments (IT and supply chain/third party)

- Identify and address potential security weaknesses.
- Informed decision making
- Prioritize risk based on their severity and impact
- Allocate Resources
- Regulatory Compliance
- Benchmarks and Improvement



# Monitoring Systems



**Sources:**

Firewalls

Intrusion Detection Systems (IDS)

Intrusion Prevention Systems (IPS)

**Proactive approach enables you to take action and stop an attack before damage occurs.**

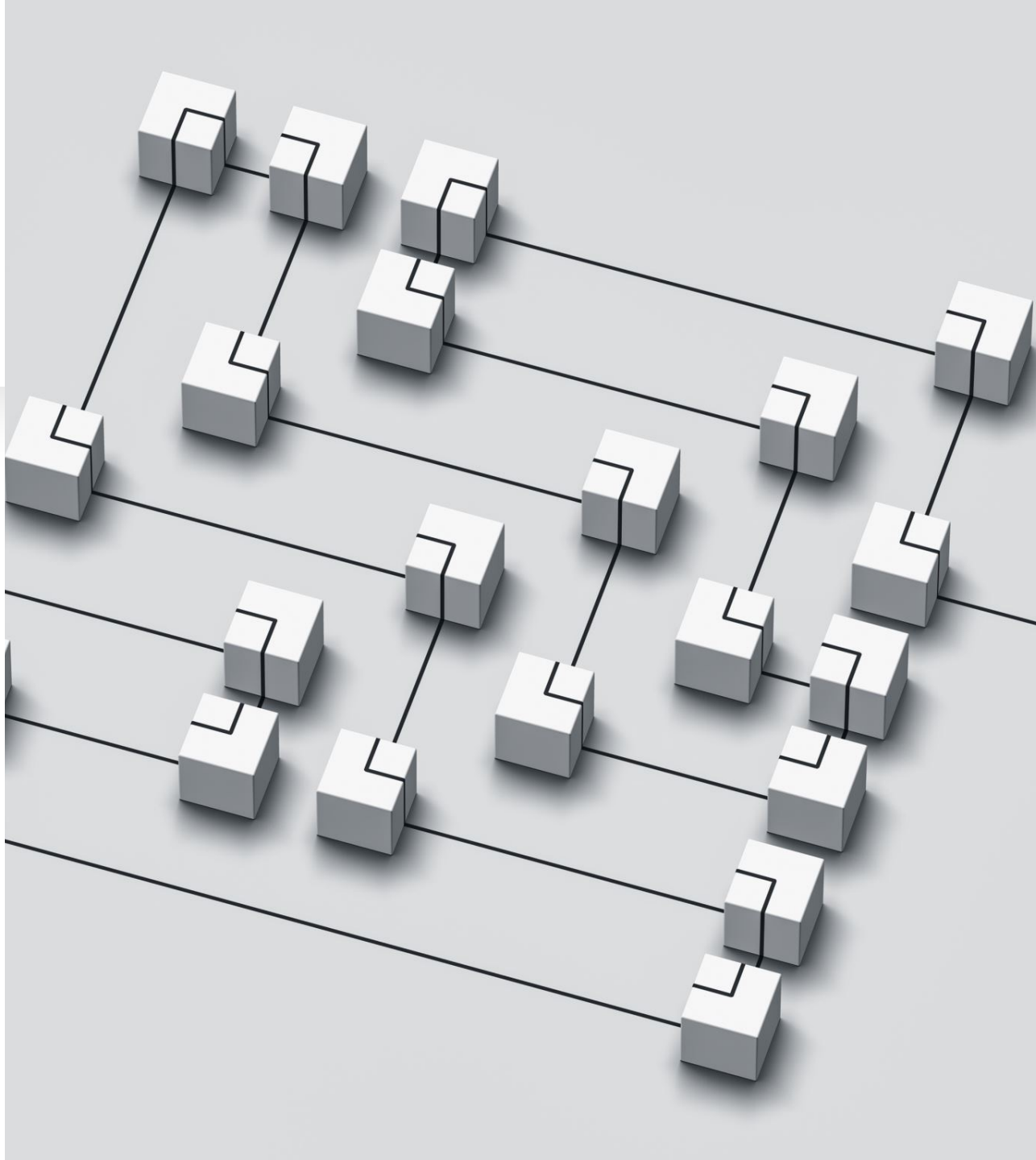
**Faster incident response**

# Event and Metrics Logging

- Security Information and Event Management (SIEM)
- Visibility into network activity
- Threat detection and investigation
- Compliance and auditing
- Critical devices and events
- Ingress/Egress traffic

