

OCTOBER 2021



Risk in the Digital Age

State Focused:

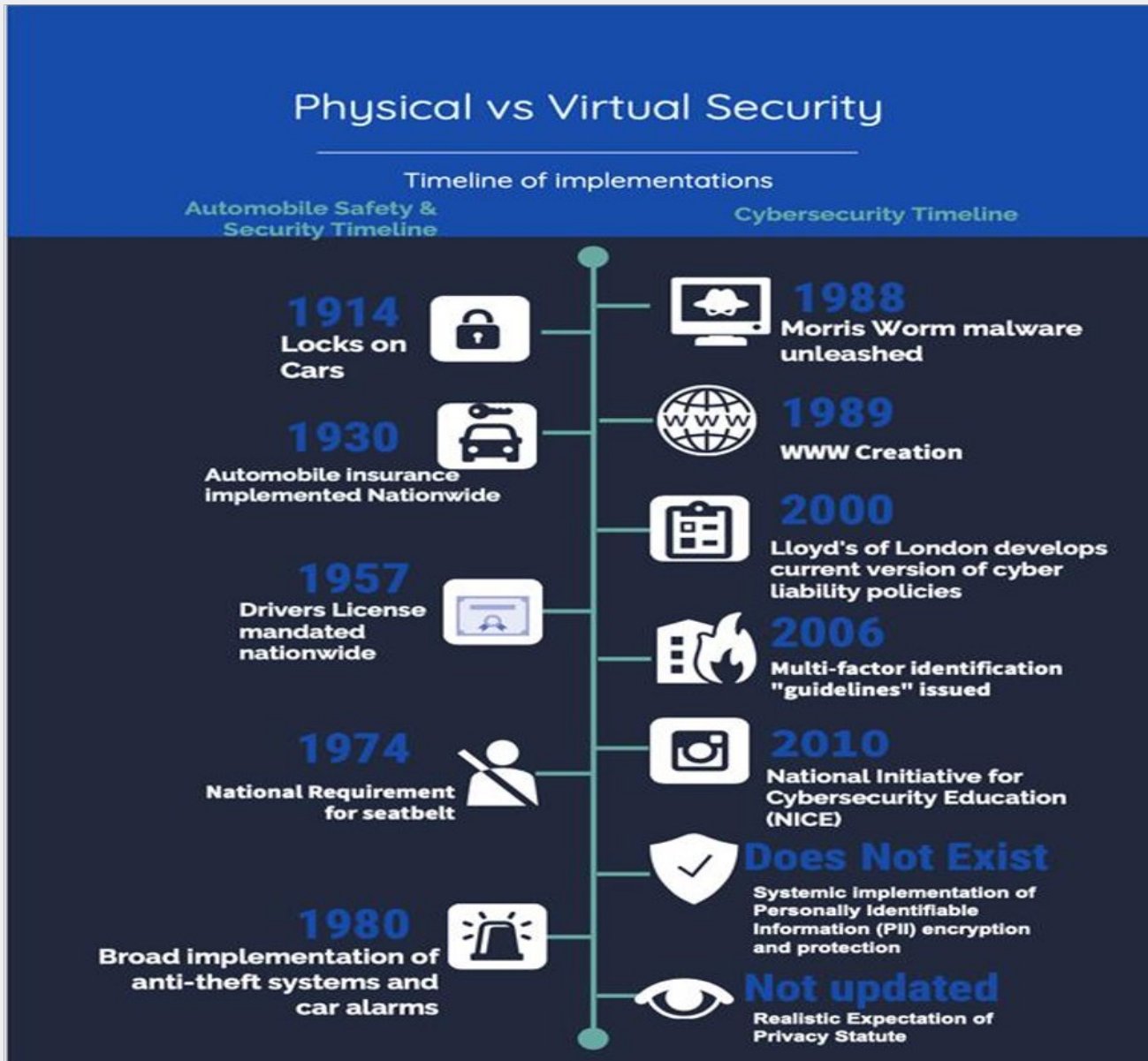
Cyber Risk Management Frameworks

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



