Building a Resilient Risk Management Program: Strategies for Success

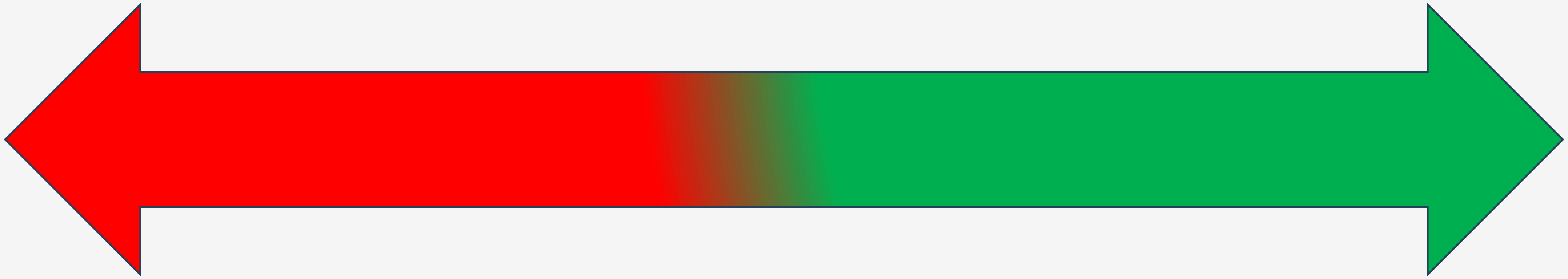
Nish Majmudar, CISO & Cybersecurity Risk Leader

Problems In Building A Good Cybersecurity Risk Program

- Lack of Executive Support and Alignment
  - Cyber risk is often seen as an IT issue, not a business issue.
  - Limited funding, misaligned priorities, and failure to integrate cyber risk into strategic decision-making.
- Poor Risk Visibility & Asset Inventory
  - Organizations often lack a complete and accurate inventory of assets
  - Inability to protect what isn't known; increased blind spots.
- Insufficient Metrics and Reporting
  - Inability to quantify risk or tie cyber risk to business impact.
  - Poor decision-making and lack of justification for investments.

Cyber-Risk Appetite

Goal is to build a sustainable cybersecurity program that balances the value of protection against the needs of running the business.



