CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Randall Sandone, CCISO
Executive Director
Critical Infrastructure Resilience Institute
rsandone@Illinois.edu

Cyber Secure Dashboard
Cyber Insurance Portfolio Analysis of Risk (CIPAR)
Cyber insurance Legal Analytics Database (CLAD)

Market Needs

- *Target Customers: "Got cyber?"*
- *Market Needs:*
  - *Better assessment and management of risk (cyber)*

Cyber

Financial

Legal

Market Needs

- *Cyber Risk:*
  - *How do we achieve "all of organization" cyber security culture?*
  - *How do we leverage that culture to reduce our financial/legal risk?*
  - *How do we establish and maintain cyber security as a process?*
- *Financial Risk:*
  - *What is the financial risk of the most likely breach?*
  - *How likely is such a breach?*
  - *How much financial risk should we transfer (insurance)?*
- *Legal Risk:*
  - *What is our exposure to third-party liability claims?*
  - *Will my insurance cover my losses?*

Market Needs

- *Cyber Risk:*
  - *How do we achieve "all of organization" cyber security culture?*
  - *How do we leverage that culture to reduce our financial/legal risk?*
  - *How do we establish and maintain cyber security as a process?*
- *Financial Risk:*
  - *What is the financial risk of the most likely breach?*
  - *How likely is such a breach?*
  - *How much financial risk should we transfer (insurance)?*
- *Legal Risk:*
  - *What is our exposure to third-party liability claims?*
  - *Will my insurance cover my losses?*

Cyber Risk Solution:

- *Design, develop, deploy a toolset:*
  - *Operationalizes a sound, standardized cyber risk management process*
  - *Intuitive, affordable, accessible tools to help manage that process*
    - *Harmonization of activities*
    - *Centralization of information, references, artifacts*
    - *Unified communications framework for internal and external stakeholders*
  - *Supports multiple cybersecurity requirements and standards*
    - *DFARS/800-171*
    - *CSF Core*
    - *Manufacturing Profile*
    - *Other NIST Profiles*
    - *Other standards (ISO, HIPAA, etc.)*

