CYBERFORCE

Cybersecurity Risk Management

Presented by: Wayne Pierce and John Reilly

MASA | Michigan Association of Superintendents & Administrators

May 2, 2023

AGENDA

- Why is Cybersecurity Difficult?
- The Three Rs of Cybersecurity Risk Management
- Step 1: Determine Your Risk Level
- Step 2: Inventory Application Processes for Risk Alignment
- Step 3: Inject Cybersecurity Information into Operational Processes?
- What is The End Goal?
- Questions

WHO WE ARE

COLLECTIVE

Malicious actors are working together to find new ways to attack organizations. To combat these threats, we partner with our clients, sharing tactical information between entities, to break down silos and make everyone stronger.

CONTINUOUS

With cybercriminals adapting every day, cybersecurity programs need to continuously advance in order to combat threats. We focus on continuous improvement in everything we do to make our customers stronger.

EVIDENCE-BASED

We provide clients with proven results, using quantifiable measurement that demonstrates evidence-based proof of your cybersecurity progress, helping you advance your security posture.

CUSTOMIZED

We know every organization is unique, which is why our team works one-on-one with you, to determine the best solutions for your specific needs, taking into account your industry, goals, and organization's technologies and processes.

PARTNERSHIPS

Minnesota Hospital Association
Endorsed Business Partner

MHA
Michigan Health & Hospital Association

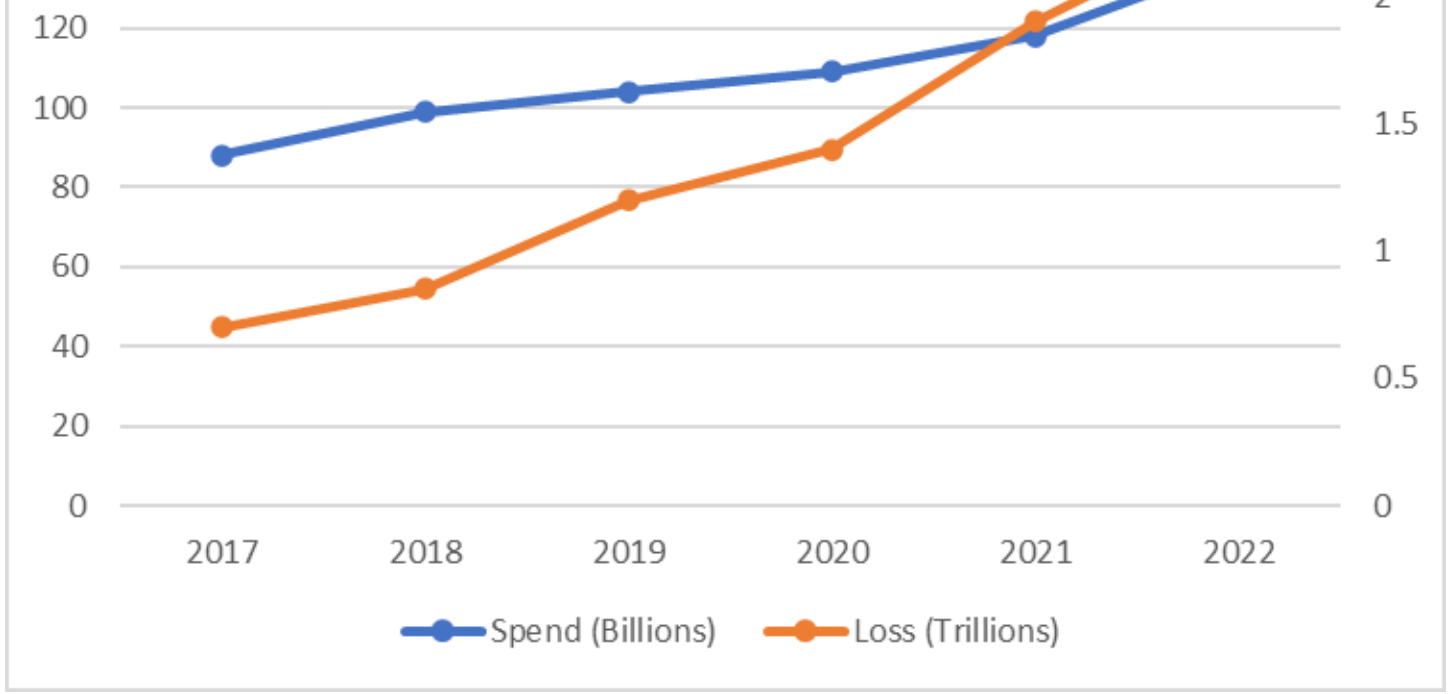
STATE OF MICHIGAN
MiDEAL
www.michigan.gov/mideal

Boards of Cooperative Educational Services
BOCES
of NEW YORK STATE

WSIPC
Inspired by education.
Empowered by technology.