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

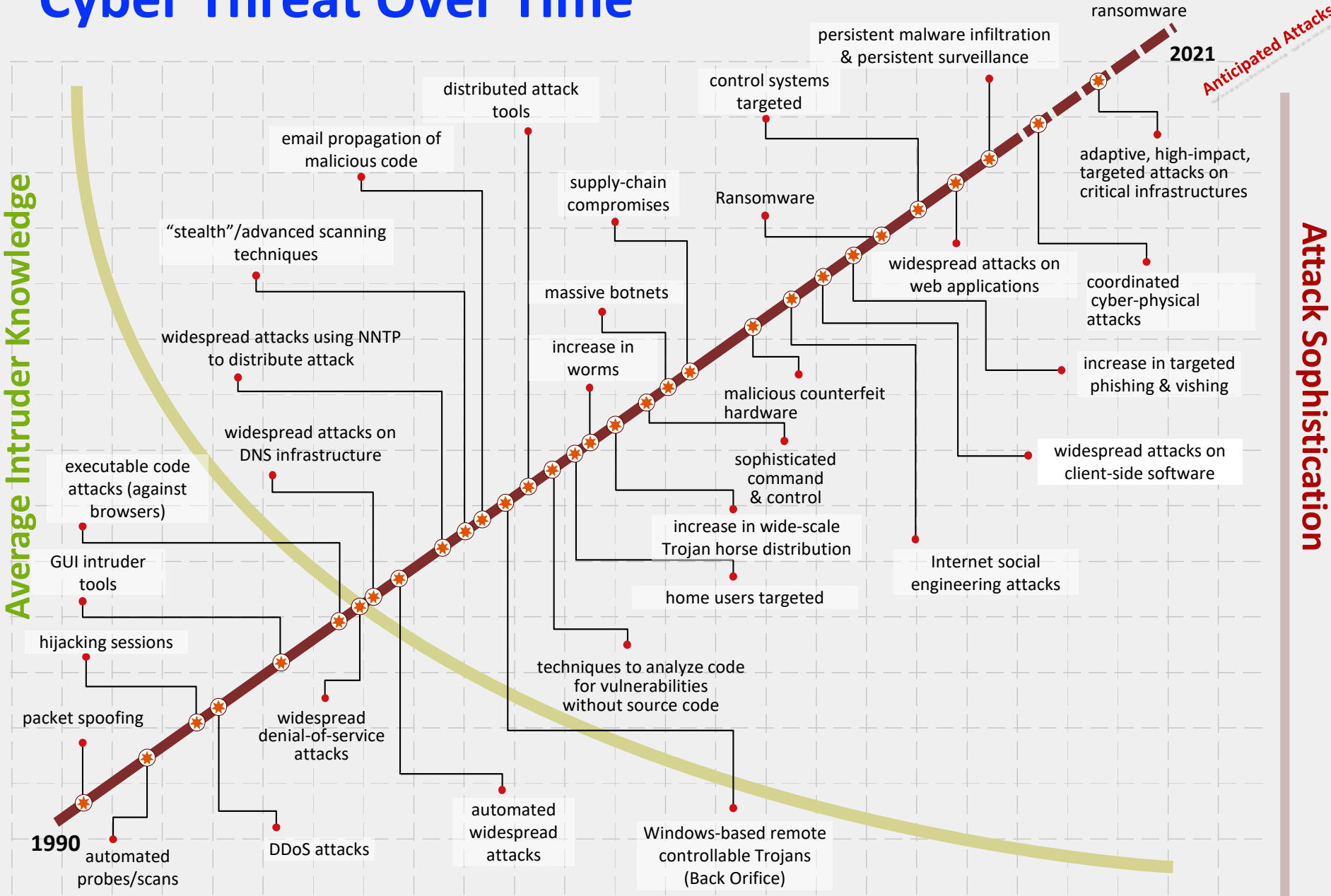
- Green Bay facility forced to shut down