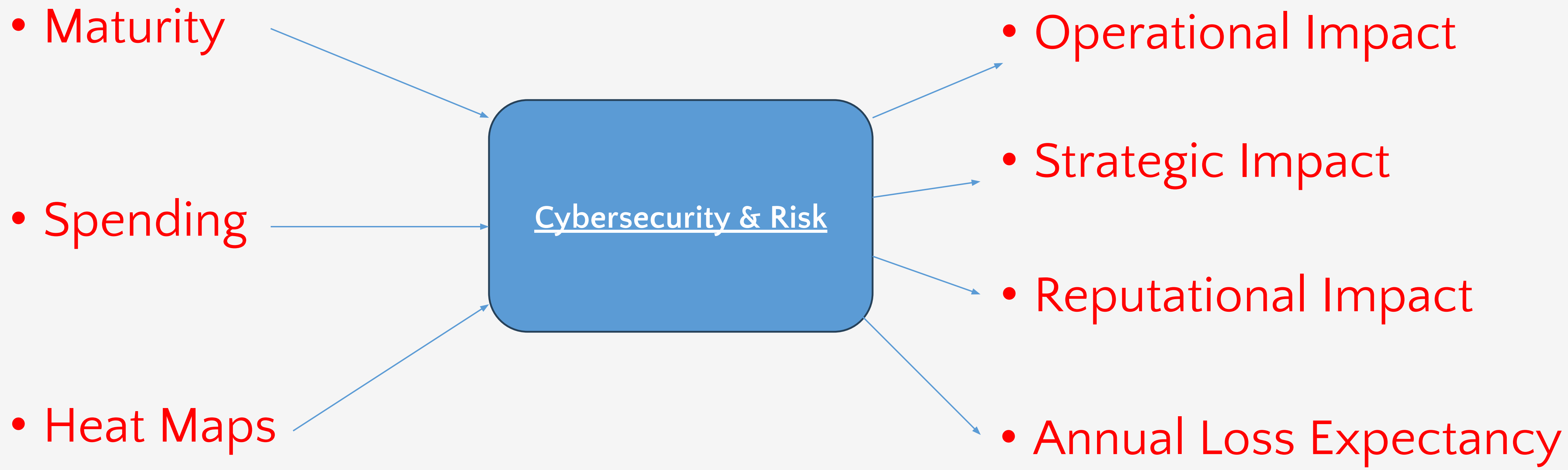
Lower Protection
Lower Defensibility

Higher Protection
Higher Defensibility

The Connections Are Missing

Traditional Cybersecurity Metrics

Risk-Appetite Statements



- Maturity
- Spending
- Heat Maps

Cybersecurity & Risk

- Operational Impact
- Strategic Impact
- Reputational Impact
- Annual Loss Expectancy

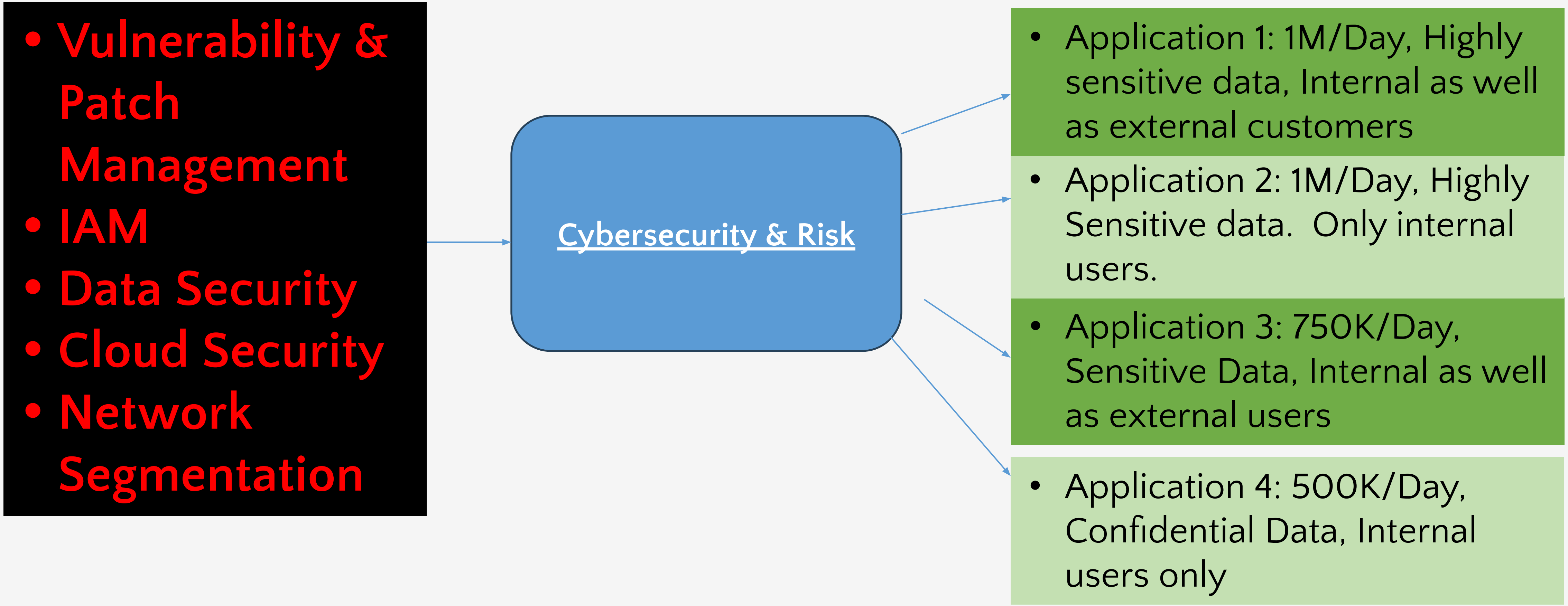
Maturity

- End-Point Protection
- Vulnerability & Patch Management
- IAM
- Data Security
- End-Point Protection
- Data Classification
- Third-party risk assessments
- Cloud Security
- Security Awareness
- Phishing Campaigns
- Incident containment and remediation time
- AI risk assessments