MEDC
MICHIGAN ECONOMIC DEVELOPMENT CORPORATION

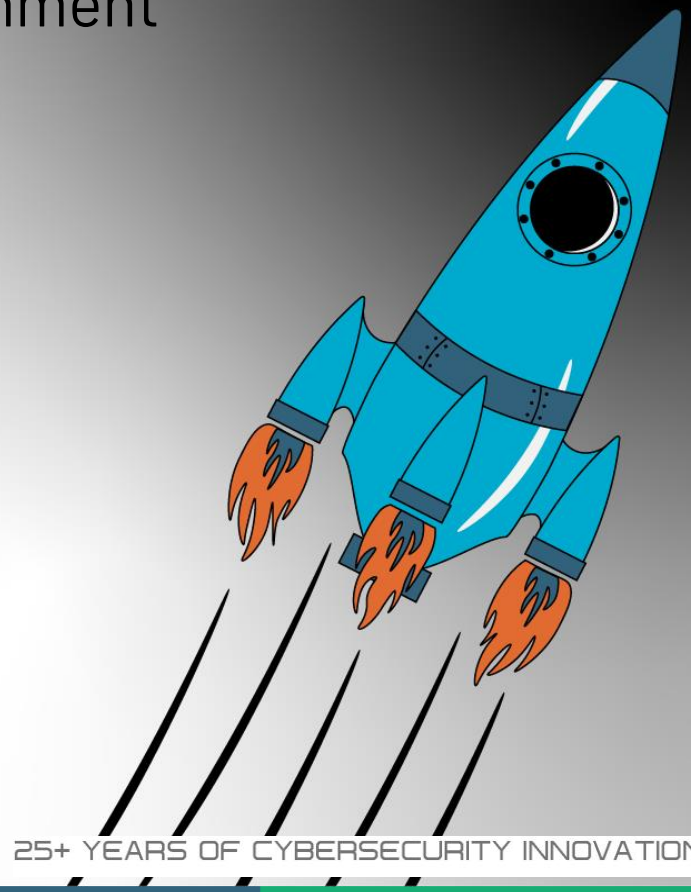
Why is Cybersecurity Difficult?



Source: Juniper Research

Complicated vs Complex Systems

- **Complicated**
  - Space Launch – 5 computer systems in closed environment
  - Structured data
- **Complex**
  - Interconnected applications
  - Open environment
  - Dynamic data
  - 3’rd party integration / Semantic integration
  - Globalization
  - Hosted regionally, on-prem, and Cloud



