UNITED STATES POSTAL SERVICE ®

“The convergence of IT Governance & Information Security Programs”

Chuck McGann

Corporate Information Security Officer

CISSP, CISM, IAM

CISO

CORPORATE INFORMATION SECURITY OFFICE

CONFIDENTIALITY · INTEGRITY · AVAILABILITY

Disclaimer

The opinions and information shared in this presentation are those of the speaker (endorsements or indictments of any product or vendor) and do not reflect the official USPS position on those resources.

UNITED STATES POSTAL SERVICE®

Key Thoughts

- Plenty of talk about Governance and Information Security Programs – when there is a breach, each can be looked at as a point of failure.
- Should the programs be interdependent or separate?
- Pros and cons of Governance and Security Programs,
- What does Governance mean to Security Programs and to The Business?
- What happened to just “doing the right thing”?

CISO
CORPORATE INFORMATION SECURITY OFFICE
CONFIDENTIALITY · INTEGRITY · AVAILABILITY

Importance of Security

- **IT Security (Info Sec):** Is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take.

- **Webster:** the quality or state of being secure, freedom from danger, safety, freedom from fear or anxiety

CISO
CORPORATE INFORMATION SECURITY OFFICE
CONFIDENTIALITY · INTEGRITY · AVAILABILITY

Importance of IT Governance

- **Corporate Governance:**

  In the case of a business or of a non-profit organization, governance relates to consistent enforcement and management, cohesive policies, guidance, processes and decision-rights for a given area of responsibility

- **IT Governance:**

  A subset discipline of corporate governance focused on information technology (IT) systems and their performance and risk management