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



Average Intruder Knowledge

Attack Sophistication

Anticipated Attacks

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



Cyber Risk Monitoring across Sector



Publicly Available Network Risk Data Sets



Quarterly Cyber Risk/Maturity Reports



Sector Wide Trend Reporting



Analytics based policies and initiatives



Automation & Scalability



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

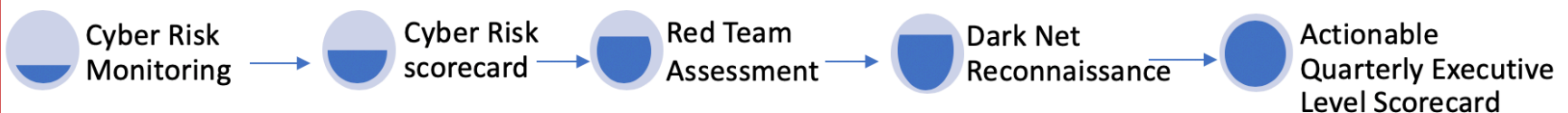
- By providing affordable access to best of breed risk rating and mitigation services and analytics Sector wide, most risks can be affordably identified and addressed.
- A Cyber Risk Management Framework, with continuous monitoring, alerting, trend reporting, gap analysis and executive level discussion points, can inform Energy Sector stakeholders of:
 - Current Cyber Risk Posture Today
 - How to Continuously Improve

Cyber Risk Management Program Deliverables

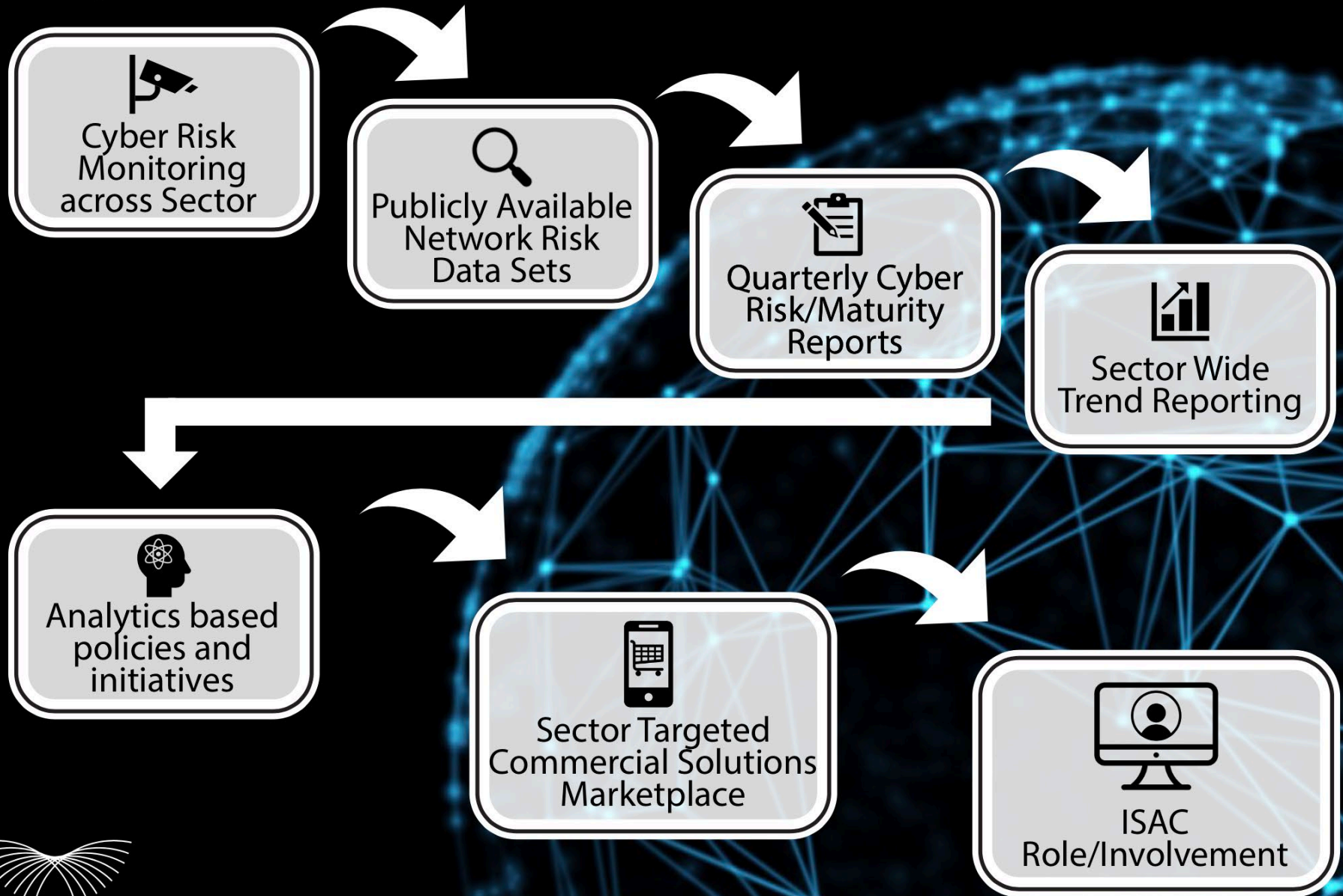
Expert, Independent, Outside-In Annual or Continuous Digital Age Risk Assessment