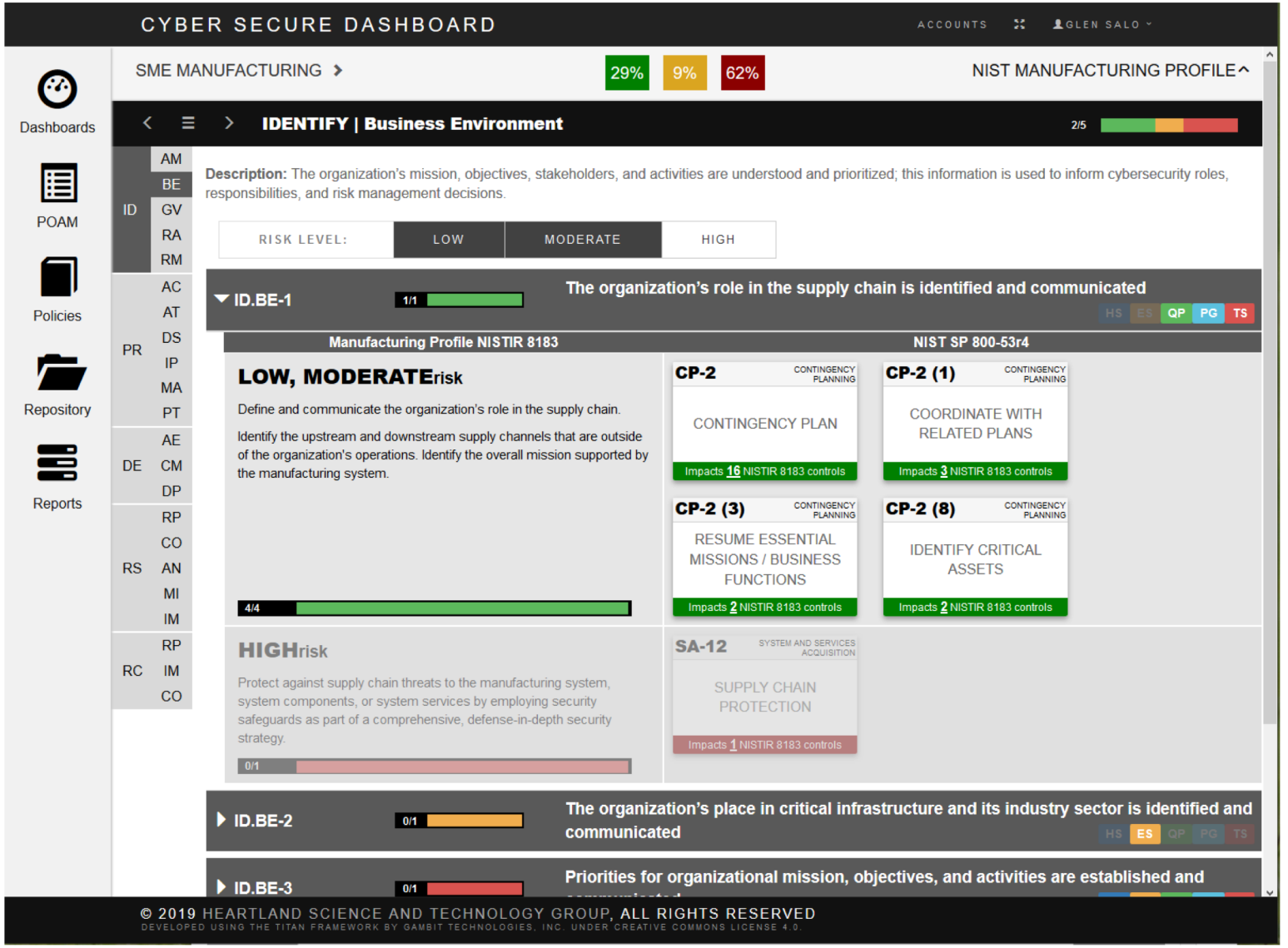
Approach – Cyber Secure Dashboard

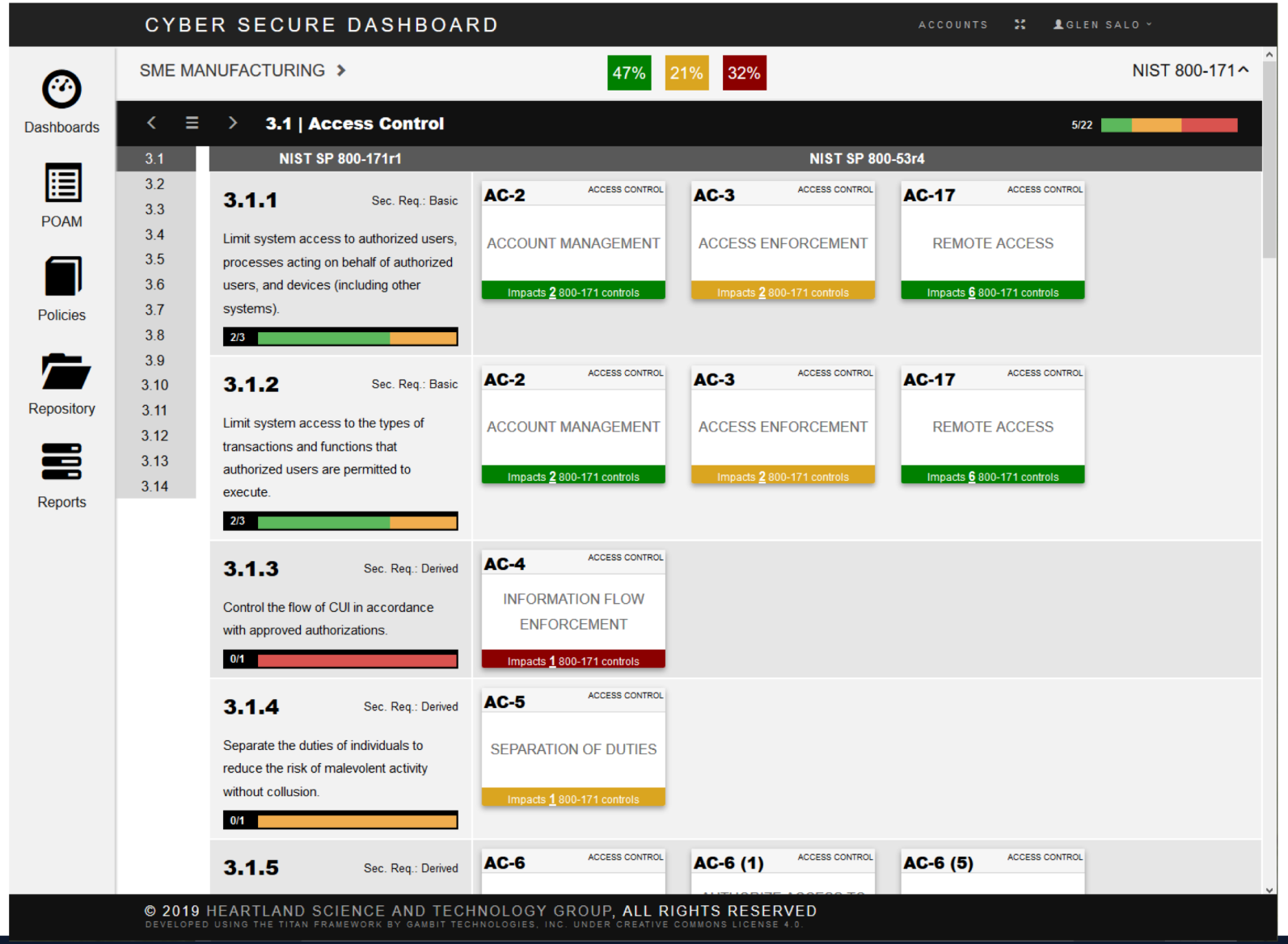
- *Collaborate to build and deploy a cloud-based SaaS**
- *"Learn-by-doing" design*
- *Address market need:*
  - *Facilitate implementation of a sound, standardized cyber risk management process*
  - *Intuitive, affordable, accessible tool to help manage that process*