# Data Backups

- Help recover from attacks or incidents
- Reduce leverage for any attackers (ransomware)
- Faster recovery and minimize disruptions
- Improve Business Continuity
- Constant testing and validation processes
- Backup of critical and essential data, system file, configurations, irreplicable or frequently used data



# Asset and Devices Management

- Endpoint management – patching/updates/configurations
- Mobile device management – remotely manage/security policies
- Endpoint detection and response
- Identity and access management – multi-factor authentication
- Should include an asset list for hardware/software/devices

# Incident Response/Disaster Recovery Plan

- Contain an incident quickly
- Faster and more efficient recovery process
- Identify causes of the security breach
- Minimize damages
- Should include team roles and responsibilities, inventory, risk assessment, training/practice, detection capabilities, containment and response procedures

# Physical Security

- Safeguard physical devices and infrastructure
- Deterrent from unauthorized access
- Mitigate social engineering attacks
- Environmental control
- Should include access controls systems, cameras, physical locks/barriers, perimeter security and security protocols in place

# Vulnerability Assessment

- Proactive defense
- Prioritize efforts
- Improve resource allocation
- Conduct regularly
- Multiple types of assessments
- Goal should be the remediation processes

# User Training and Testing

- Train, train, and train some more!
  - How to handle incidents
  - How to handle social engineering
- Test your employees to validate the training and fine-tune future trainings (inspect what you expect)
- Email and file sharing should be a focus
- Safeguards for users (AV, Email rule/filters, group policies)

# Strategic Planning and Improvements

- Ensure cybersecurity efforts alignment with overall business goals (buy-in)
- Provides a roadmap for security efforts
- Resource allocation
- Improve communication
- Effectively address evolving threats
- Should include a budgeting process, regular reviews and updates, metrics and measurements and communication/awareness

# Considerations

IDENTIFY YOUR CROWN JEWELS

RESEARCH AND IDENTIFY THE MOST COMMON THREATS (ISAC/MITRE)

ADDRESS SECURITY GAPS BEFORE THEY ARE EXPLOITED

TAILOR THINGS TO YOUR SPECIFIC NEEDS

BOARD BUY IN

# Board Buy In

| | |
|---|---|
| Focus on | Focus on Business Impacts |
| Quantify | Quantify the risks |
| Present | Present a clear strategy |
| Focus on | Focus on Return-on-Investment (RIO) |
| Share | Share real-world examples |
| Highlight | Highlight the regulatory landscape (rules/fines) |

