OCTOBER 2021

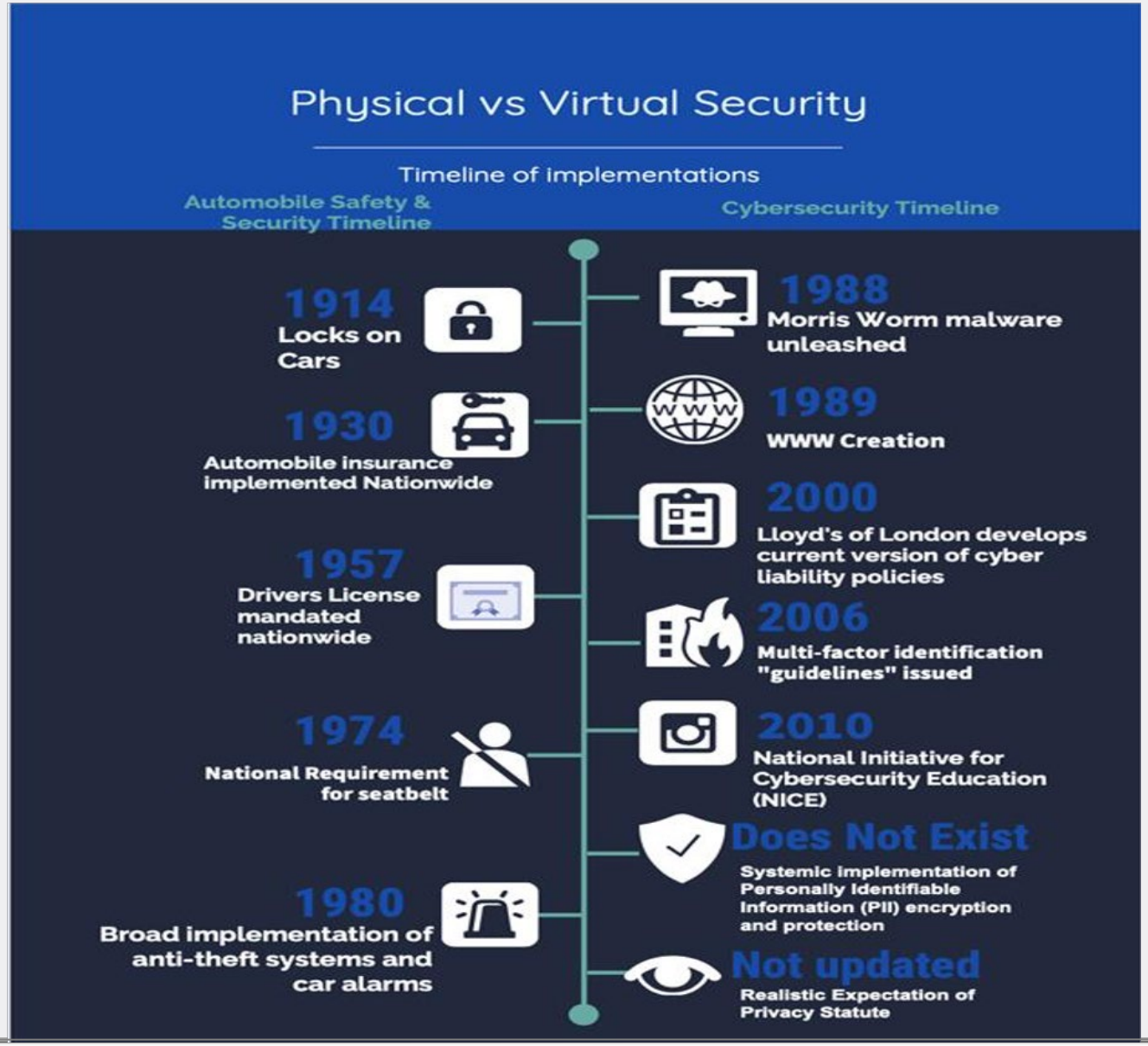
Risk in the Digital Age

State Focused:
Cyber Risk Management Frameworks

Digital Age Impact:

- Work, Comms, Transactions, Social Interaction Online
- IOT Exponential Growth
- Every Org & Person Has a Digital Footprint
- Software Foundational To All Online Functionality
- Criminals Entering & Living Within Your Networks
- Unless It Is Encrypted, Assume Someone Has It
- Limitless Publicly Available Data Sets
- AI Based Risk & Business Intelligence Solutions

Crime, Fraud & Disruption – Alignment of Capability, Intention, Opportunity


Physical vs Virtual Security
Timeline of implementations
Automobile Safety & Security Timeline
Cybersecurity Timeline
1914
Locks on Cars
1930
Automobile insurance implemented Nationwide
1957
Drivers License mandated nationwide
1974
National Requirement for seatbelt
1980
Broad implementation of anti-theft systems and car alarms
1988
Morris Worm malware unleashed
1989
WWW Creation
2000
Lloyd's of London develops current version of cyber liability policies
2006
Multi-factor identification "guidelines" issued
2010
National Initiative for Cybersecurity Education (NICE)
Does Not Exist
Systemic implementation of Personally Identifiable Information (PII) encryption and protection
Not updated
Realistic Expectation of Privacy Statute

Wisconsin Exemplars:
Impacts from Online Crime, Fraud & Disruption

SolarWinds C-SCRM

- U.S. Bankruptcy Court for the Western District of Wisconsin
- Affected Case Management - Electronic Case Files system (CM/ECF)
- Highly sensitive documents stored there (including sealed filings) were at risk