Applying Maturity To Applications

Maturity

Risk-Appetite Statements



- Vulnerability & Patch Management
- IAM
- Data Security
- Cloud Security
- Network Segmentation

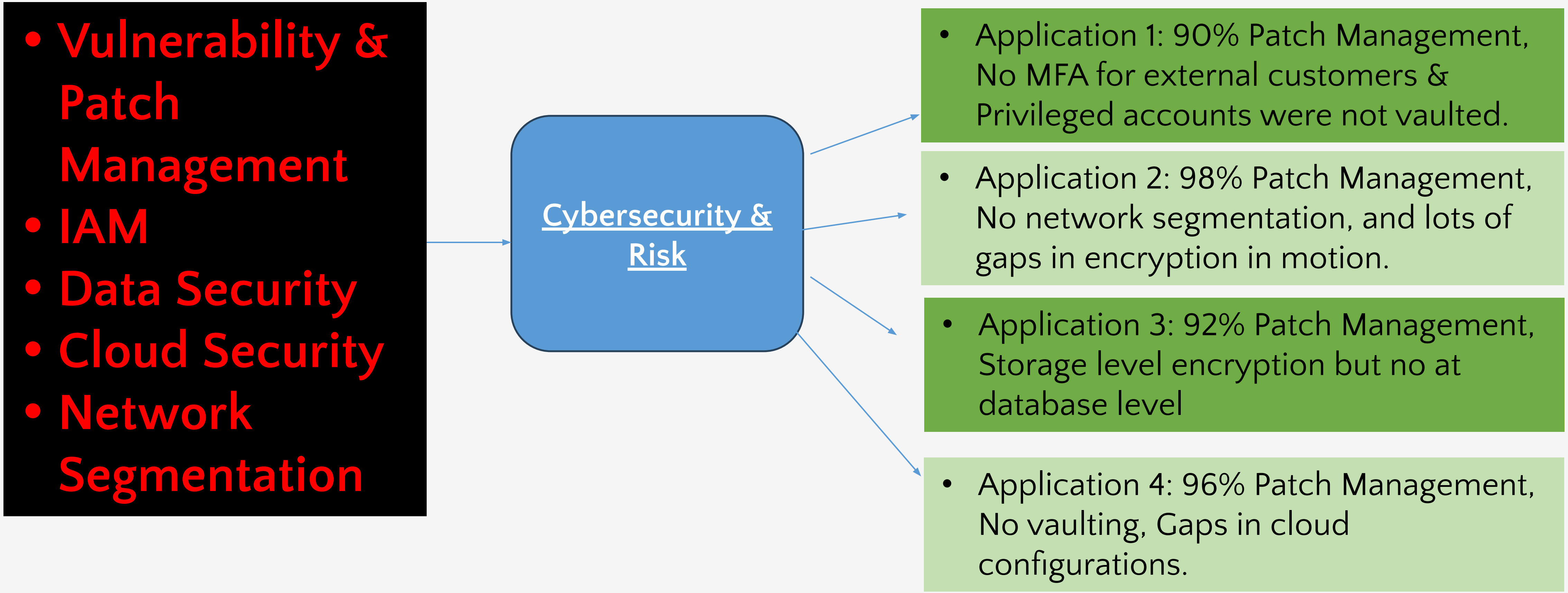
Cybersecurity & Risk

- Application 1: 1M/Day, Highly sensitive data, Internal as well as external customers
- Application 2: 1M/Day, Highly Sensitive data. Only internal users.
- Application 3: 750K/Day, Sensitive Data, Internal as well as external users
- Application 4: 500K/Day, Confidential Data, Internal users only

Applying Maturity To Applications

Maturity

Risk-Appetite Statements



- Vulnerability & Patch Management
- IAM
- Data Security
- Cloud Security
- Network Segmentation

Cybersecurity & Risk

- Application 1: 90% Patch Management, No MFA for external customers & Privileged accounts were not vaulted.
- Application 2: 98% Patch Management, No network segmentation, and lots of gaps in encryption in motion.
- Application 3: 92% Patch Management, Storage level encryption but no at database level
- Application 4: 96% Patch Management, No vaulting, Gaps in cloud configurations.