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



Cyber Risk – Continuous Monitoring

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

Entity List

List your entities you follow by ecosystem

Company List | Ecosystem List

My Companies x Search: Filter Action

Company	Ecosystem(s)	Industry	Country	Last Update Date	Grade	Cyber Rating	Financial Impact	Compliance Rating	DBI	RSI	
General Electric Company ge.com	- My Companies	Manufacturing (NAICS: 31)		15 days ago	73 0 percent 100	C	\$857.8K	93%	1	0.759	
FireEye, Inc. fireeye.com	- My Companies	Software Publishers (NAICS: 5112)		18 days ago	83 0 percent 100	B	\$21.3K	95%	0.199	0.04	
iidos iidos.com	- My Companies	Computer Systems Design and Related Services (NAICS: 5415)		15 days ago	75 0 percent 100	C	\$606.5K	96%	1	0.213	
WhiteHawk whitehawk.com	- My Companies	Cyber, Computer, Information and Network Security (NAICS: 519190)		5 days ago	93 0 percent 100	A	\$594.1	99%	0	0.329	
SolarWinds solarwinds.com	- My Companies	Cyber, Computer, Information and Network Security (NAICS: 519190)		14 days ago	80 0 percent 100	B-	\$169.6K	93%	0.478	0.274	
mongodb mongodb.com	- My Companies	Other Services (except Public Administration) (NAICS: 81)		29 days ago	76 0 percent 100	C	\$87.5K	96%	0.083	0.056	
Miami-Dade County Public Schools dadeschools.net	- My Companies	Other Services (except Public Administration) (NAICS: 81)		16 days ago	75 0 percent 100	C	\$936.3K	76%	0.242	0.554	
Colonial Pipeline Company colpipe.com	- My Companies	Other Services (except Public Administration) (NAICS: 81)		25 days ago	77 0 percent 100	C+	\$87.4K	72%	0.012	0.473	
PrivacyDuck privacyduck.com	- My Companies	Other Services (except Public Administration) (NAICS: 81)		4 days ago	87 0 percent 100	B+	\$22.7K	88%	0	0.512	