JBS Ransomware Attack

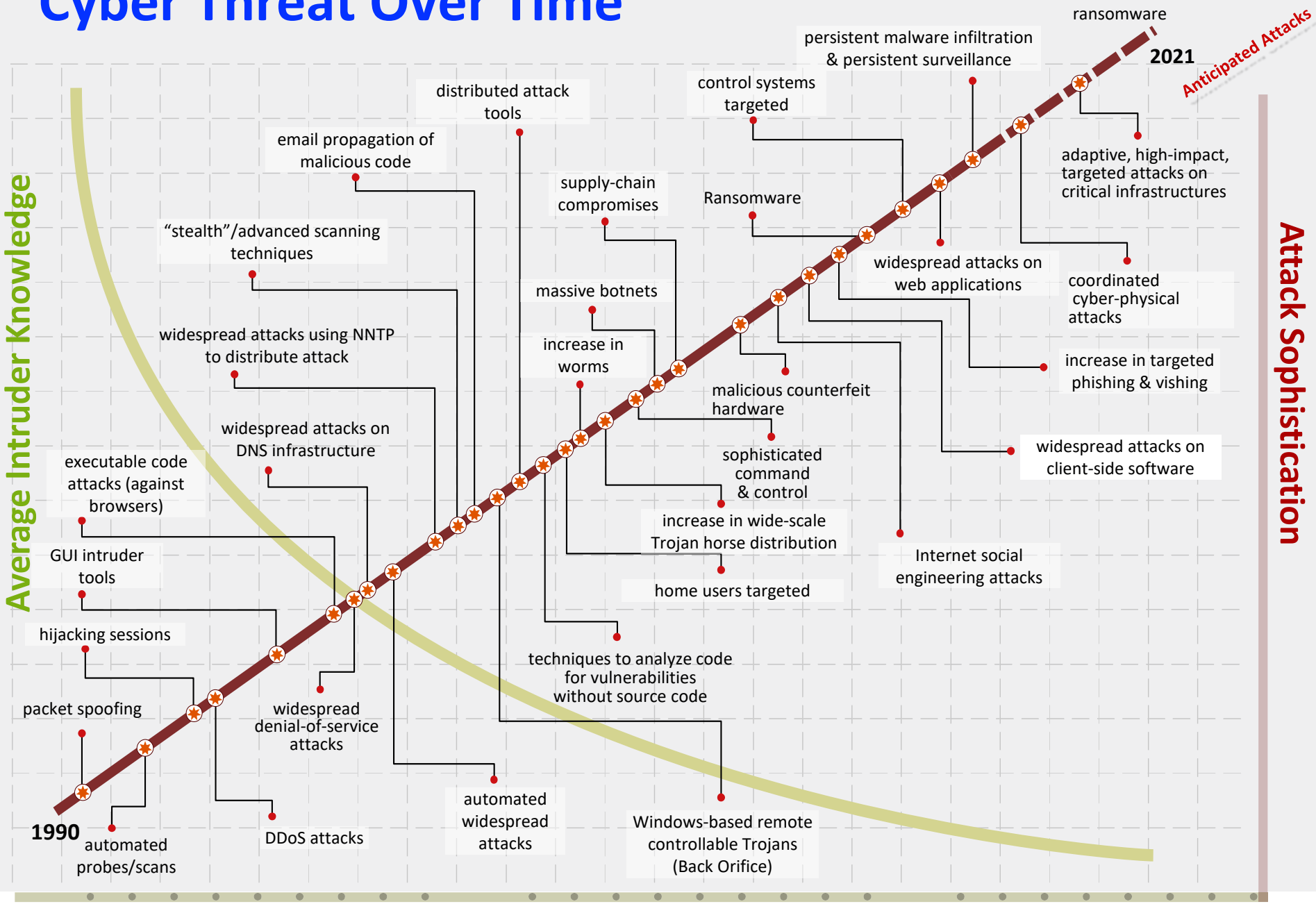
- Green Bay facility forced to shut down

Reported Trends:

- Business Email Compromise (BEC) (EAC) - $16,409,640
- Identity Theft - $1,266,777
- Corporate Data Breach - $1,201,186
- Ransomware - $886,386

* From the FBI IC3 Report

Cyber Threat Over Time



State and Local Sector

Landscape Dynamics and Challenges

- **The Threat -** This Sector and its architectures face a relentless cyber threat from a broad range of sophisticated cyber actors

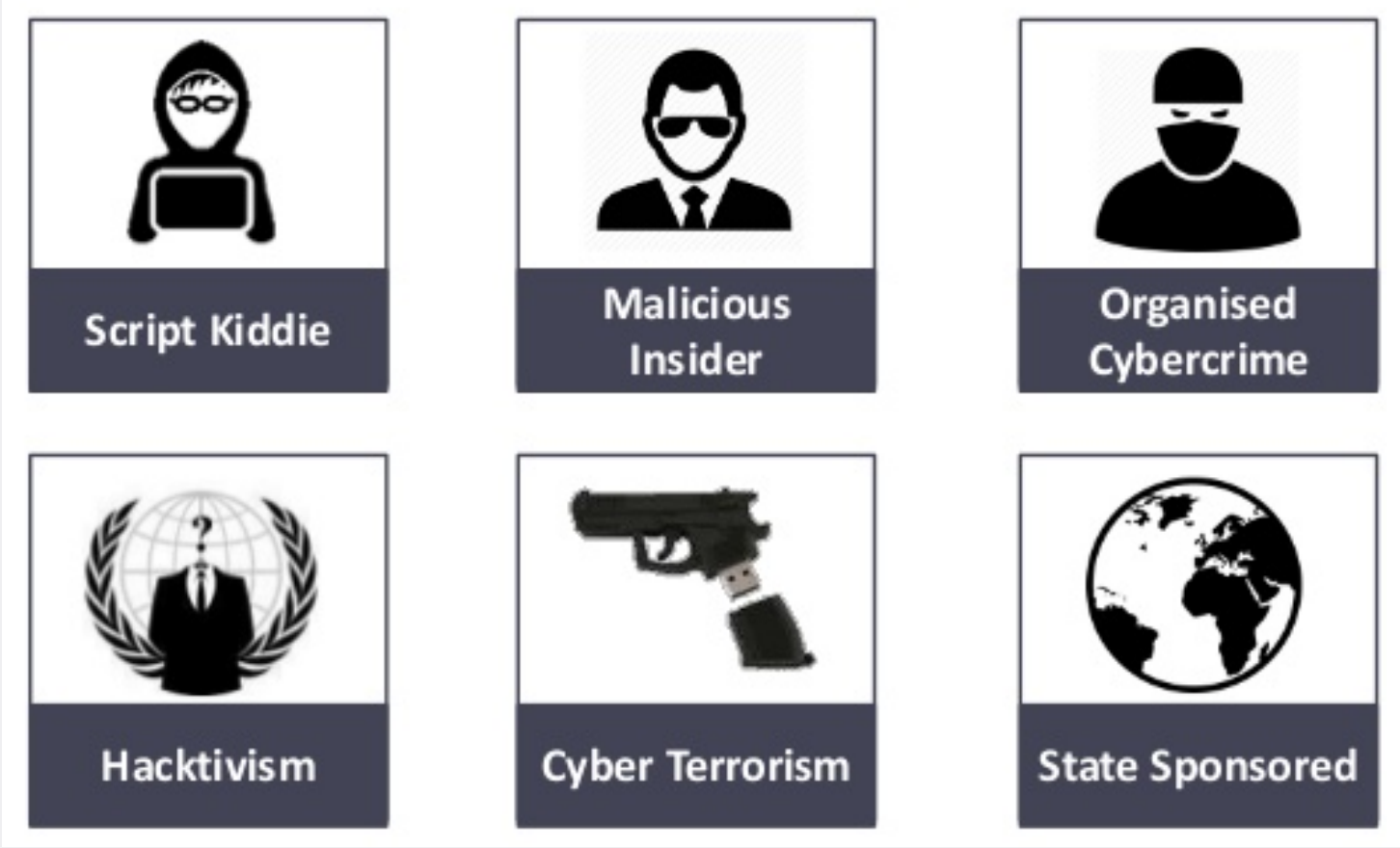
- **Complexity -** According to the census, Wisconsin has **3,096 governments**, the 11th-most in the country. Nearly two-thirds of the state's local governments are “general purpose”: counties (72), cities and villages (601), and towns (1,251)