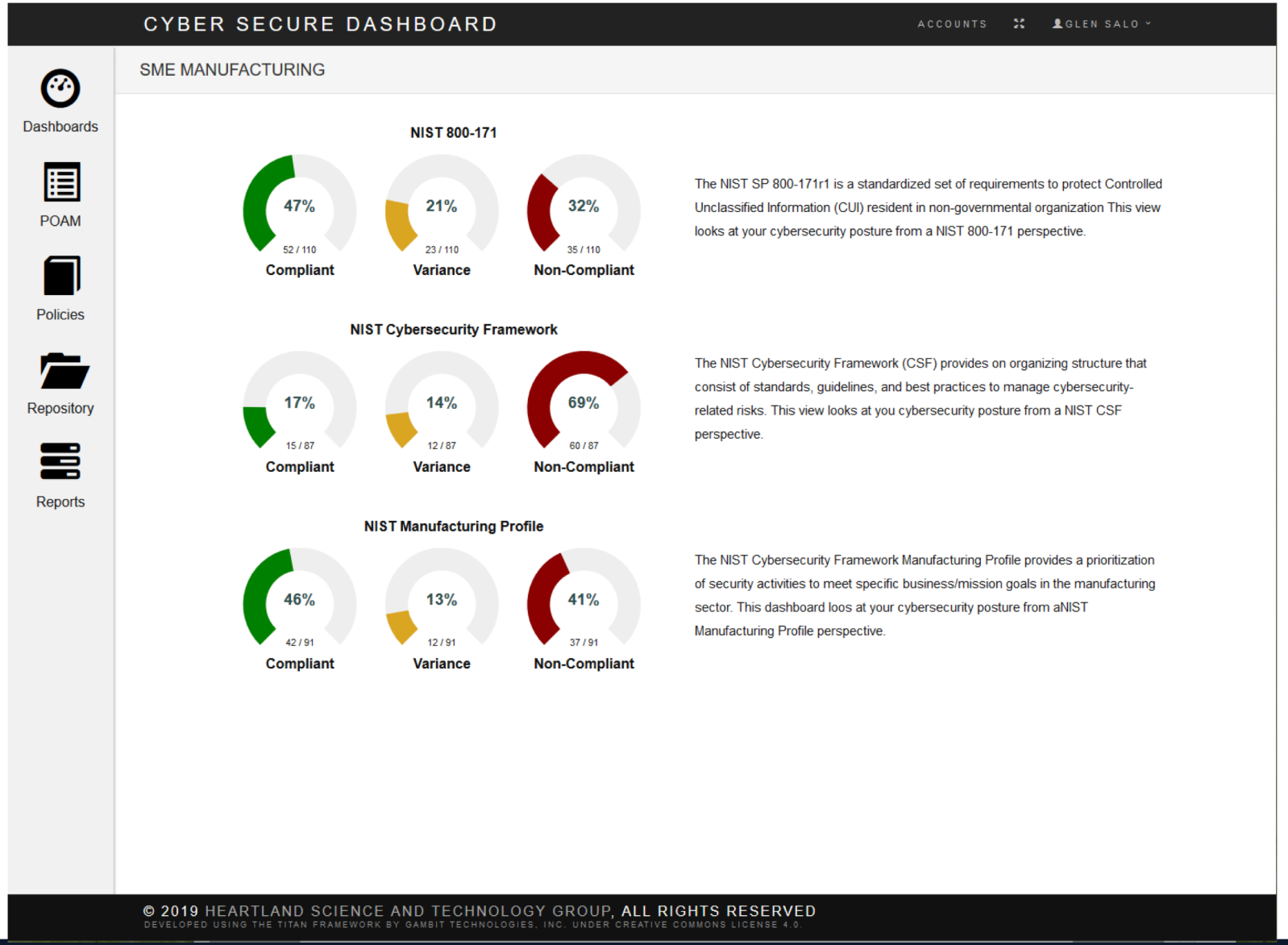
* Hosted at cybersecuredashboard.com and available for in-house deployment via Docker