Show 10 entries

Showing 1 to 9 of 9 entries

First Previous 1 Next Last

Cyber Risk – Compliance

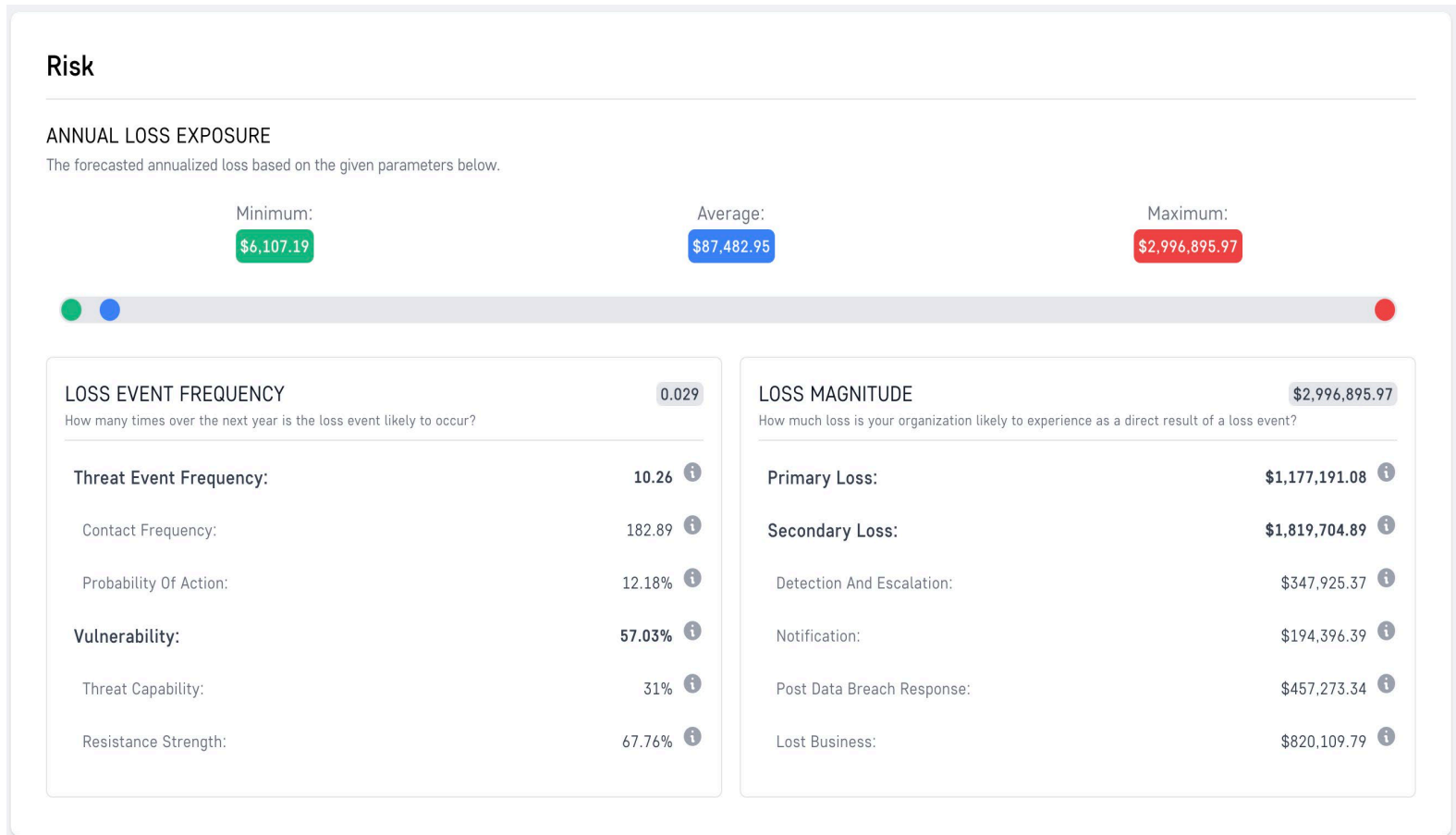
Estimation of an Entity’s Overall Compliance Health

- 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

Latest Alerts

June 19, 2021	Info	June 15, 2021	Info	June 15, 2021	Info	June 15, 2021	Info	June 11, 2021	Info
Accenture - Plans to Acquire Exton Consulting		Accenture - Appoints Nicole Van Det as Country Managing Director, Effective July 1, 2021 - Netherlands		Accenture - Pland to Acquire Umlaut		Accenture - Pland to Acquire Engineering Capabilities from DI Square		Accenture - Appoints Mauro Macchi as Chief Executive Officer - Italy	

Immediate - Alerts

April 28, 2021 **Immediate**
 Technology Companies - Report Service Disruption as Workforce Struggle Amid Deadly Triple Mutant of COVID-19 - India

High - Alerts

Oct. 11, 2017 **High**
 Accenture's Sensitive Data Exposed due to Unsecured Servers

Medium - Alerts

Sept. 2, 2020 **Medium**
 Update 2: IT Services Companies - H-1B Visa Denial Rates Continue to Remain High

Low - Alerts

April 9, 2021 **Low**
 Accenture - Multiple Lawsuits Filed Against the Company for the Week of April 09, 2021

Automated Cyber Risk Reporting

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

Company			Domain			
mongodb			mongodb.com			
Security Rating			Risk Vector Performance			
<i>Ratings measure a company's relative security effectiveness.</i>			<i>Risk Vector grades show how well the company is managing each risk vector.</i>			
C (76.0/100)	Advanced:	100 – 80	Compromised Systems:	B	System Patching:	B
	Intermediate:	79 – 70	Communications Encryption:	B	Application Security:	F
	Basic:	60 – 0	Attack Surface:	A	Email Security:	A
			Public Disclosure:		B	
Factor Analysis of Information Risk (FAIR) - Annualized Risk			Prioritized Areas of Focus			
<i>Forecasted annualized loss magnitude risk of a potential loss to your company.</i>			<i>WhiteHawk Cyber Analyst has identified top-3 Focus Areas the company should consider.</i>			
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						
<i>Solution options that address primary business risks identified in the Cyber Risk Scorecard. Alternatives for each are included in the product details section.</i>						
Essential Bundle		Balanced Bundle		Premier Bundle		
<ul style="list-style-type: none"> - Flexera Software: AdminStudio Suite - Mimecast: Email Signature Management 		<ul style="list-style-type: none"> - ClearNetwork Services: SOC-As-A-Service - Juniper Networks: SRX Series Services Gateways - Symantec: Blue Coat Malware Analysis Appliance 		<ul style="list-style-type: none"> - 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 /