- **Awareness -** Majority of Executives/Managers are aware of the general cyber risks impacting their Sector, but do not have continuous insight into - current cyber risk indicators, capability gaps and threat trends across their organization/s, region, nor supply chain

- **Approach -** Therefore, today’s focus is primarily on implementing best practices and known standards, all of which is foundational but not sufficient, to ensure Sector Wide resilience and performance - through any major cyber event

https://www.wisconsin.gov/Pages/AllAgencies.aspx

Primary Cyber Bad Actors:
Now Targeting ALL Businesses & Organizations



Majority are just plain cyber criminals

Cyber Risk Management Framework Approach

WHITEHAWK

Achieving Cyber Resilience

- Continuous Risk Insight
- Identify & Prioritize Gaps
- Sector/Sub-Sector & Regional Risk Trends
- Plan of Action to Mitigate Risks
- Response Plan
- Team Enablement & OJT
- Cost Effectiveness

Cyber Risk Management Framework:

- Fast tracks all risk discovery and prioritization
- Save limited manpower and resources
- Provide actionable, sourced and prioritized risks
- Delivers action plans to address key cyber risks

Provides decision-makers with executive level risk context & insight foundational to policy & initiative development

Cyber Risk Management Framework Premise

LEVERAGE BEST OF BREED AI TECH & OPEN DATA ANALYTICS

- With access to open network & ICS data sets, AI-driven analytics, and instrumentation, commercial grade IT, OT & ICS risk rating capabilities can now provide effective transparency, risk monitoring, alerting & mitigation in real-time.

ACHIEVING A RISK BASELINE WITH LIMITED RESOURCES

- By providing affordable access to best of breed risk rating and mitigation services and analytics Sector wide, most risks can be affordably identified and addressed.

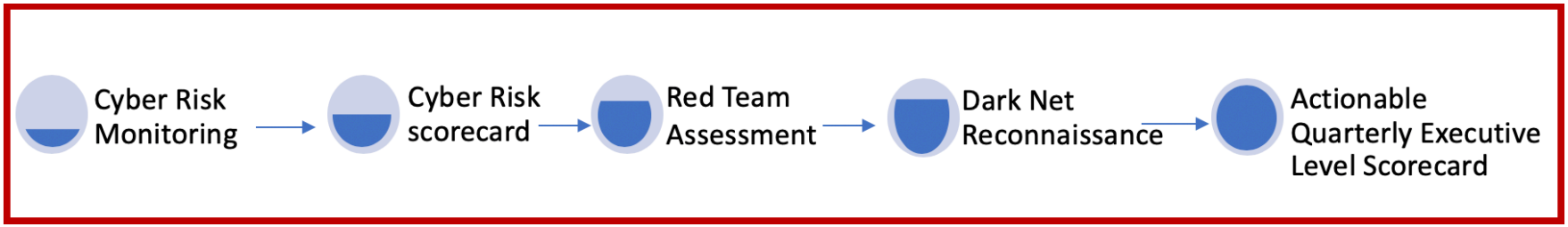
- A Cyber Risk Management Framework, with continuous monitoring, alerting, trend reporting, gap analysis and executive level discussion points, can inform Energy Sector stakeholders of:
  - Current Cyber Risk Posture Today
  - How to Continuously Improve

Cyber Risk Management Program Deliverables

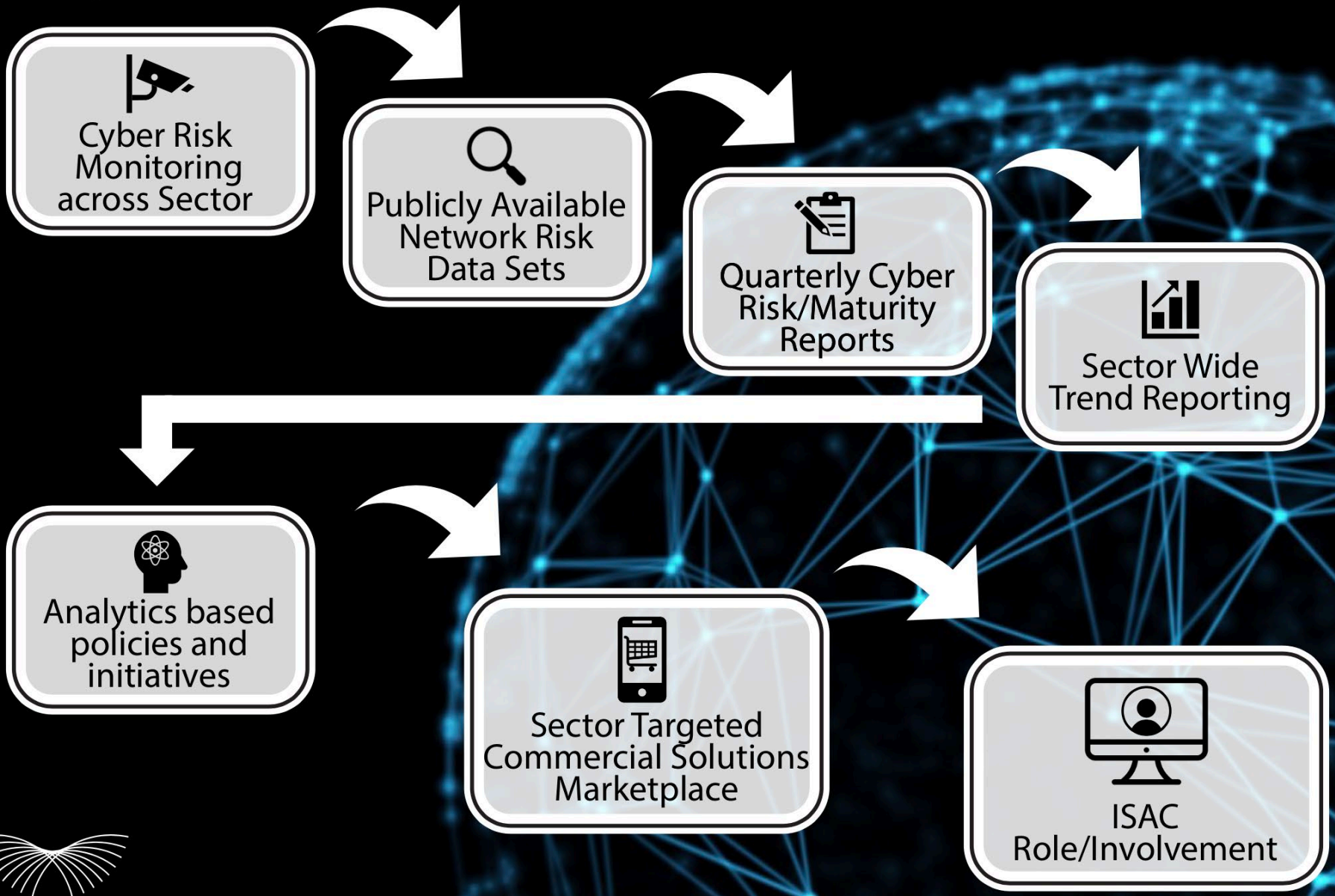
Expert, Independent, Outside-In Annual or Continuous Digital Age Risk Assessment