Mapping Threats To Applications

Maturity

- Vulnerability & Patch Management
- IAM
- Data Security
- Cloud Security
- Network Segmentation

Ransomware

DDOS

Data Breaches & Theft

Supply Chain Attacks

Risk-Appetite Statements

- Application 1: 90% Patch Management, No MFA for external customers & Privileged accounts were not vaulted.

- Application 2: 98% Patch Management, No network segmentation, and lots of gaps in encryption in motion.

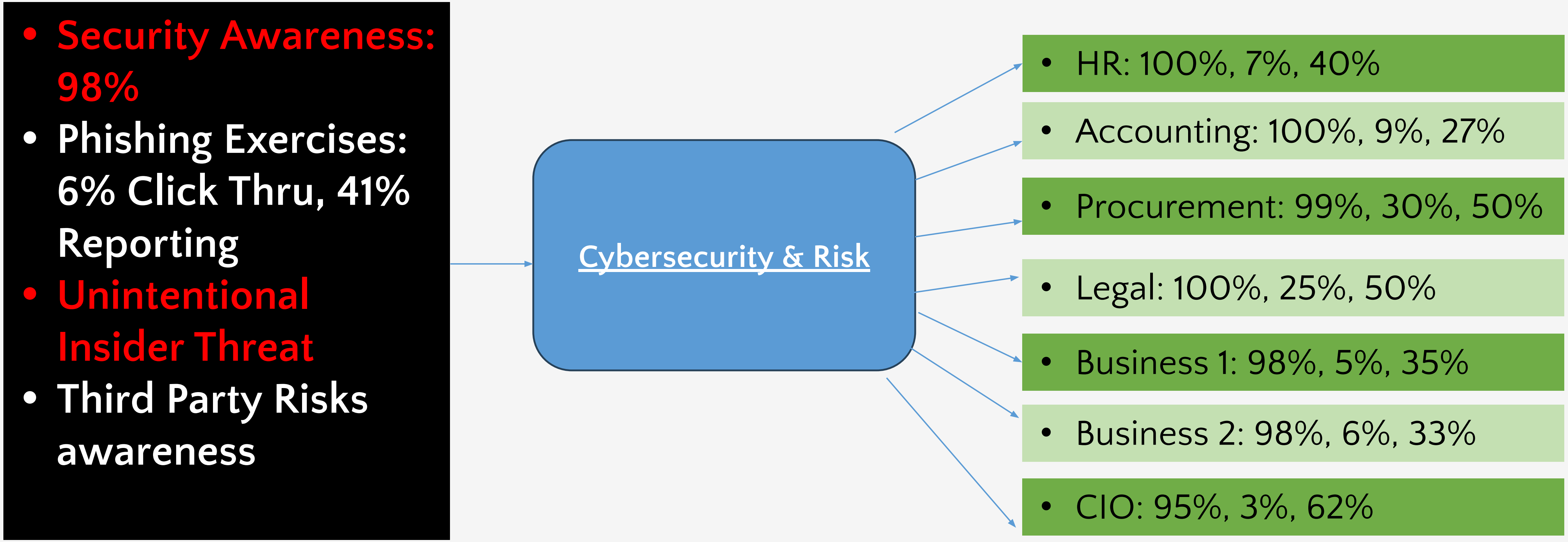
- Application 3: 92% Patch Management, Storage level encryption but no at database level

- Application 4: 96% Patch Management, No vaulting, Gaps in cloud configurations.