Organization Considerations

MITIGATING RISK

POLICY & PROCEDURE COMPLIANCE

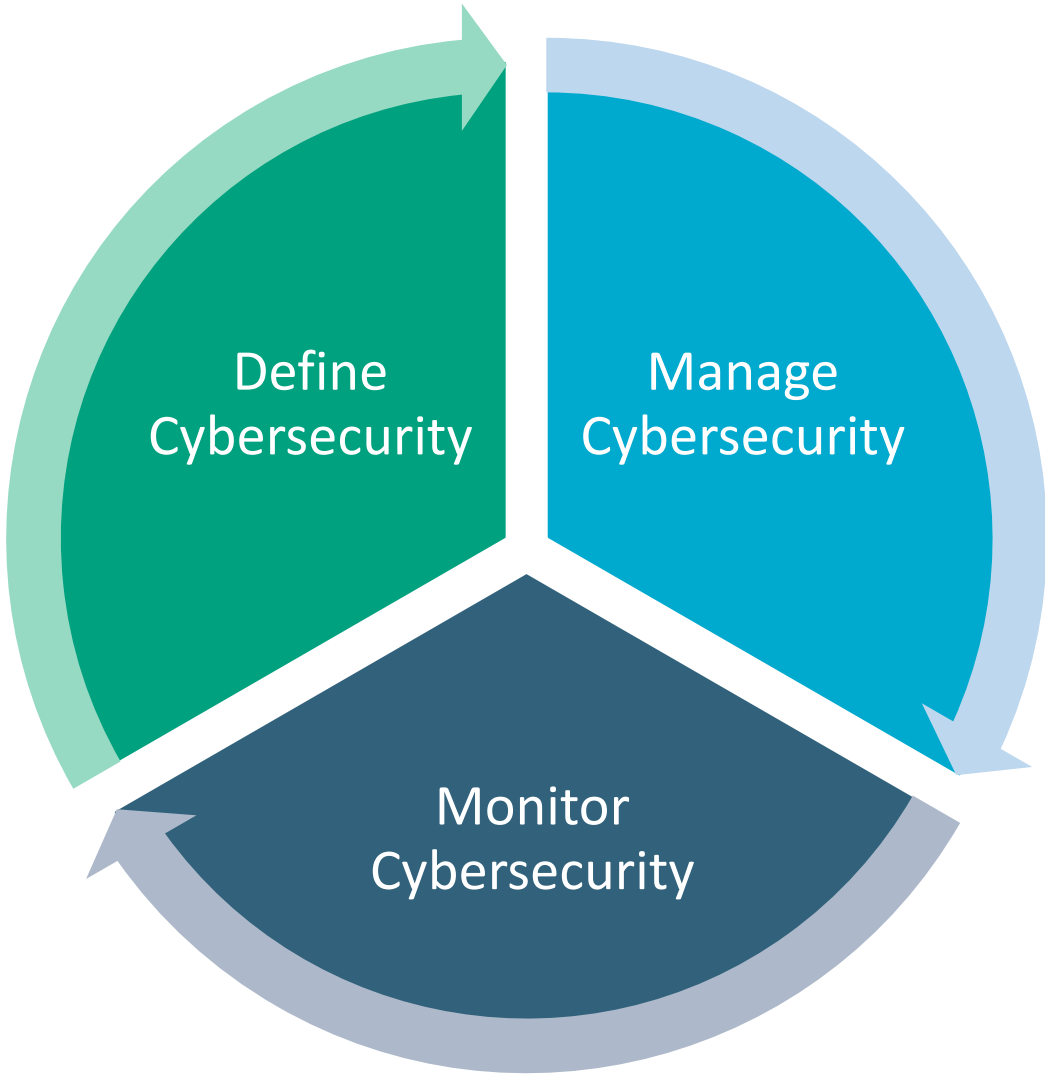
INSURANCE PREMIUMS

What is the business problem you are attempting to solve?