How to enable IT Manager/CIO/CSO/CISO's, Exec Teams & Review Boards to ensure or validate:

- The Truth About Your Organization's Cyber Resilience
- Your Inside Team, Managed Service Provider or Security Vendors' Cyber Resilience is on Track
- An Annual or Continuous Cyber Risk Audit
- Where to place your next cyber resilience investment or how to make smart cost reductions
- Effective quarterly communication to your Leadership on how you have accomplished your Cyber Due Diligence and Resourcing Priorities



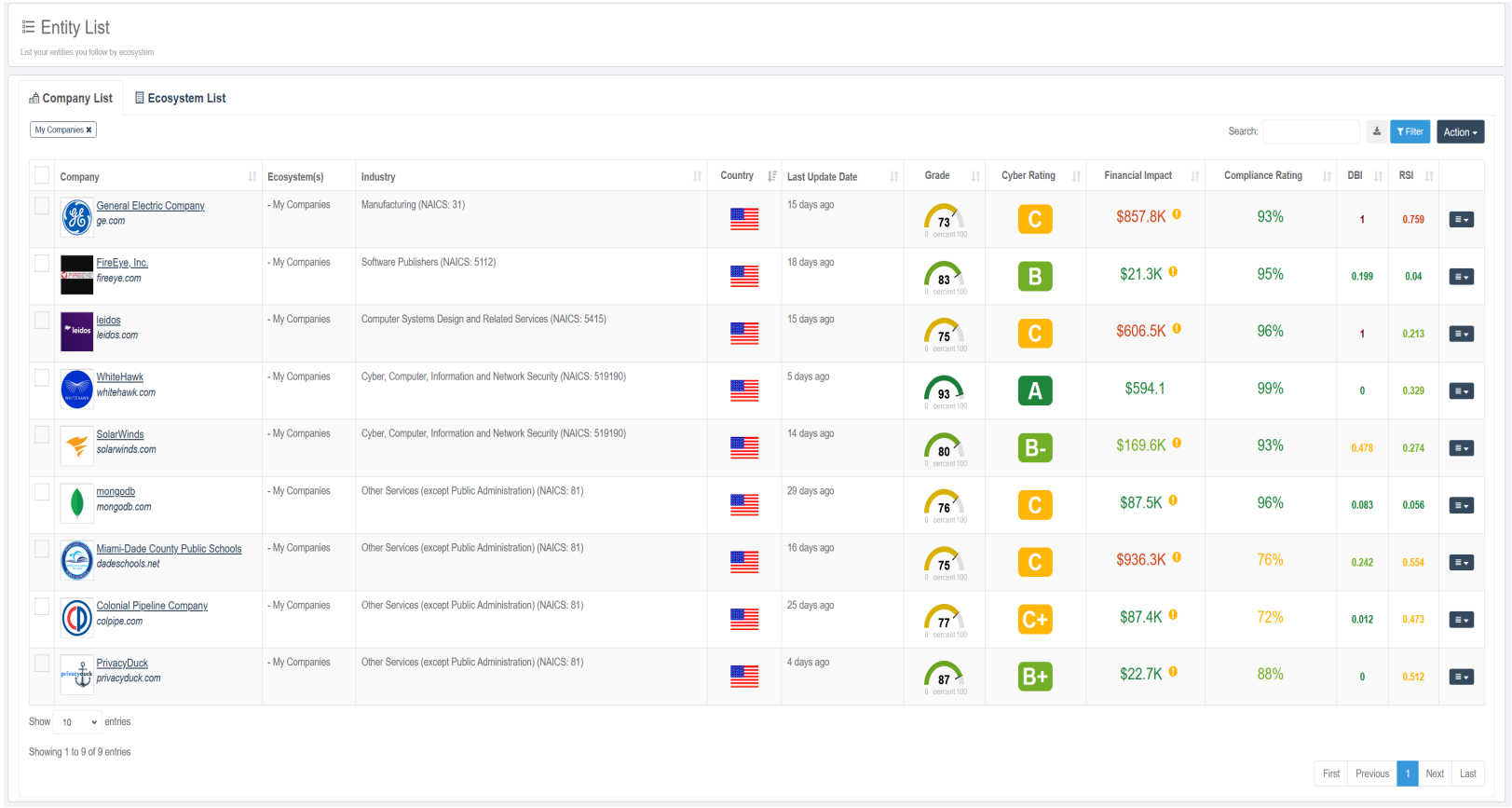
Cyber Risk Management Framework Approach