Security Awareness

Maturity

Departments Within Organization

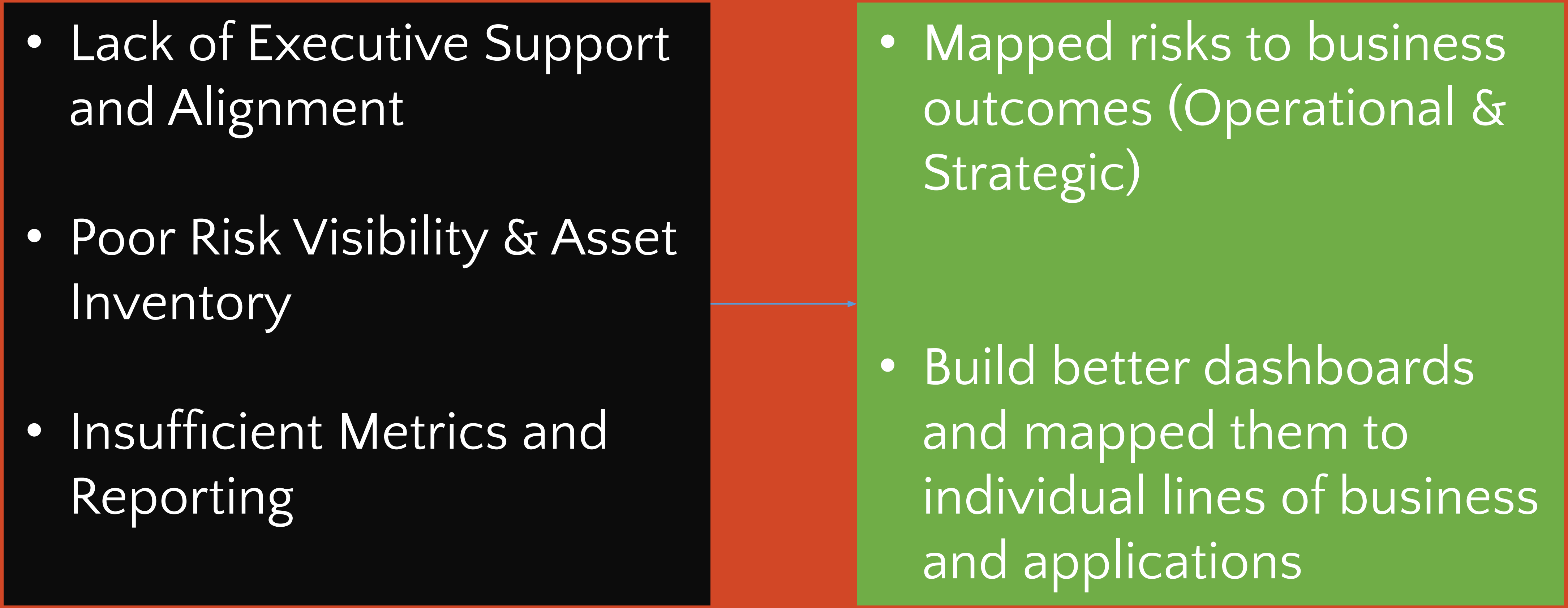


- Security Awareness: 98%
- Phishing Exercises: 6% Click Thru, 41% Reporting
- Unintentional Insider Threat
- Third Party Risks awareness

Cybersecurity & Risk

- HR: 100%, 7%, 40%
- Accounting: 100%, 9%, 27%
- Procurement: 99%, 30%, 50%
- Legal: 100%, 25%, 50%
- Business 1: 98%, 5%, 35%
- Business 2: 98%, 6%, 33%
- CIO: 95%, 3%, 62%

Conclusion



- Lack of Executive Support and Alignment
- Poor Risk Visibility & Asset Inventory
- Insufficient Metrics and Reporting

- Mapped risks to business outcomes (Operational & Strategic)
- Build better dashboards and mapped them to individual lines of business and applications

Questions & Thoughts

?