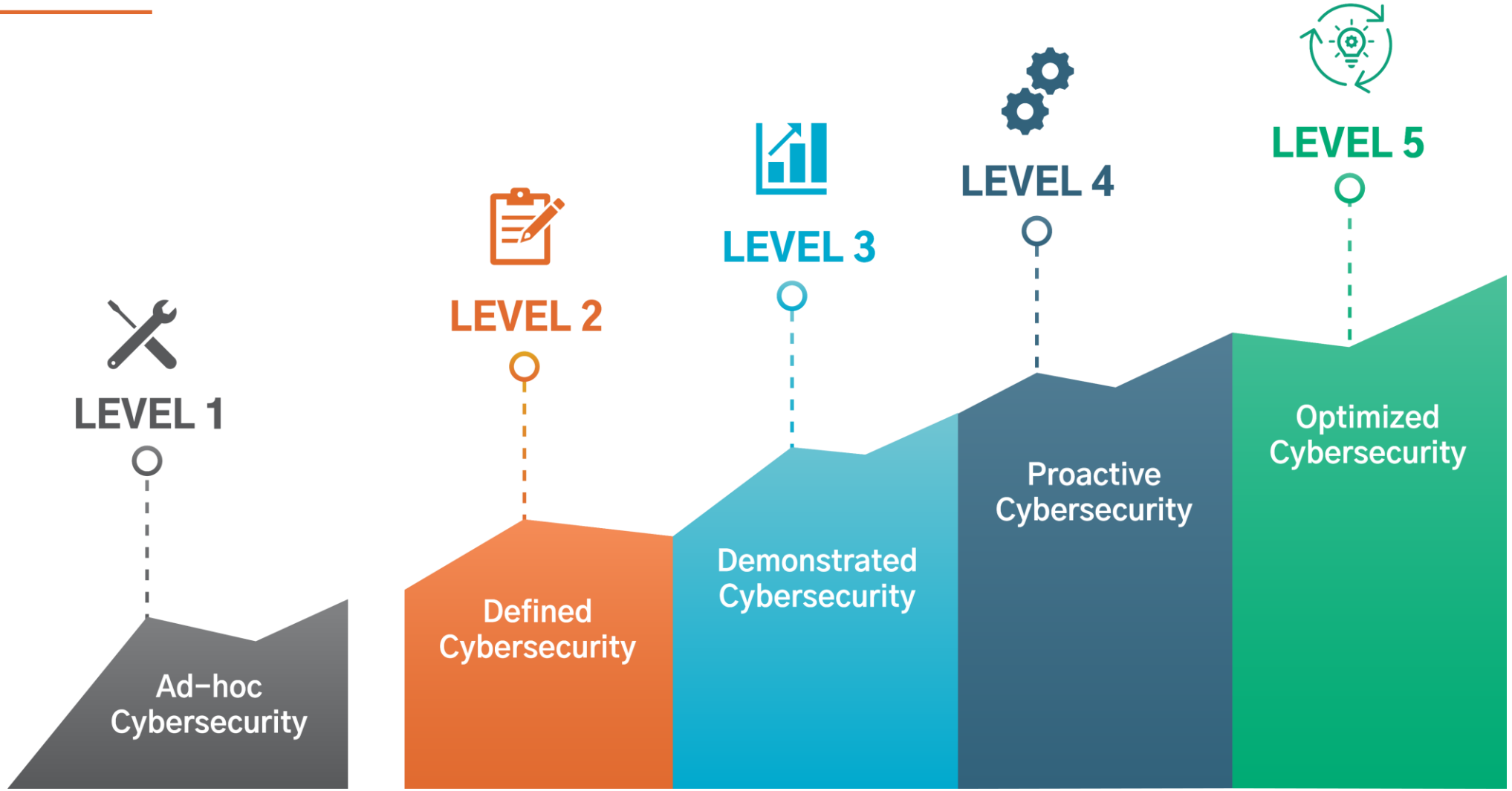
The Three R's Of Cybersecurity Risk Management