WHITEHAWK

Cyber Risk – Continuous Monitoring

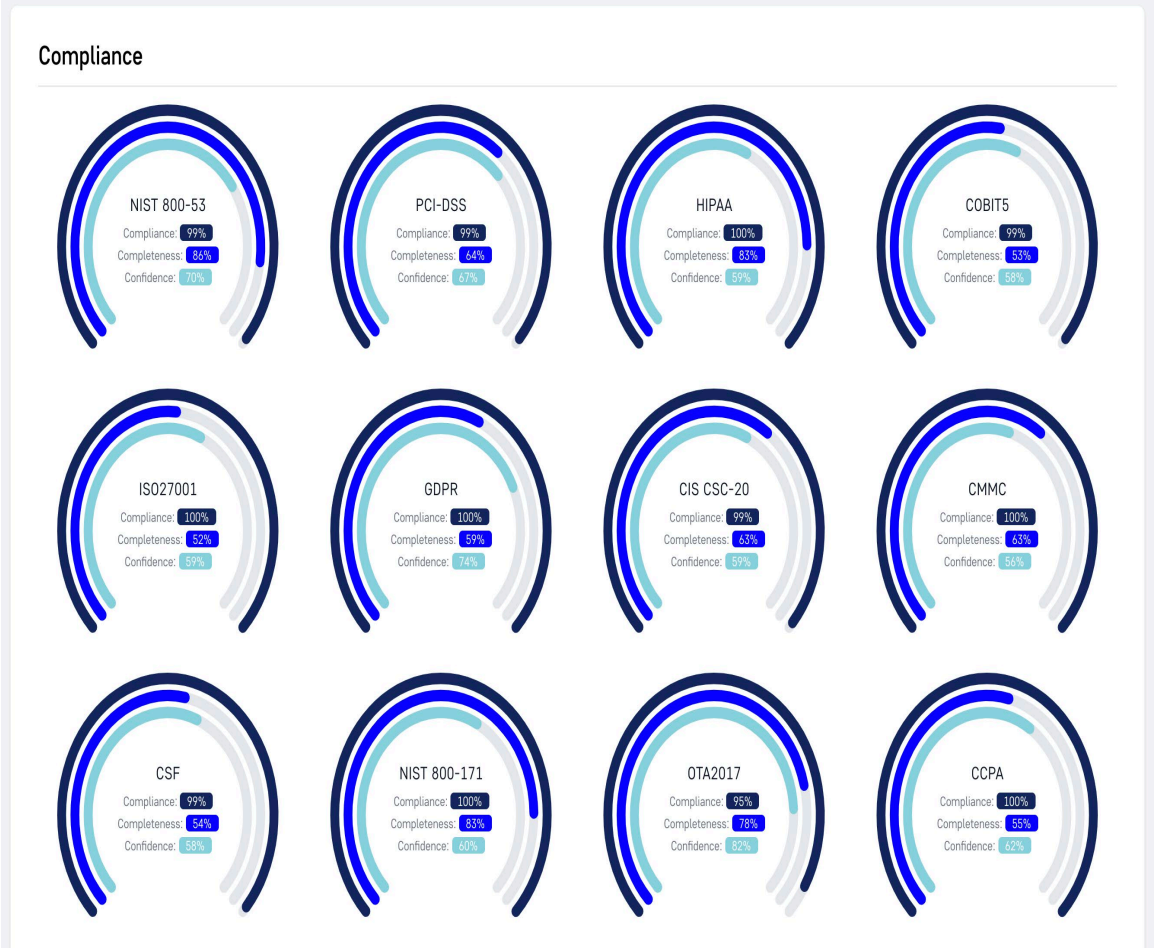
Individual and/or Portfolio of Public/Private Entities – Easily Tailorable to Accommodate Internal IT, Programs, and Compliance Needs



Cyber Risk – Compliance

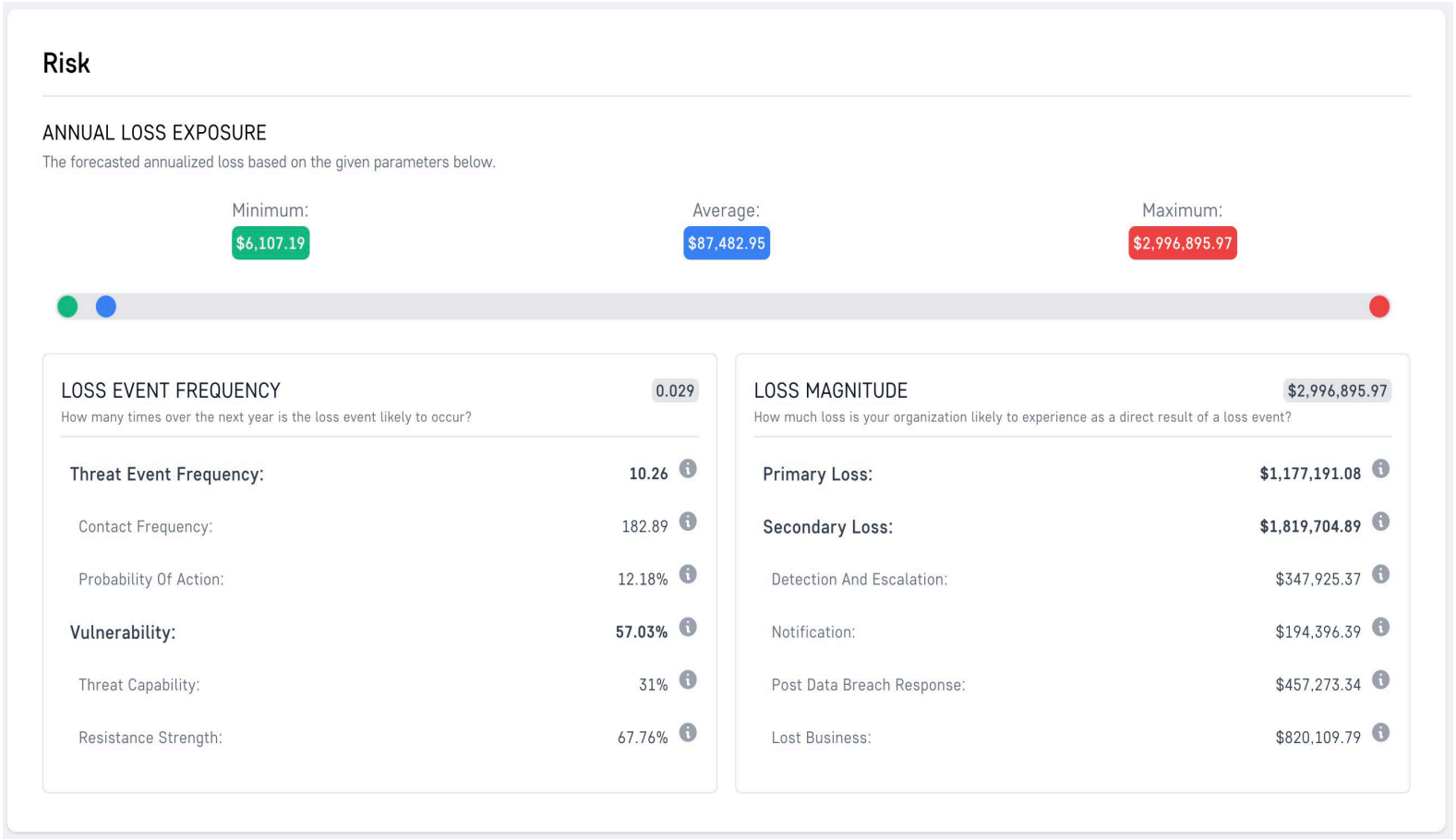
Estimation of an Entity's Overall Compliance Health

- **Compliance:** *The overall compliance score is how much of the specified framework we believe you are following, based on platform validation and self-attestation.*
- **Completeness:** *The level of confidence in the estimation. Without access to internal systems and processes, only able to provide a score based on the information available and how much it aligns with the controls in the framework.*
- **Confidence:** *The degree to which the compliance requirements can be measured with the collected information. This score is generated by matching collected artifacts to framework control areas. Each area of the framework has requirements that can be met by policy or configuration*



Cyber Risk – Financial Impact of Event

Through the FAIR Model, Understand Cyber Risks in terms of Potential Financial Loss Due to Breaches.