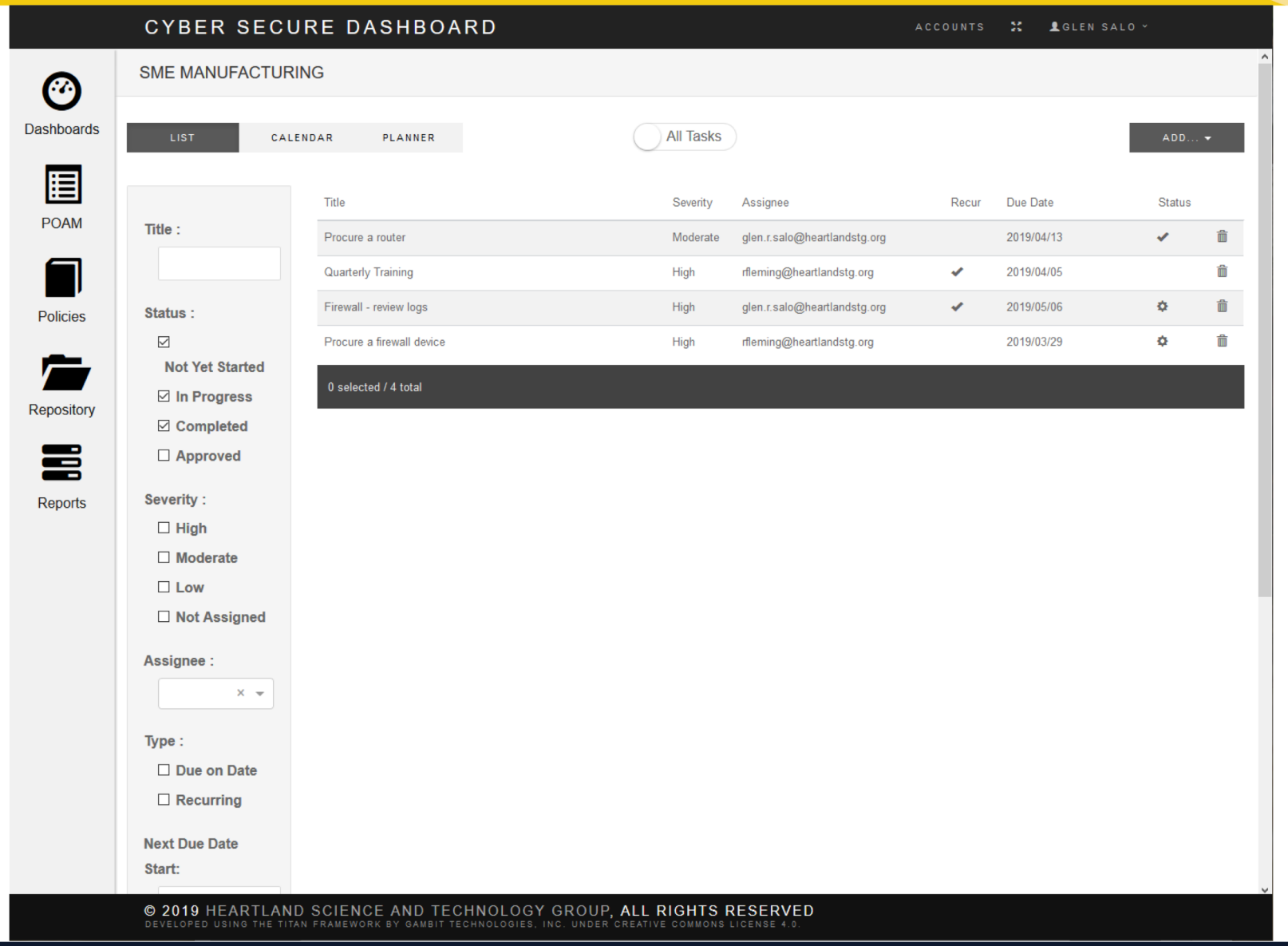
Key Features: Cyber Secure Dashboard

- *Operationalize Standards*
  - *Map requirements to controls*
- *Collaboration*
  - *Centralizes and harmonizes efforts for internal & external stakeholders (e.g., Supply Chain)*
  - *Provides centralized repository for all compliance artifacts*
  - *Provides access for easy third-party validation*
- *Resources*
  - *Best practices*
  - *Policy templates*
  - *Links to external resources (incl. educational tools), etc.*
- *Plan of Action and Milestones (POAM)*
  - *Scope and prioritize activities and investments in cyber security*
  - *Serves as foundation for long-term maintenance and improvement of cyber security culture*


CYBER SECURE DASHBOARD
ACCOUNTS
GLEN SALO
Dashboards
POAM
Policies
Repository
Reports
SME MANUFACTURING
29%
9%
62%
NIST MANUFACTURING PROFILE
IDENTIFY | Business Environment
2/5
ID AM BE GV RA RM
PR AC AT DS IP MA PT
DE AE CM DP
RS RP CO AN MI IM
RC RP IM CO
Description: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
RISK LEVEL: LOW MODERATE HIGH
ID.BE-1
1/1
The organization's role in the supply chain is identified and communicated
HS ES QP PG TS
Manufacturing Profile NISTIR 8183
NIST SP 800-53r4
LOW, MODERATE risk
Define and communicate the organization's role in the supply chain.
Identify the upstream and downstream supply channels that are outside of the organization's operations. Identify the overall mission supported by the manufacturing system.
4/4
CP-2 CONTINGENCY PLANNING
CONTINGENCY PLAN
Impacts 16 NISTIR 8183 controls
CP-2 (1) CONTINGENCY PLANNING
COORDINATE WITH RELATED PLANS
Impacts 3 NISTIR 8183 controls
CP-2 (3) CONTINGENCY PLANNING
RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS
Impacts 2 NISTIR 8183 controls
CP-2 (8) CONTINGENCY PLANNING
IDENTIFY CRITICAL ASSETS
Impacts 2 NISTIR 8183 controls
HIGH risk
Protect against supply chain threats to the manufacturing system, system components, or system services by employing security safeguards as part of a comprehensive, defense-in-depth security strategy.
0/1
SA-12 SYSTEM AND SERVICES ACQUISITION
SUPPLY CHAIN PROTECTION
Impacts 1 NISTIR 8183 controls
ID.BE-2
0/1
The organization's place in critical infrastructure and its industry sector is identified and communicated
HS ES QP PG TS
ID.BE-3
0/1
Priorities for organizational mission, objectives, and activities are established and
© 2019 HEARTLAND SCIENCE AND TECHNOLOGY GROUP, ALL RIGHTS RESERVED
DEVELOPED USING THE TITAN FRAMEWORK BY GAMBIT TECHNOLOGIES, INC. UNDER CREATIVE COMMONS LICENSE 4.0.