- **R**esiliency
- **R**edundancy
- **R**ecovery

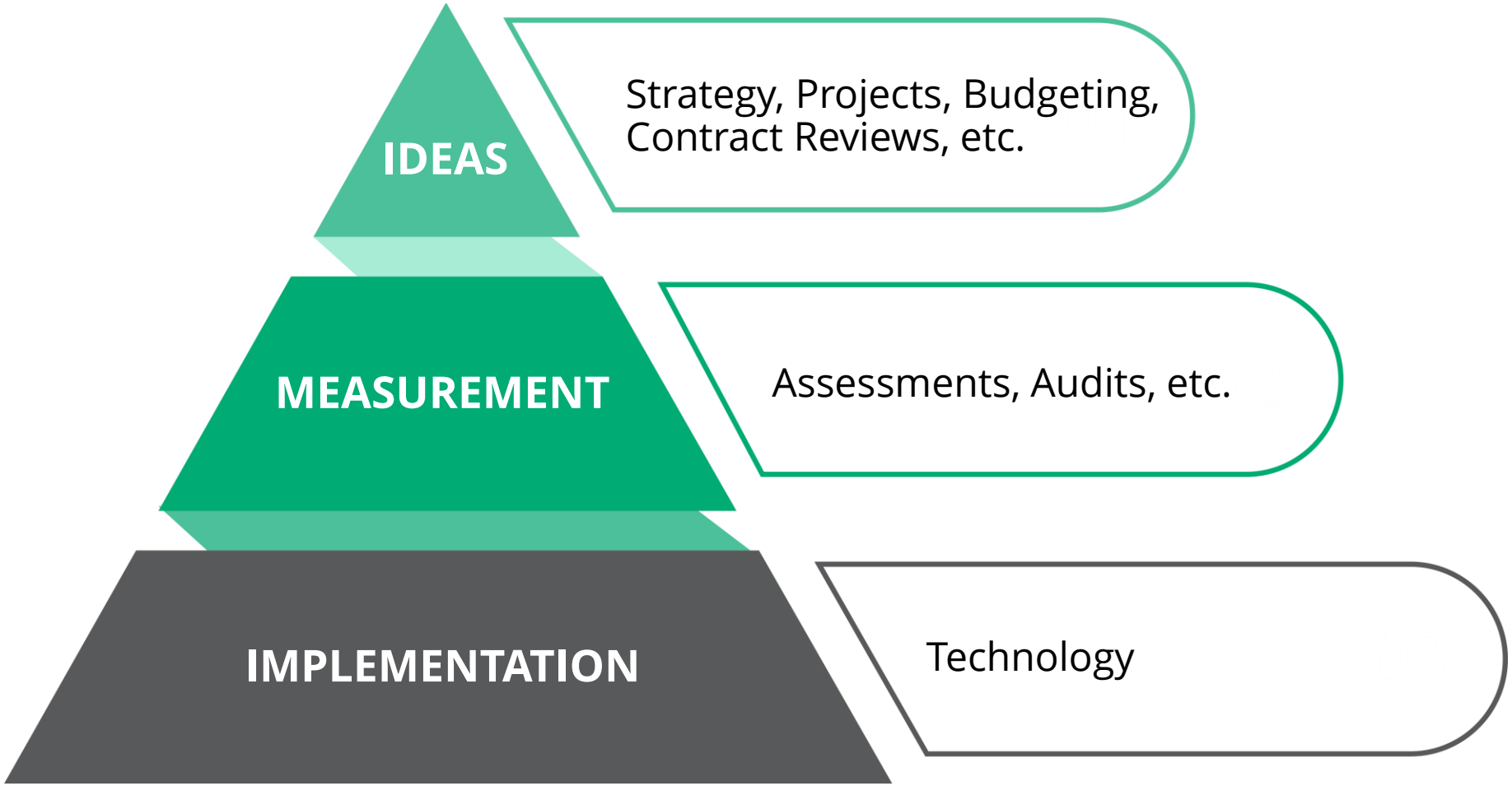
CYBERSECURITY LIFECYCLE



PROGRESSION TO OPTIMIZATION

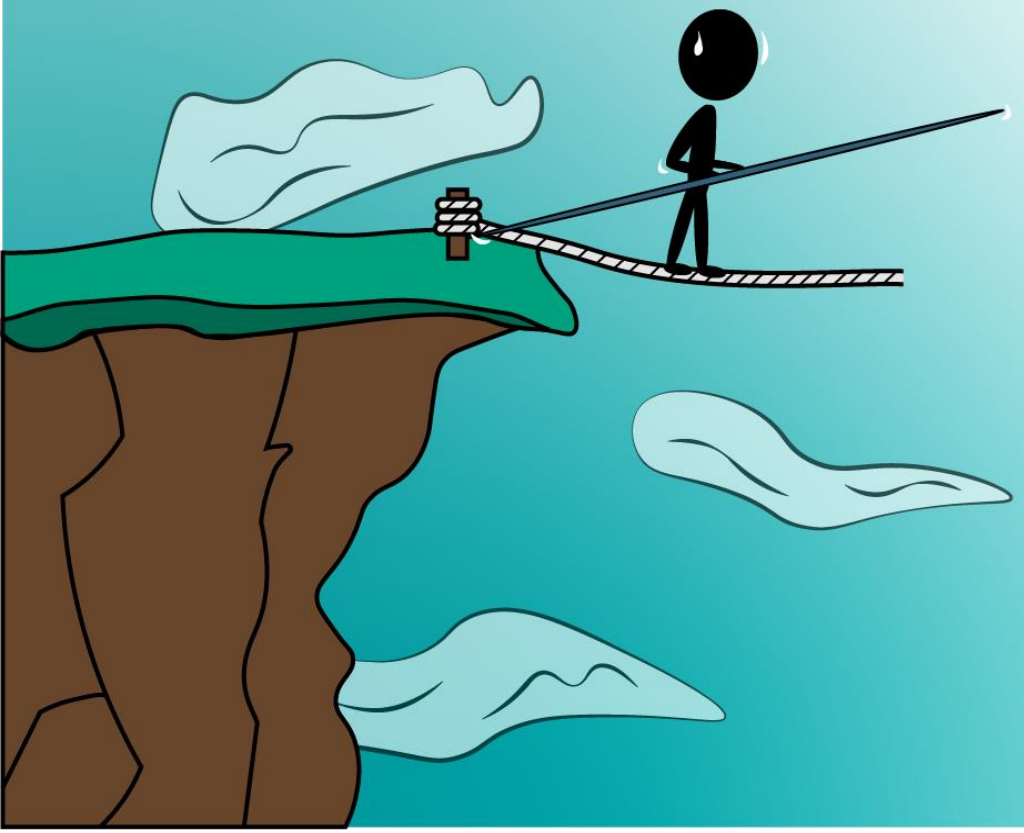


Breaking Down Operational Silos



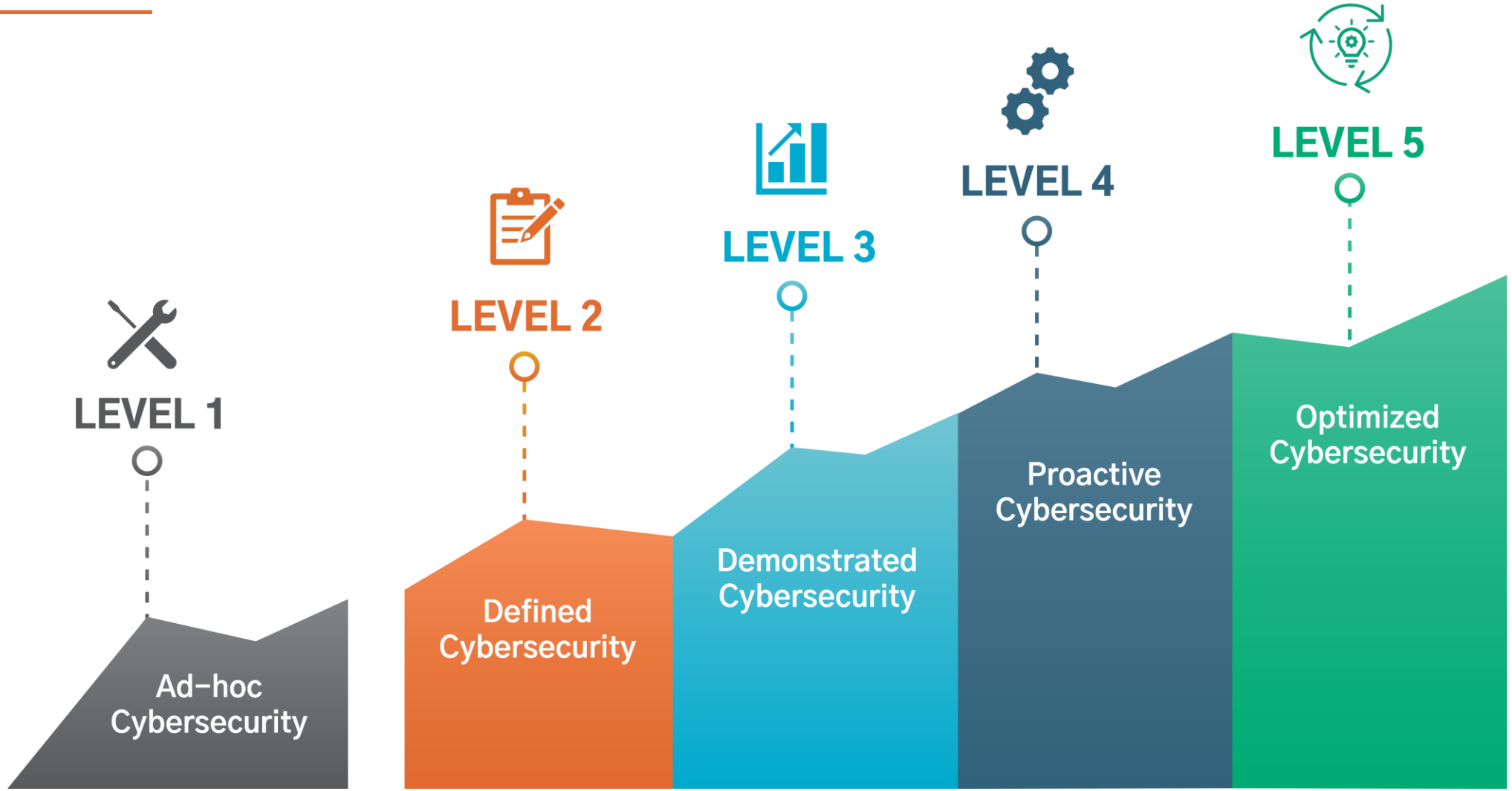
Step 1: Determine your risk tolerance

Risk Tolerance



- Variant system and user behavior
- Pure Risk vs. Speculative Risk
- “More things can happen than will happen” -Dimson
- Probability of threat vs. probability of significant loss