Organizational Risk

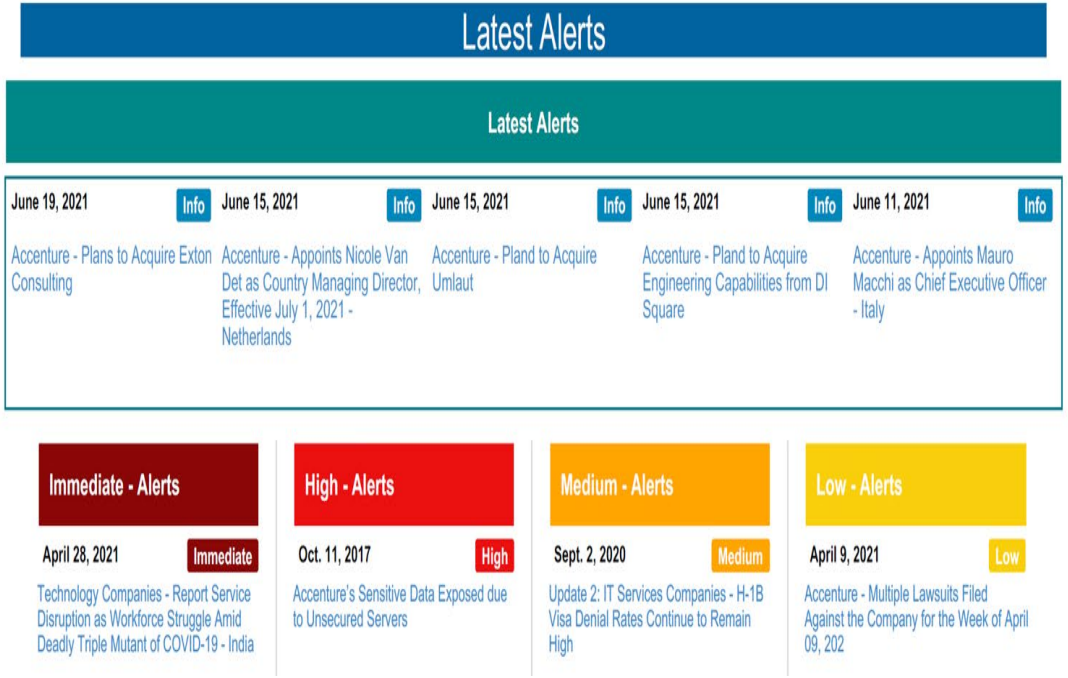
Track and Be Alerted to an Organization's Operational, Governance, and People Risks.

Executive Summary

Risk Snapshot

Manager Category	Q4 2020		Q1 2021		22-Jun-2021
Composite Risk	N/A		4.10		4.14
Financial Risk	N/A		5.30		5.30
Solutions Maturity Risk	N/A		2.49		2.59
People Risk	N/A		4.45		4.45
Client Risk	N/A		2.65		2.65
Governance, Regulatory & Compliance Risk	N/A		4.00		4.10
Cyber Security Risk	N/A		4.80		4.80

Latest Alerts



Automated Cyber Risk Reporting

Prioritized Areas of Focus, Executive Level Summary, Including Shareable/Actionable 20-page Report.

Company			Domain				
mongodb			mongodb.com				
Security Rating *Ratings measure a company's relative security effectiveness.*			**Risk Vector Performance** *Risk Vector grades show how well the company is managing each risk vector.*				
C (76.0/100)	Advanced: Intermediate: Basic:	100 – 80 79 – 70 60 – 0	Compromised Systems: Communications Encryption: Attack Surface:	B B A	System Patching: Application Security: Email Security: Public Disclosure:	B F A B	
Factor Analysis of Information Risk (FAIR) - Annualized Risk *Forecasted annualized loss magnitude risk of a potential loss to your company.*			**Prioritized Areas of Focus** *WhiteHawk Cyber Analyst has identified top-3 Focus Areas the company should consider.*				
Most Likely:	$87,482.95		**Focus Area 1:**	Application Security			
Minimum:	$6,107.19		**Focus Area 2:**	Compromised Systems			
Maximum:	$2,996,895.97		**Focus Area 3:**	Communications Encryption			

Solution Options

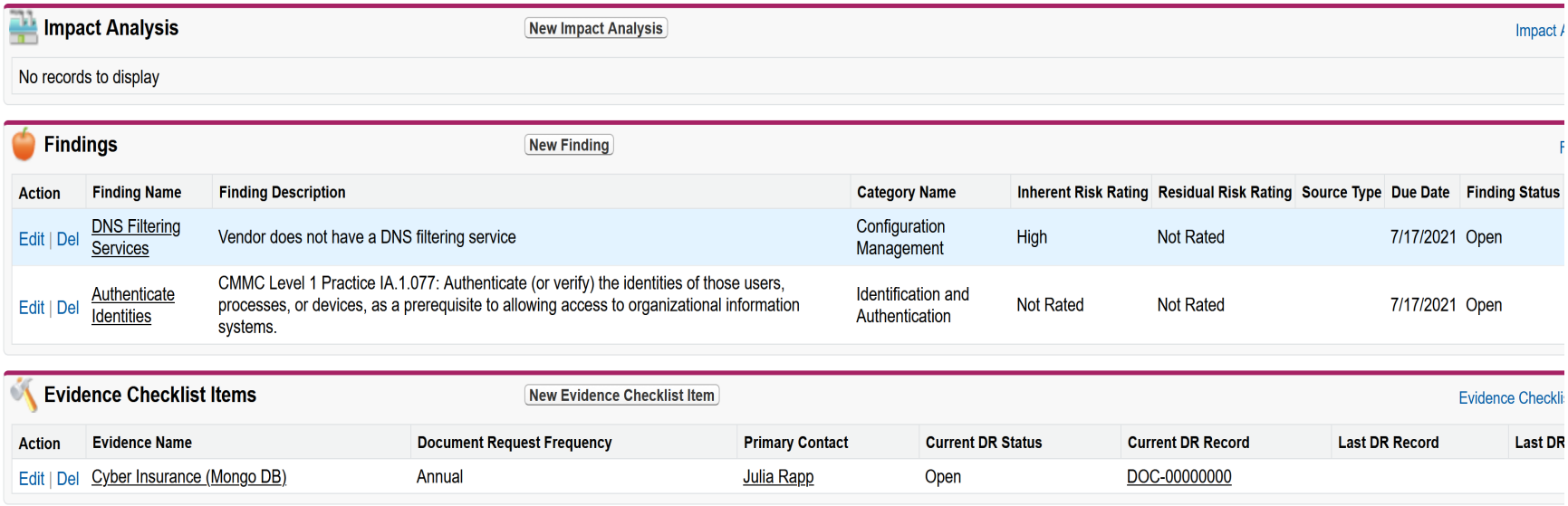
Solution options that address primary business risks identified in the Cyber Risk Scorecard. Alternatives for each are included in the product details section.