# Timelines

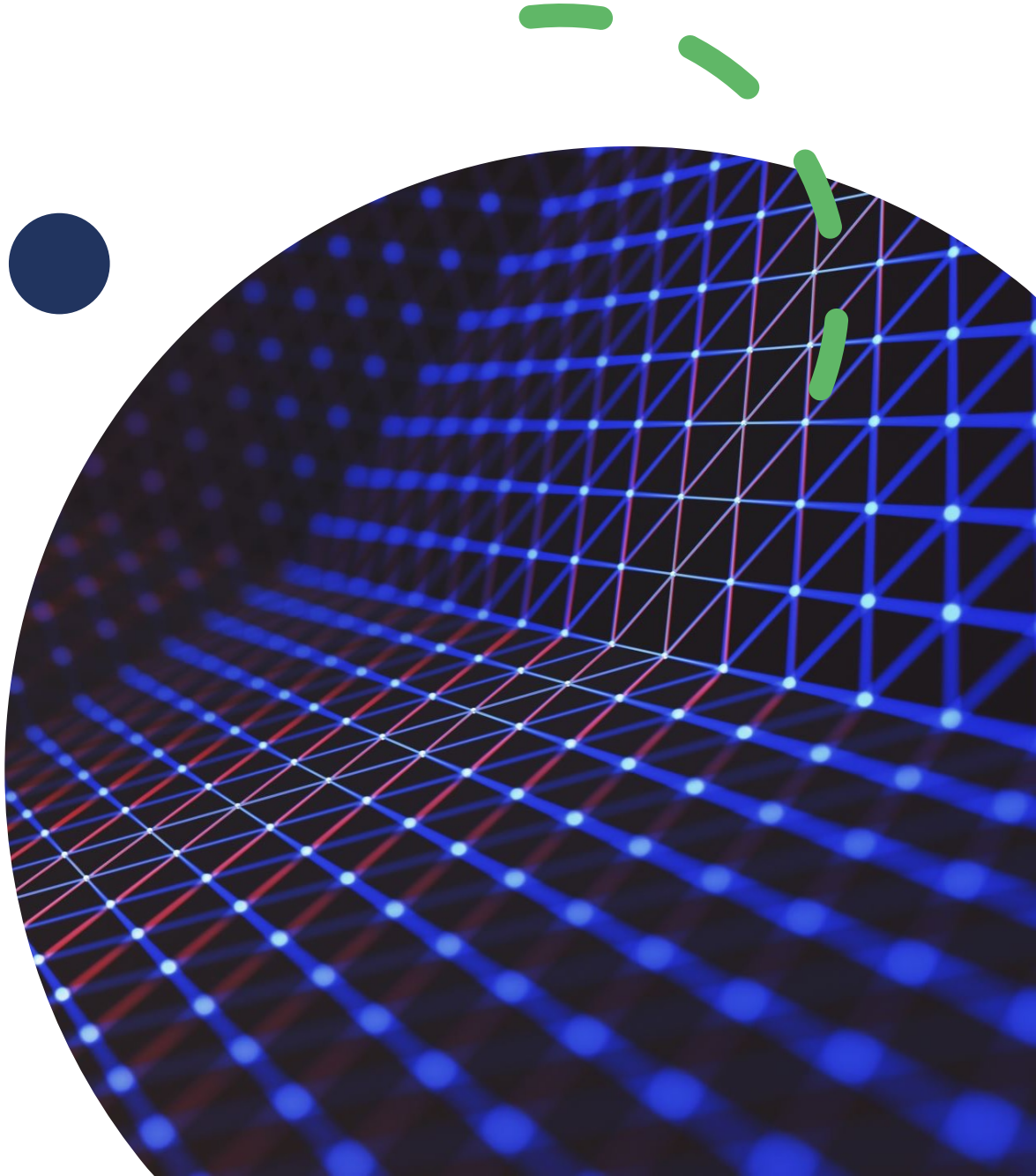
- When do I do what?
- Depends on:
  - Size of organization
  - Oversight
  - Budgeting/resources
  - Culture
  - Starting point

# Cybersecurity Funding Requirements

- Broadband Equity, Access and Deployment (BEAD) program
- Enhanced Alternative Connect America Cost Model (ACAM) program
  - Cybersecurity Plan
    - Should align with the latest NIST Cybersecurity Framework 2.0
    - Include risk assessment and continuous reevaluation
  - Cybersecurity Supply Chain Risk Management (C-SCRM)
    - Third party critical vendors and service providers
    - Include NIST 800-161 and NISTIR 8276

# Real world consequence

- Data loss including breaches
- Operation disruption and downtime
- Compliance issues and fines
- Financial loss or revenue loss from incidents



# Data Breaches

- AT&T – 74 Million customers - passcodes and social security numbers, emails and mailing addresses, phone numbers and birth dates.
- T-Mobile – 37 Million customers – Names, email and mailing address, birth dates, phone numbers
- Carriers have a unique responsibility to protect customer information. When they fail to do so, we will hold them accountable”.  Said the FCC spokesperson

# Fines and regulatory issues

- T-Mobile – 2021 - $350 Million in fines, $150 Million in upgrades - $500 Million in total
- AT&T– 2015 – $25 million in fines

## Malware/ransomware

CGM Software Solutions - unauthorized party accessed consumers' sensitive information, names, social security numbers, financial account information, health insurance information, addresses, dates of birth, and driver's license numbers.