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-0000000		

- ✓ 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 Risk Trends of Small Sized Companies: Oil/Energy

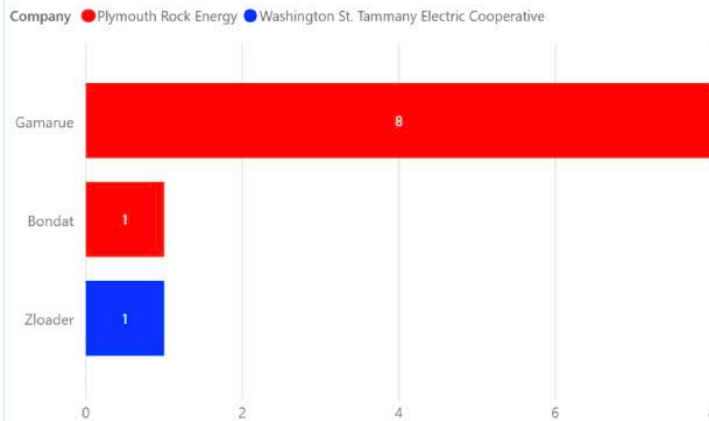


Location of Companies

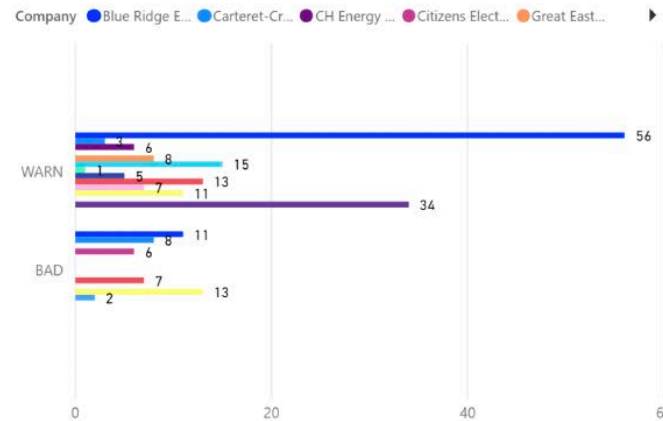


Analyst Overview: Cyber Risk Trends are evaluated by looking at subsector, country (U.S.), size, number of incidents, trends, and top risks. Small sized companies with <250 employees within the oil/energy sector are assessed. Application security vulnerabilities resulting from mobile device software shows that network access to the internet ran on unsupported systems. Other Issues identified include botnet infections, open ports, torrent file sharing, missing patches and updates on desktop and server software, expired SSL certificates and improper configuration of SSL certificates.

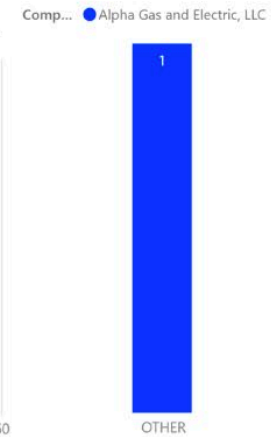
Botnet Infection Incidents



Unsupported OS and Browser Devices



File Sharing



Cyber Marketplace



Cloud Based

Prioritized Risk

Shopping List

Maturity Compliance

Compliance

Wish List (28 Items)

View Descriptions

- #1 boldonjames Mac Classifier
- #2 FORTINET FortiAnalyzer

Maturity Level Assessment

Basic Foundational Organizational

- Inventory and Control of Hardware Assets
- Inventory and Control of Software Assets
- Continuous Vulnerability Management
- Controlled Use of Administrative Privileges
- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- Maintenance, Monitoring and Analysis of Audit Logs

To Do Item

Add Cancel

Focus Areas mapped to FAIR model

NIST 800-53

A framework required for federal government systems that have received a FIPS classification or systems that store sensitive federal data. These controls are required to comply with the Federal Information Security Management Act (FISMA) requirements and consist of a total of 900 controls that are encompassed in 18 control families.