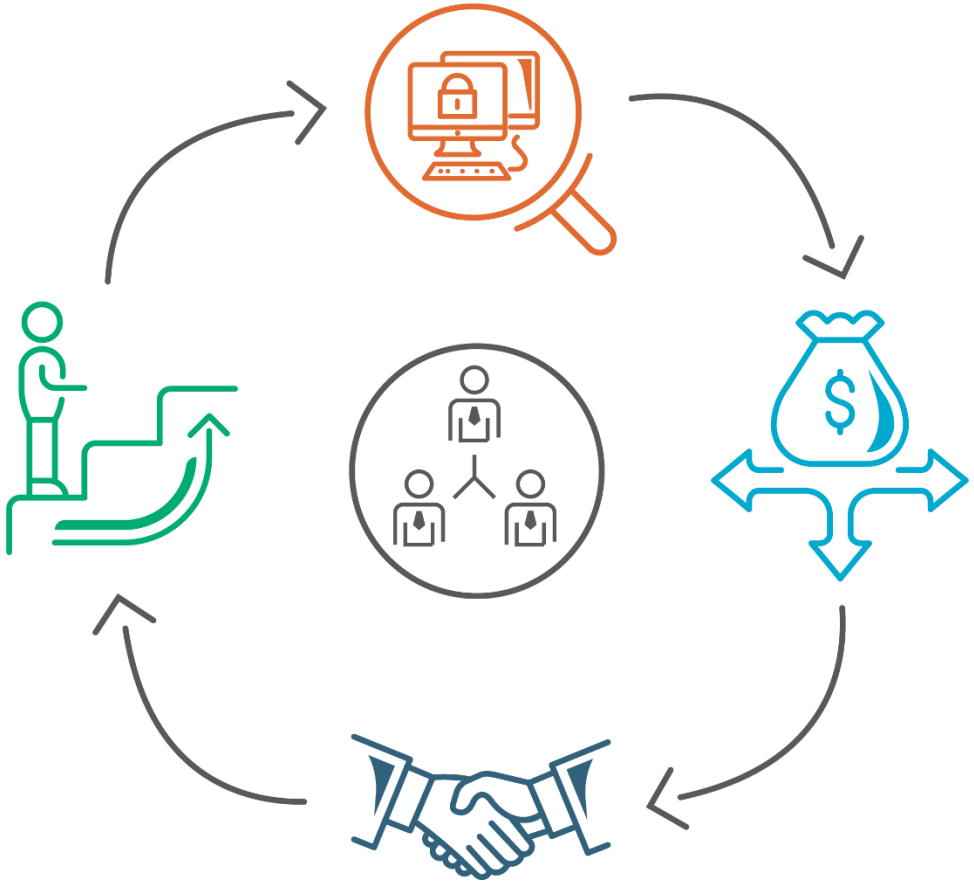
Cybersecurity Risk is Reduced by Maturity



Step 2: Inventory operational processes for risk alignment

Building Momentum & Reducing Friction

1. Evaluate and prioritize cybersecurity needs
2. Where should the next dollar of effort be spent
3. Align cybersecurity with operational processes
4. Each unit of work builds up to next unit work



Who Are Your Operational Allies?

- Contracting/Purchasing
  - Risk exceptions can be used during negotiating contract renewals
- PMO/IT
  - Incident response, downtime testing, validating documentation, and risk exceptions should be validated during upgrades and maintenance
- Finance
  - Signature Authority for risk exception approval and tracking financial risk commitment
- Business Leaders
  - Cybersecurity remediation may help move their initiatives forward