CYBER SECURE DASHBOARD
ACCOUNTS
GLEN SALO
Dashboards
POAM
Policies
Repository
Reports
SME MANUFACTURING
47%
21%
32%
NIST 800-171
3.1 | Access Control
5/22
3.1
3.2
3.3
3.4
3.5
3.6
3.7
3.8
3.9
3.10
3.11
3.12
3.13
3.14
NIST SP 800-171r1
NIST SP 800-53r4
3.1.1
Sec. Req.: Basic
Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
2/3
AC-2
ACCESS CONTROL
ACCOUNT MANAGEMENT
Impacts 2 800-171 controls
AC-3
ACCESS CONTROL
ACCESS ENFORCEMENT
Impacts 2 800-171 controls
AC-17
ACCESS CONTROL
REMOTE ACCESS
Impacts 6 800-171 controls
3.1.2
Sec. Req.: Basic
Limit system access to the types of transactions and functions that authorized users are permitted to execute.
2/3
AC-2
ACCESS CONTROL
ACCOUNT MANAGEMENT
Impacts 2 800-171 controls
AC-3
ACCESS CONTROL
ACCESS ENFORCEMENT
Impacts 2 800-171 controls
AC-17
ACCESS CONTROL
REMOTE ACCESS
Impacts 6 800-171 controls
3.1.3
Sec. Req.: Derived
Control the flow of CUI in accordance with approved authorizations.
0/1
AC-4
ACCESS CONTROL
INFORMATION FLOW ENFORCEMENT
Impacts 1 800-171 controls
3.1.4
Sec. Req.: Derived
Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
0/1
AC-5
ACCESS CONTROL
SEPARATION OF DUTIES
Impacts 1 800-171 controls
3.1.5
Sec. Req.: Derived
AC-6
ACCESS CONTROL
AC-6 (1)
ACCESS CONTROL
AC-6 (5)
ACCESS CONTROL
© 2019 HEARTLAND SCIENCE AND TECHNOLOGY GROUP, ALL RIGHTS RESERVED
DEVELOPED USING THE TITAN FRAMEWORK BY GAMBIT TECHNOLOGIES, INC. UNDER CREATIVE COMMONS LICENSE 4.0.


CYBER SECURE DASHBOARD
ACCOUNTS
GLEN SALO
Dashboards
POAM
Policies
Repository
Reports
SME MANUFACTURING
NIST 800-171
47%
52 / 110
Compliant
21%
23 / 110
Variance
32%
35 / 110
Non-Compliant
The NIST SP 800-171r1 is a standardized set of requirements to protect Controlled Unclassified Information (CUI) resident in non-governmental organization This view looks at your cybersecurity posture from a NIST 800-171 perspective.
NIST Cybersecurity Framework
17%
15 / 87
Compliant
14%
12 / 87
Variance
69%
60 / 87
Non-Compliant
The NIST Cybersecurity Framework (CSF) provides on organizing structure that consist of standards, guidelines, and best practices to manage cybersecurity-related risks. This view looks at you cybersecurity posture from a NIST CSF perspective.
NIST Manufacturing Profile
46%
42 / 91
Compliant
13%
12 / 91
Variance
41%
37 / 91
Non-Compliant
The NIST Cybersecurity Framework Manufacturing Profile provides a prioritization of security activities to meet specific business/mission goals in the manufacturing sector. This dashboard loos at your cybersecurity posture from aNIST Manufacturing Profile perspective.
© 2019 HEARTLAND SCIENCE AND TECHNOLOGY GROUP, ALL RIGHTS RESERVED
DEVELOPED USING THE TITAN FRAMEWORK BY GAMBIT TECHNOLOGIES, INC. UNDER CREATIVE COMMONS LICENSE 4.0.


CYBER SECURE DASHBOARD
ACCOUNTS
GLEN SALO
Dashboards
POAM
Policies
Repository
Reports
SME MANUFACTURING
LIST
CALENDAR
PLANNER
All Tasks
ADD...
Title :
Status :
Not Yet Started
In Progress
Completed
Approved
Severity :
High
Moderate
Low
Not Assigned
Assignee :
Type :
Due on Date
Recurring
Next Due Date
Start:
Title
Severity
Assignee
Recur
Due Date
Status
Procure a router
Moderate
glen.r.salo@heartlandstg.org
2019/04/13
Quarterly Training
High
rfleming@heartlandstg.org
2019/04/05
Firewall - review logs
High
glen.r.salo@heartlandstg.org
2019/05/06
Procure a firewall device
High
rfleming@heartlandstg.org
2019/03/29
0 selected / 4 total
© 2019 HEARTLAND SCIENCE AND TECHNOLOGY GROUP, ALL RIGHTS RESERVED
DEVELOPED USING THE TITAN FRAMEWORK BY GAMBIT TECHNOLOGIES, INC. UNDER CREATIVE COMMONS LICENSE 4.0.