CISO
CORPORATE INFORMATION SECURITY OFFICE
CONFIDENTIALITY · INTEGRITY · AVAILABILITY

Example of the Difference

CISO
CORPORATE INFORMATION SECURITY OFFICE
CONFIDENTIALITY · INTEGRITY · AVAILABILITY

Threats Across Industries

GoDaddy Sites Down, May Be Victim Of Anonymous Cyberattack

Zappos cyber attack

ID info hacked

MasterCard website is target of cyber attack

Wells Fargo is latest victim in cyber attack spree

September 25, 2012 | By E. Scott Reckard

6.5 Million of LinkedIn Passwords Stolen By Cyber Criminals

Software news

Cyber attacks on Android devices increasing

Banks on High Alert After Cyber Attacks

Cyber Breach Exposes EPA Staff's Bank Numbers, Addresses

Bank of America Hit By Cyber Attack

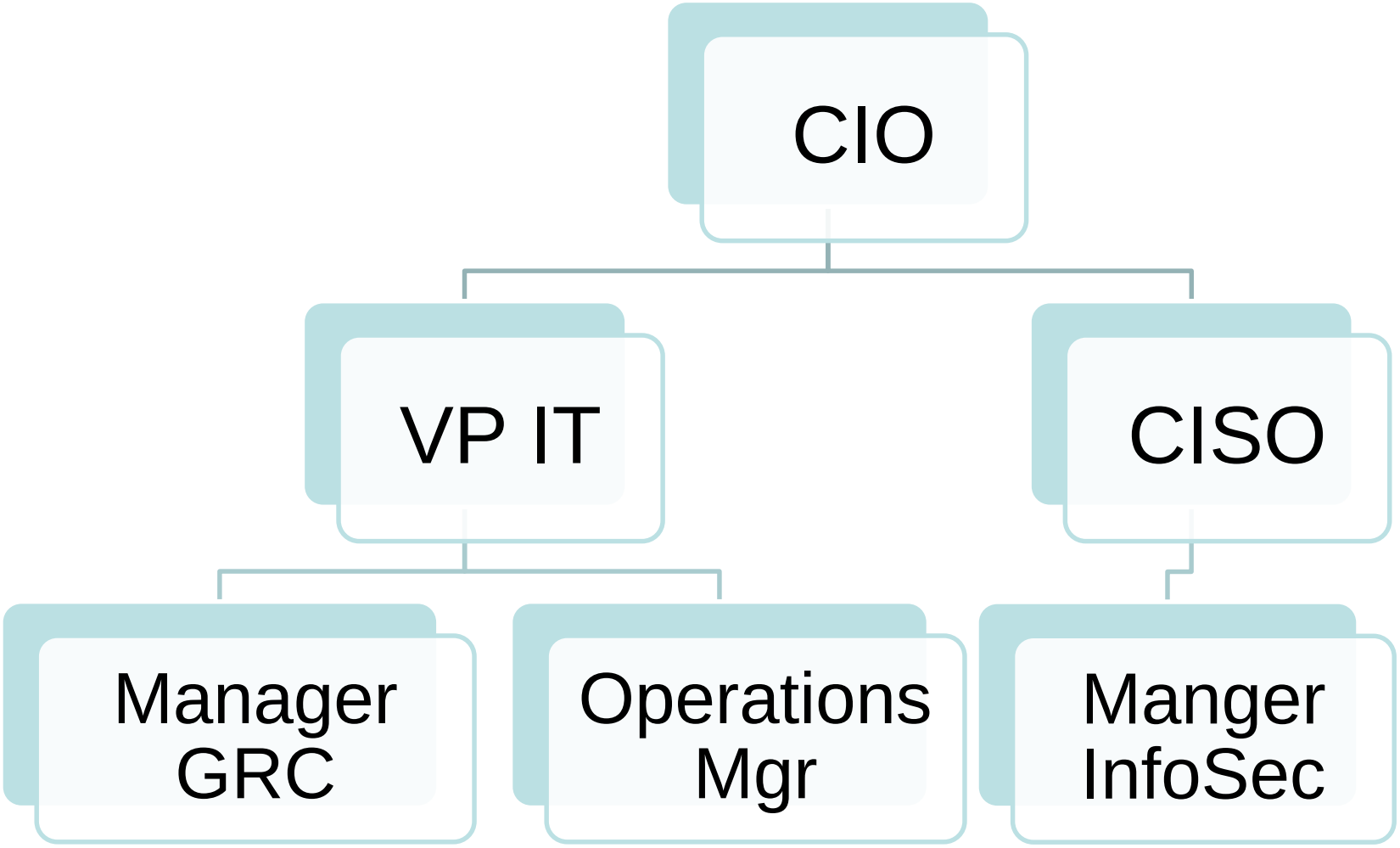
Governance Tools

- Accountability
- Business objectives
- Compliance reports
- System outages
- Customer complaints
  - Internal/External
- Successful Compromises

Security Tools

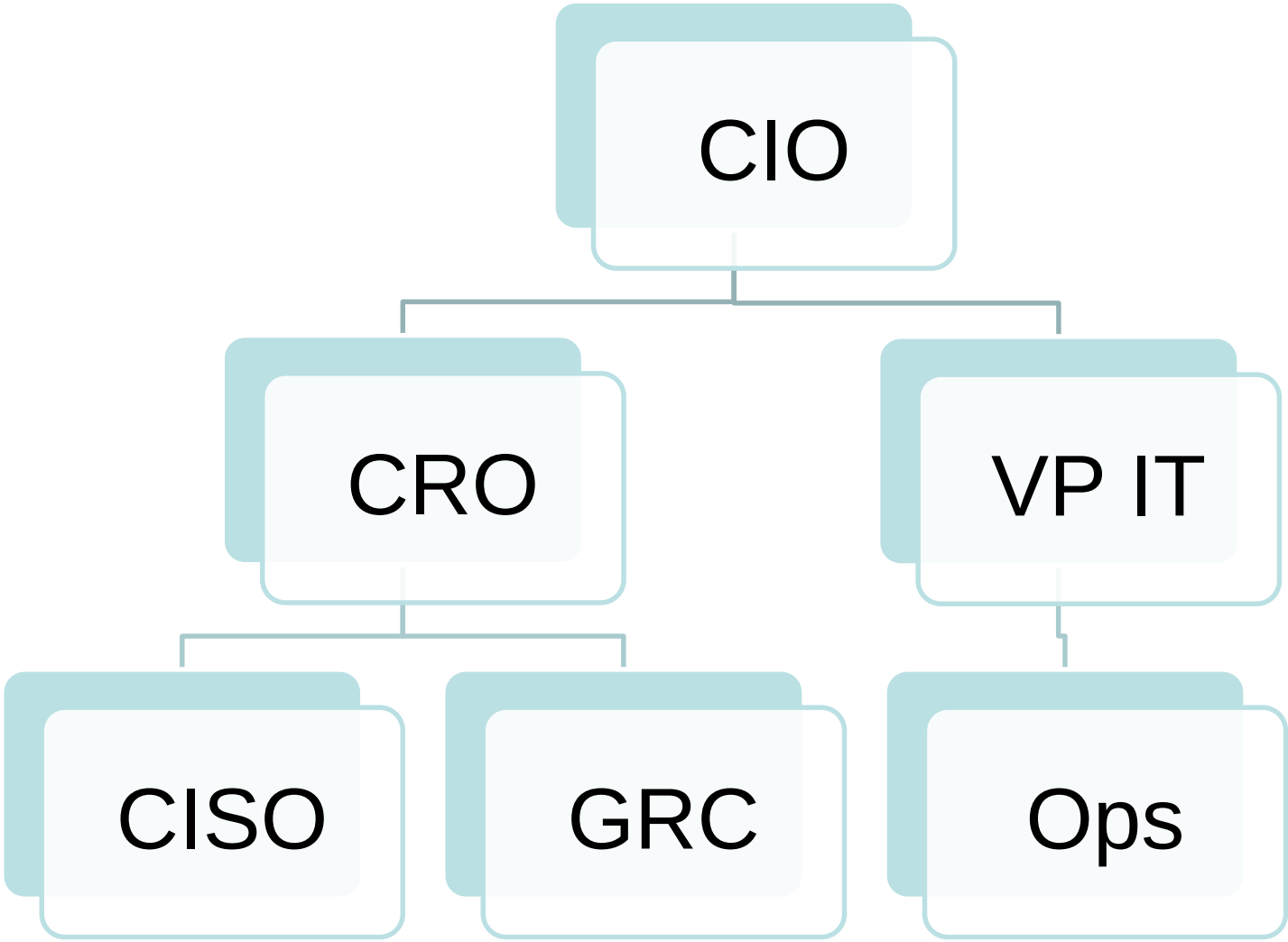
- Vulnerability cans
  - Data at rest/in-transit
  - Networks
  - Applications
- Data loss prevention
- Continuous monitoring
- Penetration testing
  - Internal/external
  - Social engineering
- Technology Review Committee
- Security code reviews
- Log analysis
  - Firewall
  - System
  - Database