Step 3: Inject cybersecurity information into operational processes

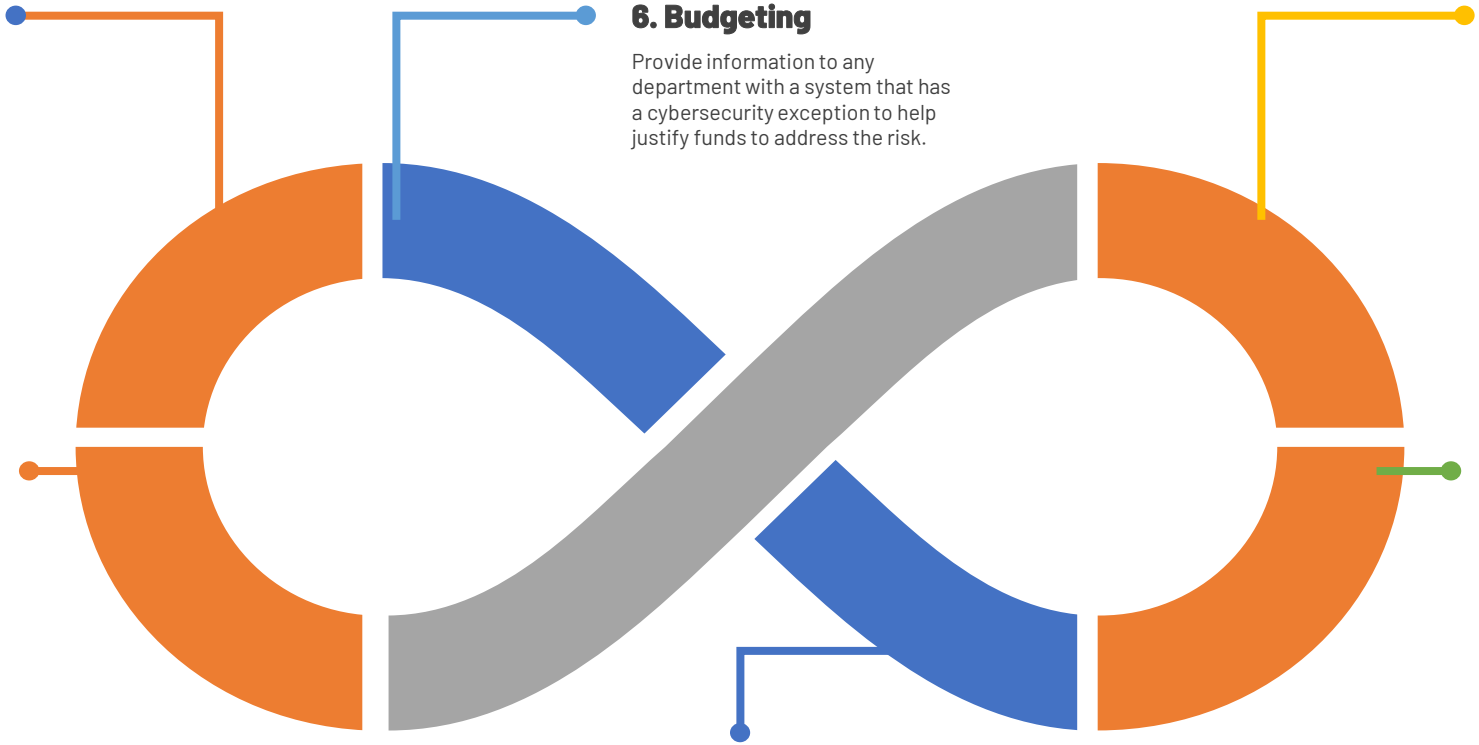
Cybersecurity Risk Lifecycle

1. Purchasing/Contract Renewal (Vendor Risk Assessment)

Cybersecurity data should be used to determine if the system meets requirements or to get commitment for addressing exceptions.

2. Scoping/Project Management

Validate that cybersecurity requirements will be met during implementation. Document any approved exceptions.



3. Implementation

Capture proof that cybersecurity requirements were met and save this as part of the audit record.

4. Maintenance/Upgrades

During upgrades require cybersecurity exceptions to be addressed, or a new exception requested. During maintenance and upgrades, validate information about the system is current to support incident response.

5. Strategic Planning

The major cybersecurity risks should be used to inform strategic requirements.

6. Budgeting

Provide information to any department with a system that has a cybersecurity exception to help justify funds to address the risk.

What Is The End Goal?

- A longitudinal audit record that is informed by key metrics
- A cross-referenced inventory of requirements
- Cybersecurity information influencing and informing operational processes
- Cybersecurity risk management must become an ongoing operational process to be effective.

Questions?