Benefits

- *Competitive/alternative approaches:*
  - *Status quo: ad hoc and reactive approach to cyber risk management*
  - *Spreadsheet-based checklists*
  - *Outsource to cybersecurity services provider*
- *Dashboard differentiators:*
  - *Holistic, all-in-one platform: assessment, implementation, training, project management*
  - *Facilitates communication and fosters common understanding*
  - *Facilitates growth of fluency, cyber maturity, "all of company" approach*

Transition Activities:

- *Business consulting engagement – Illinois Business Consulting*
- *Additional technical enhancements*
- *Identification of industry partners*
- *Implement novel sales & distribution models*

Access at https://cybersecuredashboard.com

Market Needs

- *Cyber Risk:*
  - *How do we achieve "all of organization" cyber security culture?*
  - *How do we leverage that culture to reduce our financial/legal risk?*
  - *How do we establish and maintain cyber security as a process?*
- *Financial Risk:*
  - *What is the financial risk of the most likely breach?*
  - *How likely is such a breach?*
  - *How much financial risk should we transfer (insurance)?*
- *Legal Risk:*
  - *What is our exposure to third-party liability claims?*
  - *Will my insurance cover my losses?*

Financial Risk Solution:

- *Target Customers: businesses; insurance companies*
- *SaaS that helps firms identify financial risks and predict future risks based on empirical and event analysis of:*
  - *Historical and real-time cyber incident databases*
  - *Historical and real-time financial and capital losses*

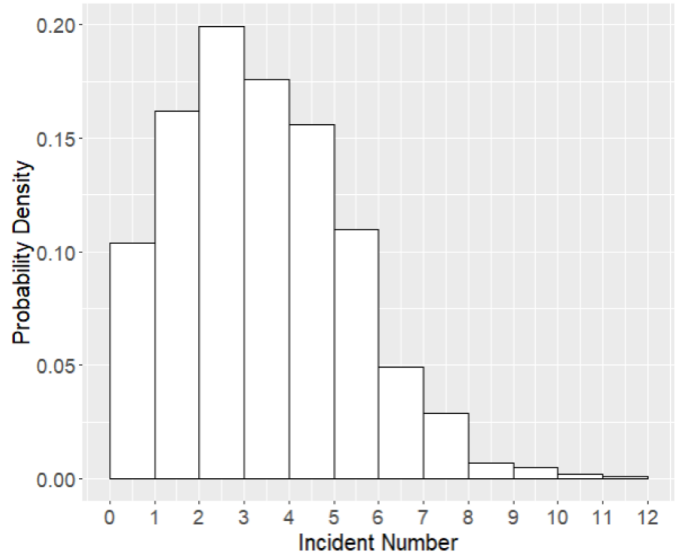
Approach - CIPAR

- *Use cyber incident data + predictive models to perform cyber risk assessment; forecast future cyber risk based on information provided by the user.*
  - *Identifying major trends in cyber risk helps prioritize risk management tasks*
  - *Estimating the frequency and severity of cyber incidents provides insights*
  - *Better management of insurance portfolios*
  - *Access CIPAR at* – https://ciri-cyber.shinyapps.io/web_app

Estimating Cyber Loss

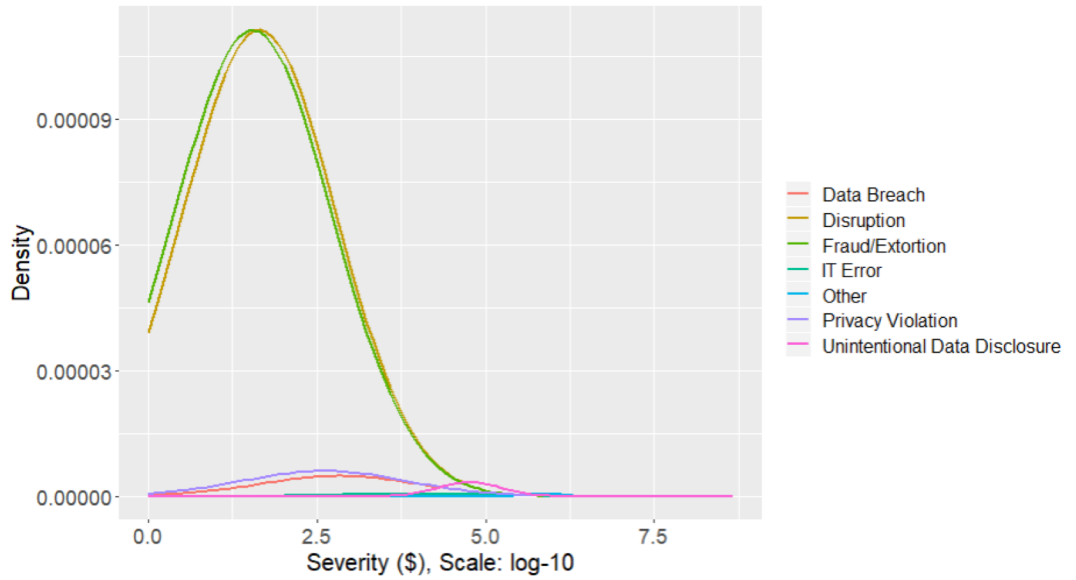
- CIPAR provides risk assessment information in detail for sophisticated users.
- For example, the figure on the left shows the distribution of incident frequency and the probability corresponding to each number of incidents. The probability of no incident is 0.104, the probability of one incident is 0.162 …
- The figure on the right shows the distributions of losses resulting from various types of incidents.