Possible Reporting Structure



CISO
CORPORATE INFORMATION SECURITY OFFICE
CONFIDENTIALITY · INTEGRITY · AVAILABILITY

Better Reporting Structure



CISO
CORPORATE INFORMATION SECURITY OFFICE
CONFIDENTIALITY · INTEGRITY · AVAILABILITY

Ultimate Governance at USPS

- United States Postal Service Inspection Service – external crimes against business, fraud, etc.
- Office of Inspection General- internal activities, audits, etc.

Security

- Pros
  - Black and white issues
  - Solid tools to help
  - Deals with technology
- Cons
  - Not always business driven
  - Security is not compliance
  - Dynamic environment

Governance

- Pros:
  - Provides visibility
  - Provides control
  - Assigns accountability
  - Black and white

- Cons:
  - Potential of being Influenced
  - Not Security-focused
  - Compliance driven

The Future

Without controls, there is no governance and without security standards and policies, there are no controls.

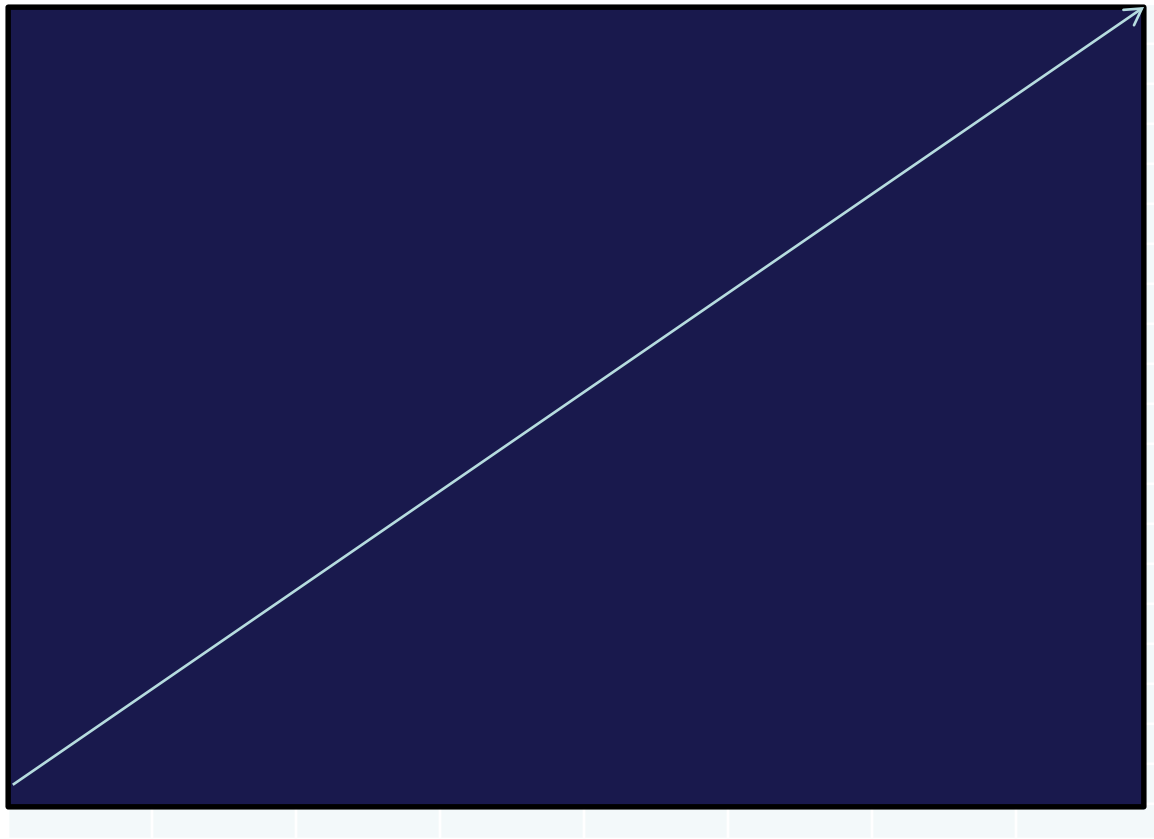
Without either, a company's ability to protect and make available the data needed to make business decisions is at risk.

The future requires both to insure viability.

CISO
CORPORATE INFORMATION SECURITY OFFICE
CONFIDENTIALITY · INTEGRITY · AVAILABILITY

The Linkage

Governance



Security Posture

Security Policy

CISO
CORPORATE INFORMATION SECURITY OFFICE
CONFIDENTIALITY · INTEGRITY · AVAILABILITY