# Most exploited vulnerabilities - MITRE

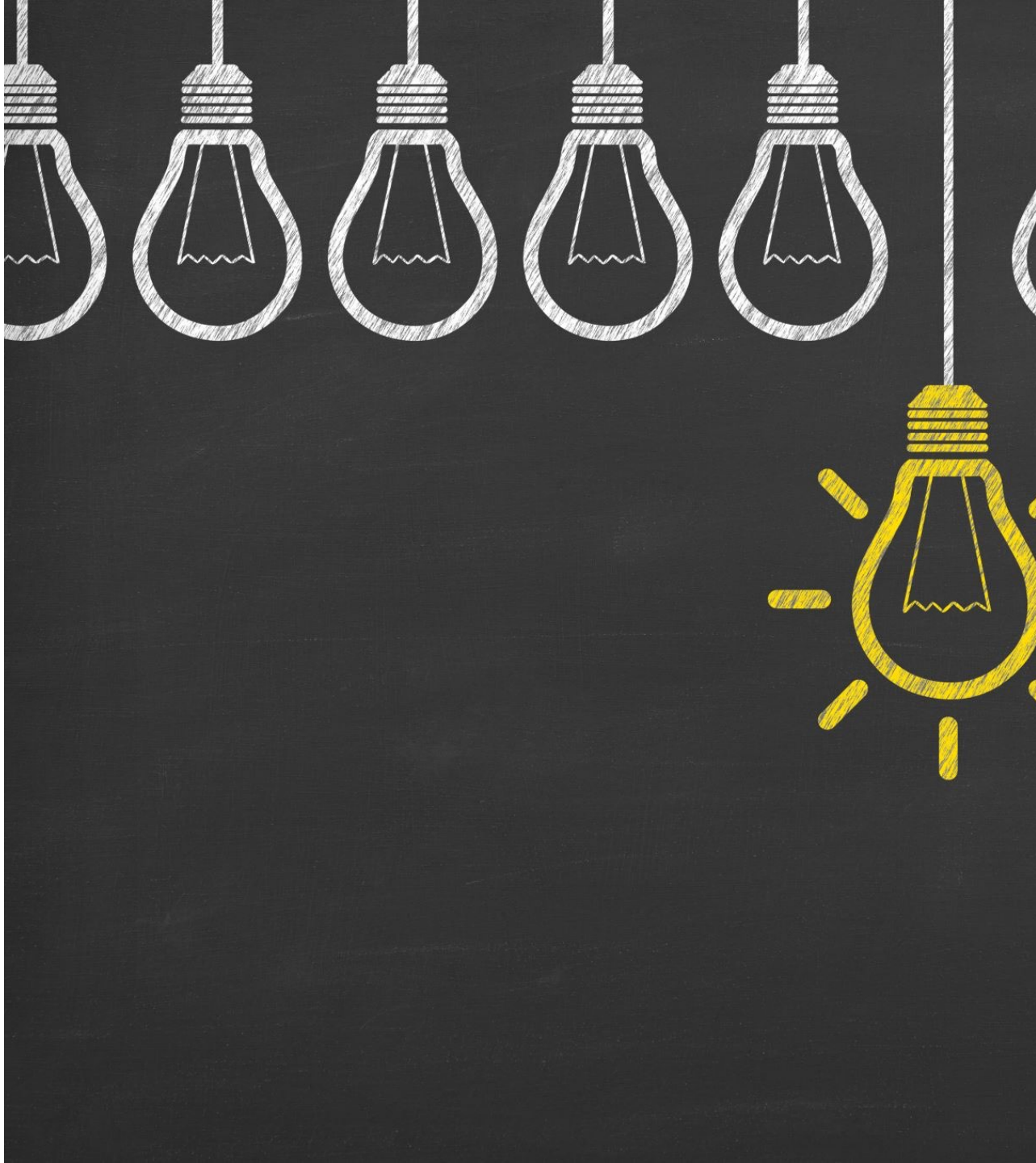
- **Vulnerability**
  - Phishing
  - Malicious scripts and software
  - Credential Access (breaches, valid accounts, old accounts)
- **Mitigation**
  - Anti-spoof email mechanisms (Filters, SPF, DKIM, DMAR), User education
  - Restrict user access, monitor behaviors, user education, system updates/patching
  - MFA, password hygiene, user education, endpoint security, access controls

# Adapting to future cybersecurity needs

- Proactive approach
- Embracing new technologies
- Holistic, layered security integration through all business processes
- Collaboration – you are not alone!

# Summary

- Why cybersecurity is so important
- What goes into a cybersecurity plan
- What are the regulatory bodies and funding requirements
- Real world consequences



# Q&A Session


- **James Taylor**
- **Vantage Point Solutions**
- *Sr. IT Consultant*
- James.Taylor@vantagepnt.com

# Thank You

VantagePoint
EMPLOYEE OWNED