- Compliance: 96%
- Completeness: 44%
- Confidence: 70%

CIS CSC-20

A framework that consists of twenty best practice guidelines that help companies establish a baseline to safeguard their systems and data from known cyber-attack vectors. The controls are sorted into three levels to prioritize the most effective actions to improve their cyber defense. This can help companies standardize and develop their security practices if they do not have an established security program set in place.

- Compliance: 94%
- Completeness: 35%
- Confidence: 59%

CMMC

A new framework established for the DoD's supply chain to follow to replace the self-assessment of NIST 800-171. Any company that plans to conduct business with the DoD will be required to undergo an audit by an authorized CMMC C3PAO auditor before bidding, winning, or participating in a contract or subcontracting to a prime. It encompasses all 110 NIST 800-171 Controls and an additional 20 controls, along with 17 control families in total and five levels of maturity.

- Compliance: 95%
- Completeness: 21%
- Confidence: 58%

NIST 800-171

A framework required for private sector organizations contracted under the federal government and do not interact with sensitive government data. Organizations must use this framework when establishing security requirements to protect Controlled Unclassified Information (CUI) confidentiality on non-federal systems. It consists of 110 controls, which are encompassed in 14 control families.

- Compliance: 98%
- Completeness: 61%
- Confidence: 50%

Company	Domain																
mongob.	mongob.com																
Security Rating	Risk Vector Performance																
Rating: measure a company's overall security effectiveness	Risk Vector grades show how well the company is managing each risk vector:																
C (76.0/100)	<table border="1"> <tr> <td>Compromised Systems:</td> <td>B</td> <td>System Patching:</td> <td>B</td> </tr> <tr> <td>Communications Encryption:</td> <td>B</td> <td>Application Security:</td> <td>F</td> </tr> <tr> <td>Attack Surface:</td> <td>A</td> <td>Email Security:</td> <td>A</td> </tr> <tr> <td></td> <td></td> <td>Public Disclosure:</td> <td>B</td> </tr> </table>	Compromised Systems:	B	System Patching:	B	Communications Encryption:	B	Application Security:	F	Attack Surface:	A	Email Security:	A			Public Disclosure:	B
Compromised Systems:	B	System Patching:	B														
Communications Encryption:	B	Application Security:	F														
Attack Surface:	A	Email Security:	A														
		Public Disclosure:	B														
Factor Analysis of Information Risk (FAIR) - Annualized Risk	Prioritized Areas of Focus																
Forecasted annualized loss magnitude risk of a potential loss to your company.	Whitehawk Cyber Analyst has identified top-3 Focus Areas the company should consider:																
Most Likely: \$2,482,85	Focus Area 1: Application Security																
Minimum: \$6,107.19	Focus Area 2: Compromised Systems																
Maximum: \$2,986,955.57	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																
<ul style="list-style-type: none"> Flarex Software: AdminStudio Suite Mimecast: Email Signature Management 	<ul style="list-style-type: none"> ClearNetwork Services: SOCA-A-Service Juniper Networks: SRX Series Services Gateways Symantec: Blue Coat Malware Analysis Appliance 																
Premier Bundle																	
<ul style="list-style-type: none"> Trend Micro: Trend Micro 24/7 Support Fortinet: FortiAnalyzer Cyber Risk: Cyber Business Development Rimeliant: Rimeliant SecureONE 																	
For more solution options, visit www.whitehawk.com/marketplace																	

Marketplace

We Are The World's First Cybersecurity Exchange

Products

Get connected to products that match your cybersecurity needs.

Sort By: Name

MICRO FOCUS	Acronis	FLASHPOINT
ACCESS CONTROL	ANTI-MALWARE, BACKUP	INCIDENT RESPONSE, PHYSICAL SECURITY, THREAT INTELLIGENCE
Access Manager	Acronis Cyber Protect	Actionable Intelligence Platform
\$\$\$	\$	\$\$\$\$
COMPARE	COMPARE	COMPARE
panda	panda	FLEXERA
THREAT INTELLIGENCE	THREAT INTELLIGENCE	APPLICATION SECURITY
Adaptive Defense 360 and Advanced Reporting Tool 1 Year	Adaptive Defense and Advanced Reporting Tool 1 Year	AdminStudio
\$	\$	\$\$\$

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](#)
-