Incident Number Distribution



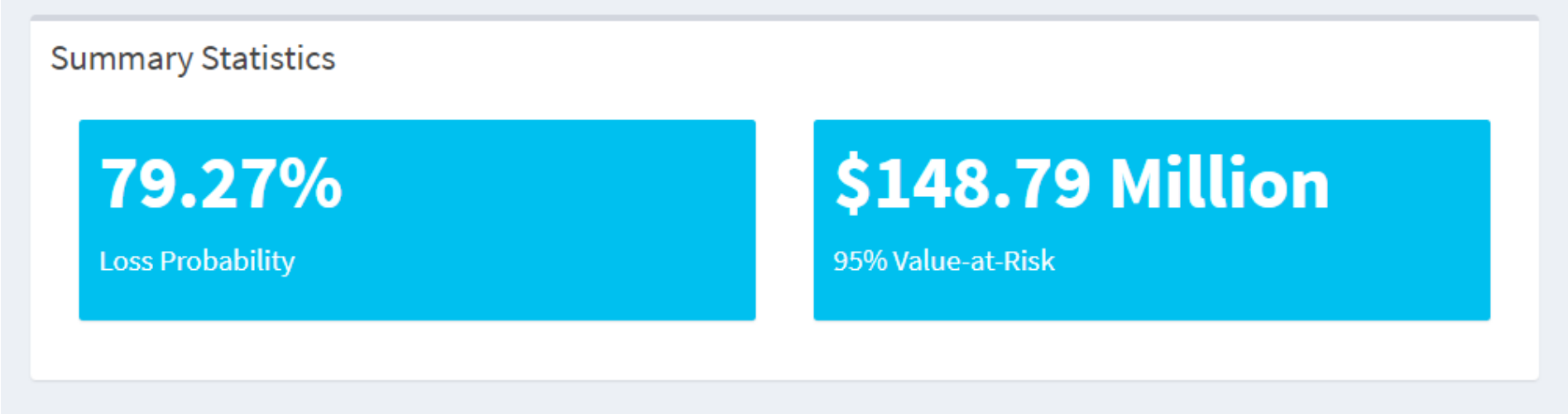
Incident Number	Probability
0	0.1040
1	0.1620
2	0.1990
3	0.1760
4	0.1560
5	0.1100
6	0.0490
7	0.0290
8	0.0070
9	0.0050
10	0.0020
11	0.0010

Severity of Loss



Estimating Cyber Loss (Cont'd)

- CIPAR forecasts the incident frequency and severity in a future year, say 2019, and provides intuitive summary statistics.
- *E.g.,* CIPAR provides an estimation that in 2019, a large financial institution has a 79.27% probability of suffering a loss from cyber incidents, and there is a 5% probability that the loss will exceed $148.79 million.



Distinguishing Risks

- CIPAR makes it easier for insurers to compare the cyber risk of different companies.

A large financial institution with more than 500 employees	**79.27%** Loss Probability	**$148.79 Million** 95% Value-at-Risk
A small financial institution with fewer than 10 employees	**1.32%** Loss Probability	**$0.09 Million** 95% Value-at-Risk

Transition Activities:

- *Further data collection to refine use cases*
  - *Live updates*
  - *Optimize policy design*
  - *Insurance policy recommendation engine*
- *Engagement with potential business partners*

Market Needs

- *Cyber Risk:*
  - *How do we achieve "all of organization" cyber security culture?*
  - *How do we leverage that culture to reduce our financial/legal risk?*
  - *How do we establish and maintain cyber security as a process?*
- *Financial Risk:*
  - *What is the financial risk of the most likely breach?*
  - *How likely is such a breach?*
  - *How much financial risk should we transfer (insurance)?*
- *Legal Risk:*
  - *What is our exposure to third-party liability claims?*
  - *Will my insurance cover my losses?*

Legal Risk Solution:

- *Affordable, accessible SaaS that allows businesses to identify legal risks and legal outcomes based on:*
  - *Historical court rulings on all cyber-relevant insurance litigations at state and federal level*
  - *Our analyses and interpretations of these litigations*

