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)*
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
SME MANUFACTURING

NIST 800-171
- 47% Compliant
- 21% Variance
- 32% Non-Compliant

The NIST SP 800-171 is a standardized set of requirements to protect Controlled Unclassified Information (CUI) resident in non-governmental organizations. This view looks at your cybersecurity posture from a NIST 800-171 perspective.

NIST Cybersecurity Framework
- 17% Compliant
- 14% Variance
- 69% Non-Compliant

The NIST Cybersecurity Framework (CSF) provides an organizing structure that consist of standards, guidelines, and best practices to manage cybersecurity-related risks. This view looks at your cybersecurity posture from a NIST CSF perspective.

NIST Manufacturing Profile
- 46% Compliant
- 13% Variance
- 41% 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 looks at your cybersecurity posture from a NIST Manufacturing Profile perspective.
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.
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.

<table>
<thead>
<tr>
<th></th>
<th>Loss Probability</th>
<th>95% Value-at-Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large financial institution with more than 500 employees</td>
<td>79.27%</td>
<td>$148.79 Million</td>
</tr>
<tr>
<td>Small financial institution with fewer than 10 employees</td>
<td>1.32%</td>
<td>$0.09 Million</td>
</tr>
</tbody>
</table>
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/](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
Nationwide Impact:

Training Curriculum & Content

Dashboard used as training tool

Community Colleges & SBDCs

Business Enterprises

SLTT Governments

Training-Augmented Cybersecure Dashboard