Essential Bundle	Balanced Bundle	Premier Bundle
– *Flexera Software: AdminStudio Suite* – *Mimecast: Email Signature Management*	– *ClearNetwork Services: SOC-As-A-Service* – *Juniper Networks: SRX Series Services Gateways* – *Symantec: Blue Coat Malware Analysis Appliance*	– *Trend Micro: Trend Micro 24/7 Support* – *Fortinet: FortiAnalyzer* – *Cyber BDA: Cyber Business Development* – *Remediant: Remediant SecureONE*

For more solution options, visit www.whitehawk.com/marketplace

SaaS Risk Management Dashboards

Track and Manage Risk Findings at the Sub-Sector or Entity level as desired



Impact Analysis — New Impact Analysis — Impact A

No records to display

Findings — New Finding — F

Action	Finding Name	Finding Description	Category Name	Inherent Risk Rating	Residual Risk Rating	Source Type	Due Date	Finding Status
Edit | Del	DNS Filtering Services	Vendor does not have a DNS filtering service	Configuration Management	High	Not Rated		7/17/2021	Open
Edit | Del	Authenticate Identities	CMMC Level 1 Practice IA.1.077: Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Identification and Authentication	Not Rated	Not Rated		7/17/2021	Open

Evidence Checklist Items — New Evidence Checklist Item — Evidence Checkli

Action	Evidence Name	Document Request Frequency	Primary Contact	Current DR Status	Current DR Record	Last DR Record	Last DR
Edit | Del	Cyber Insurance (Mongo DB)	Annual	Julia Rapp	Open	DOC-00000000		

- ✓ DETECT: risks from multiple internal & external sources.
- ✓ MONITOR: compliance, maturity, risk mitigation
- ✓ SECURE ACCESS: to all stakeholders with appropriate permissions
- ✓ MITIGATION: track all risk mitigation status

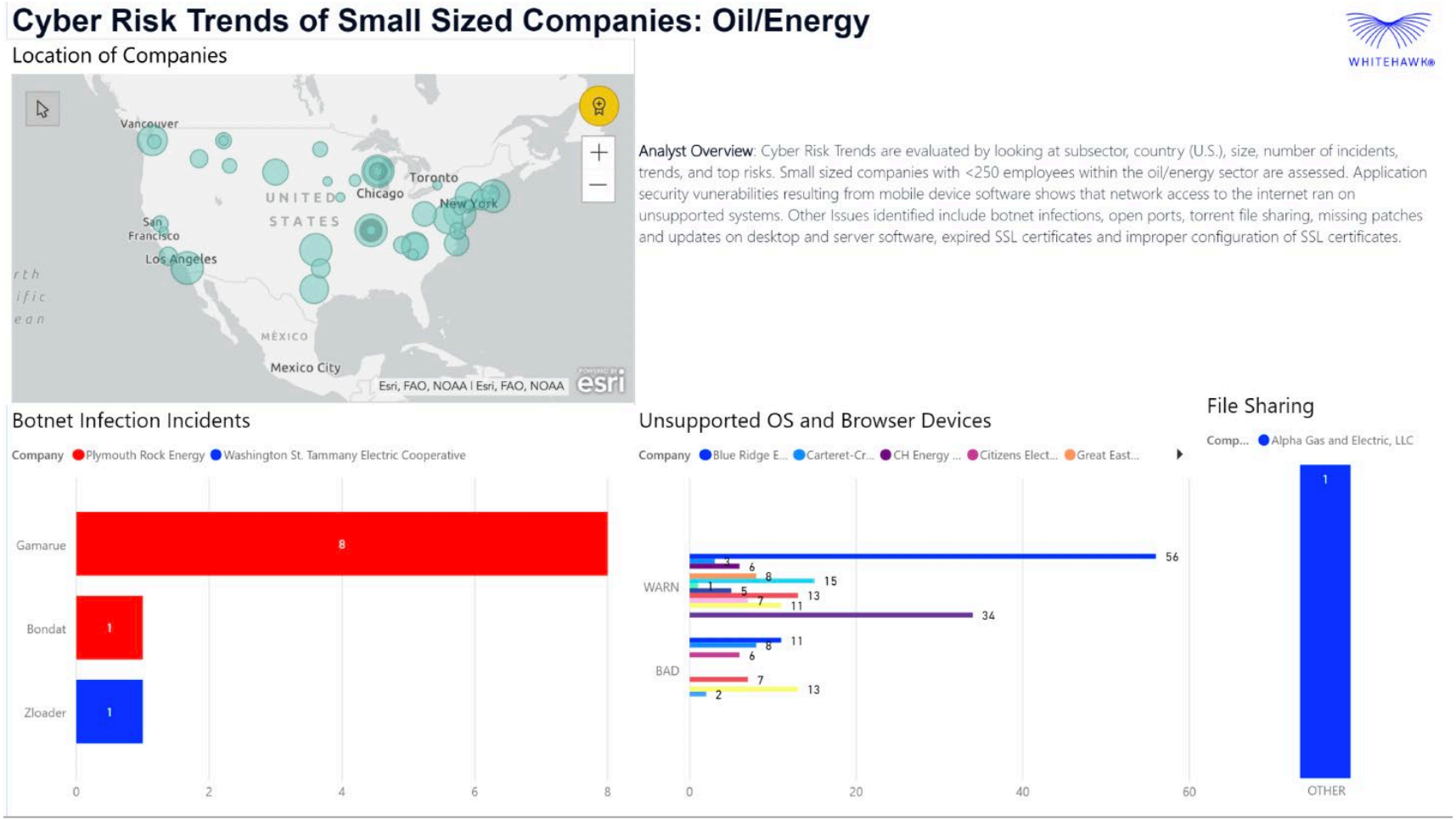
Cyber Risk Management Framework: Program Objectives

Continuous Cyber Risk Monitoring, Alerting, and Scoring of Cyber Risk Indicators across the State, by sub-sector, by region, and down to the entity level:

- **Identification and tracking of priority cyber vulnerabilities and gaps** across all Sub-Sectors and Regions
- **Integrated SaaS Dashboard and Portal** access and insights into risk ratings and risk mitigation in real-time
- **Creation and Tailoring of Executive Level Reporting** of Trends, Measures, and Metrics to meet reporting and risk mitigation requirements
- **Foundational trend analysis and key gap overviews** mapped to potential policy, standard, and technology recommendations and initiatives