Approach - CLAD

- *Build an extensive legal repository of cyber insurance lawsuits*
- *Analyze these lawsuits and study all the court filings by the parties and the rulings by the court*
- *Code these lawsuits across a large number of relevant variables (e.g., parties, issues raised, duration, outcomes across issues, etc…)*
- *Check out CLAD at: https://ciri-cyber.shinyapps.io/clad/*

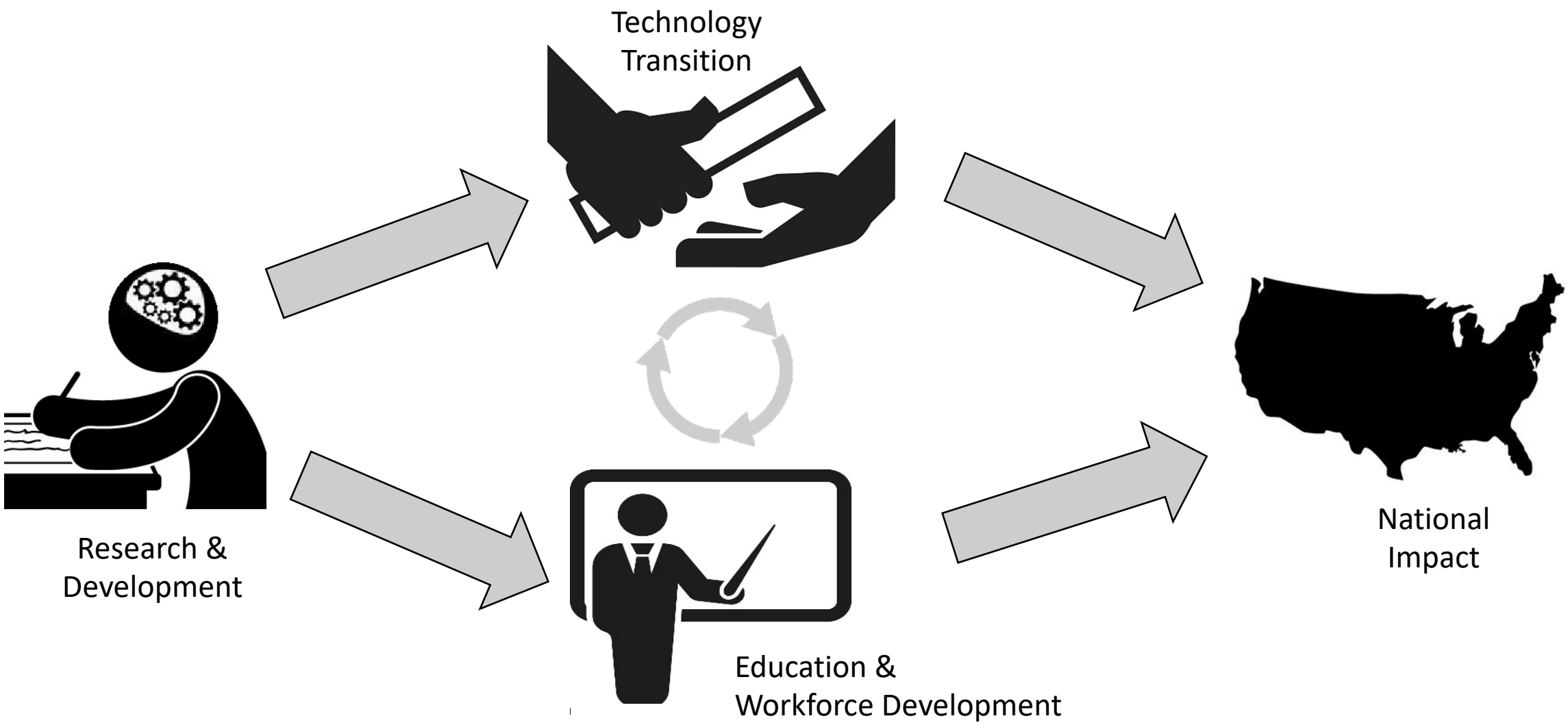
Benefits

- *Fills a gap – no other current database addresses cyber insurance litigation*
- *Provides SMEs with detailed and accurate information to:*
  - *Inform insurance policy design*
  - *Prepare for litigation*
  - *Inform enhancements to internal company processes*
- *Long term: more mature cyber insurance market*
  - *Better policies*
  - *Less uncertainties*
  - *More affordable premiums*

Transition Activities:

- *Validate market and value proposition*
- *Examine go-to-market strategies*
- *Explore appropriate business model*
- *Engagement with potential business partners*

Exemplar Project: Integrating Tech Transition & Workforce Development


Technology Transition
Research & Development
Education & Workforce Development
National Impact

Nationwide Impact:

Training-Augmented Cybersecure Dashboard

Training Curriculum & Content

Community Colleges & SBDCs

Dashboard used as training tool

MEP • MANUFACTURING EXTENSION PARTNERSHIP

AMERICA'S SBDC
SMALL BUSINESS DEVELOPMENT CENTERS

SLTT Governments

Business Enterprises