Development of consistent measures and metrics of cyber risk mitigation, maturity levels, and continuous improvements

Visualization Exemplar



Cyber Marketplace

WHITEHAWK

Cloud Based

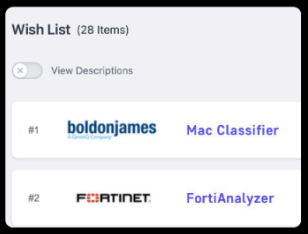
Prioritized Risk

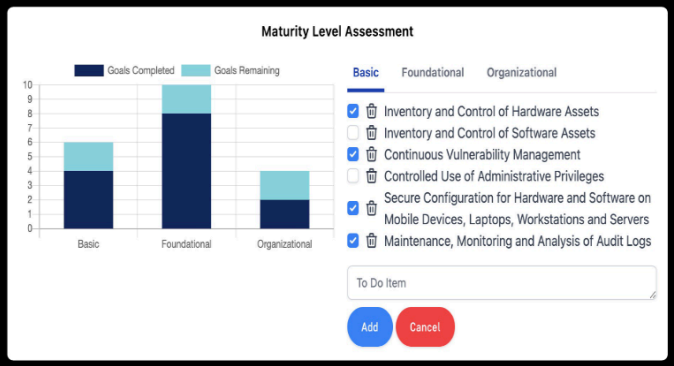
Shopping List

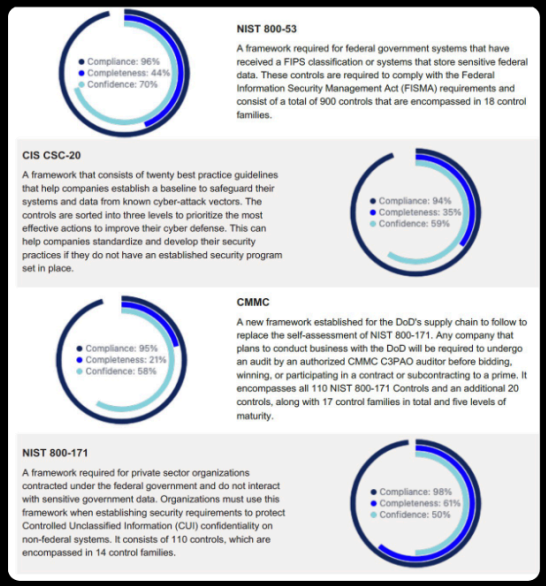
Maturity Compliance

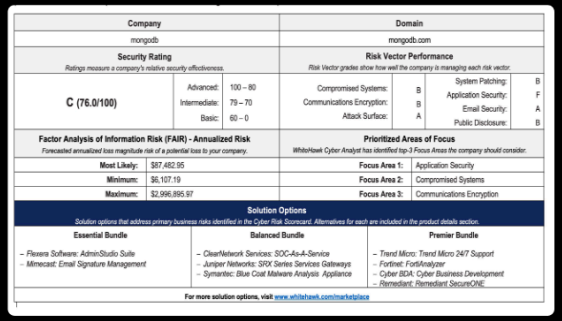
Compliance

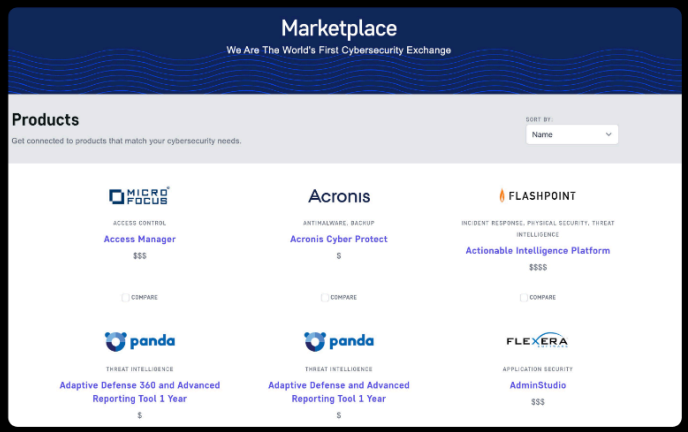
Focus Areas mapped to FAIR model











Vendor Vetting → Testing → Available for Sale

Mapping to Cybersecurity E.O.

Executive Order on Improving the Nation's Cybersecurity – May 12, 2021

Sec. 2. Removing Barriers to Sharing Threat Information: *Leverage all Publicly Available risk & threat data – including IT, OT, and ICS datasets*

Sec. 3. Modernizing Federal Government Cybersecurity: *Continuously identify vulnerable, obsolete & porous tech & frameworks - replace them*

Sec. 4. Enhancing Software Supply Chain Security: *Implement SaaS based testing & continuous monitoring of all software-based solutions sold to the Federal Market via DHS CISA QSMO Cybersecurity Marketplace*

Sec. 5. Establishing a Cyber Safety Review Board: *Provide quarterly Cyber Risk portfolio reporting across each Sector, identifying key risk trends, potential policies and initiatives to address them*

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Mapping to Cybersecurity E.O.

Executive Order on Improving the Nation's Cybersecurity – May 12, 2021

Sec. 6. Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents: *Start by arming leadership with comprehensive vulnerability & incident trends by Sub-Sector/Region/Size*

Sec. 7. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks: *Conduct "Hacker View" continuous risk monitoring & Red Team validation of all Federal Government Networks*

Sec. 8. Improving the Federal Government's Investigative and Remediation Capabilities: *Alert on & share in real-time key threat vectors from continuous risk monitoring & SaaS based commercial Red Team findings*

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Establish: Your Cyber Risk Baseline, Action Plan & Response Plan

Management Team/Review Boards:

- Know the truth about your cyber resilience
- No inside team, managed service provider nor solution vendor is infallible
- Don't assume - get the facts with a “Hacker View” of your cyber risks
- Validate where to place your next cyber resilience investment or how to make smart cost cuts
- Conduct cyber due diligence continuously

Demonstrate ROI for your risk mitigation investments & make smart cuts when needed

Get Started Today

Are you organized/aligned for Success: Cyber Readiness Index 2.0 https://potomacinstitute.org/academic-centers/cyber-readiness-index

- **Determine What You Need To Protect First**:
  - Intellectual property, client/employee information, financial data, communications, etc.
- **Keep Up With The Technology**
  - Legacy IT, Software upgrades, IT security patches, passwords and protocols, cyber risk ratings and continuous monitoring
- **Be an Active Consumer:**
  - Demand assurance, protection and additional security measures from your service or product providers. Start with your Home Office!
- **Know the Current Cybercrime and Fraud Trends Impacting Your State:**
  - https://wifusion.widoj.gov/form/cyber-incident-reporting
  - Cyber Threat Alliance