

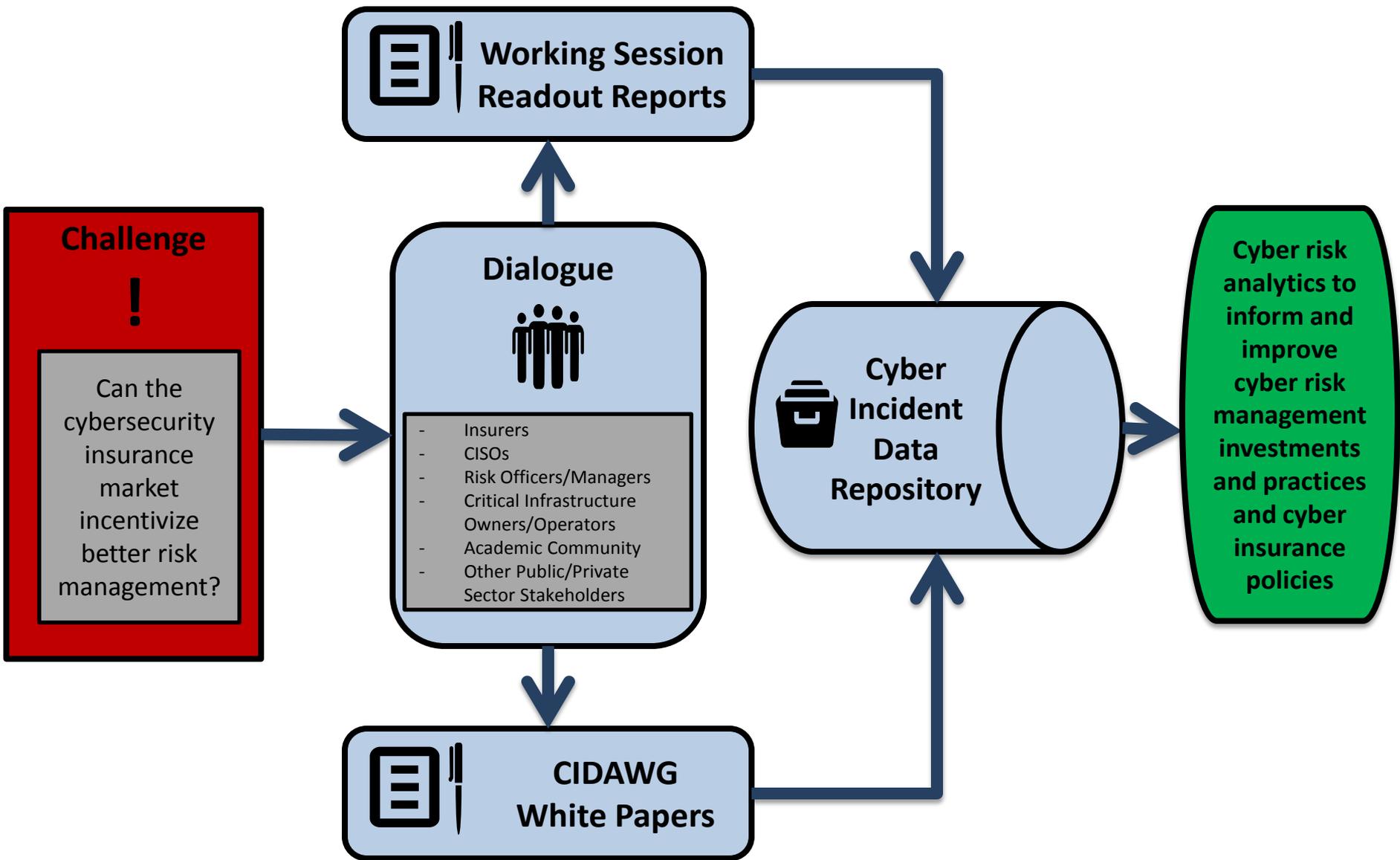


# Homeland Security

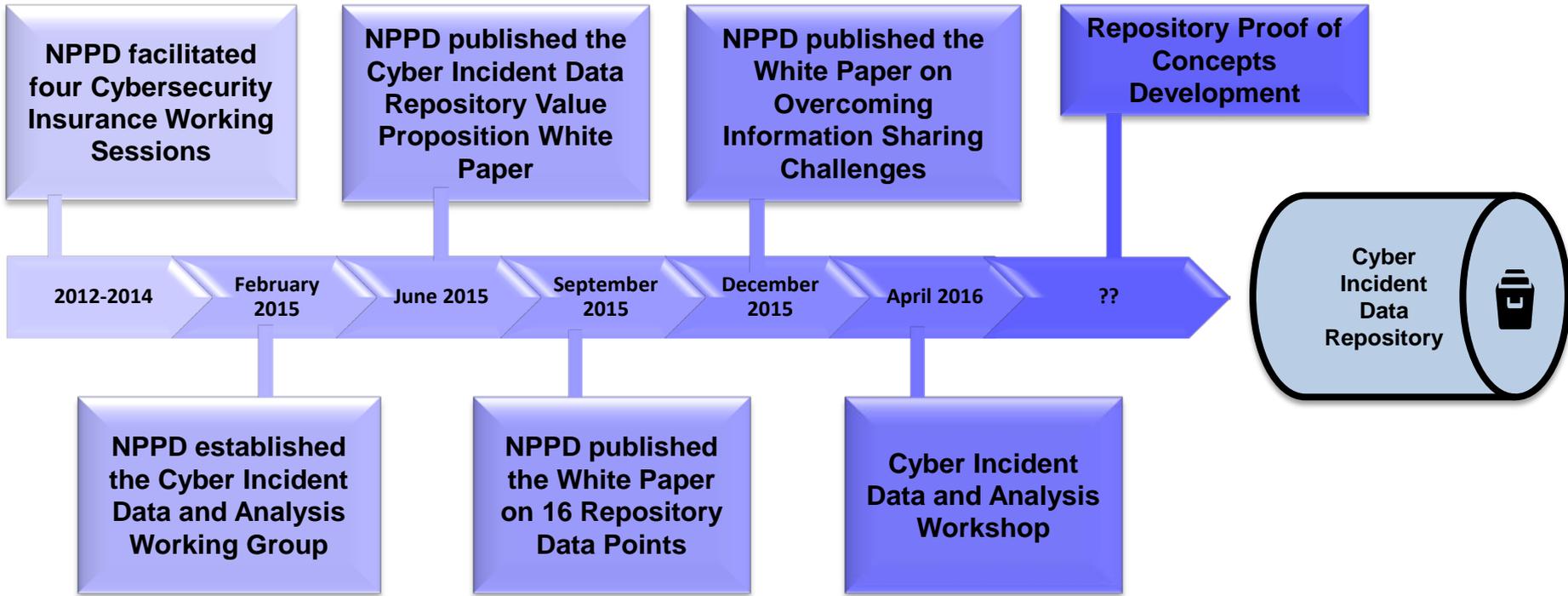
## **Cyber Incident Data and Analysis Repository Workshop**

April 19-20, 2016

# Repository Concept Development



# Repository Concept Development Timeline

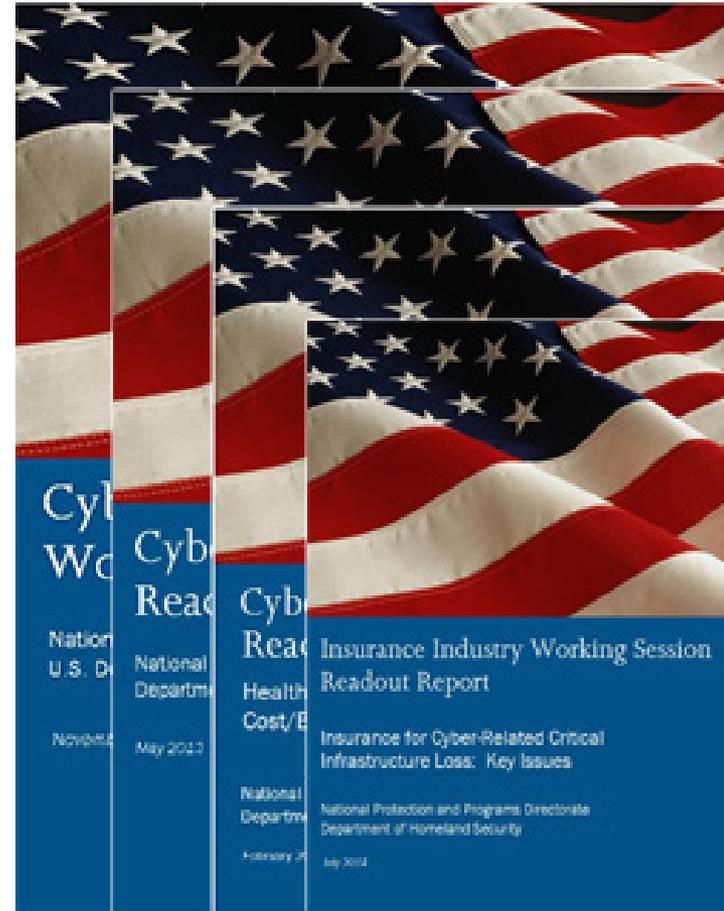


## Key obstacles:

- Lack of actuarial data;
- Absence of best practices, standards, and metrics;
- Limited knowledge of critical infrastructure dependencies & interdependencies; and
- Underdeveloped enterprise risk management programs.

## Key Recommendations

- Focus on the concept of a **cyber incident data repository (CIDAR)**
- Engage Chief Information Security Officers (CISOs) and other cybersecurity professionals as essential discussion partners in the development of a CIDAR.



Available on DHS' Cybersecurity Insurance webpage at:  
[www.dhs.gov/publication/cybersecurity-insurance](http://www.dhs.gov/publication/cybersecurity-insurance)



- NPPD established the Cyber Incident Data and Analysis Working Group (CIDAWG) in February 2014 to explore the benefits and the feasibility of cyber incident data repository.
- CIDAWG participants include private sector IT risk management professionals representing various critical infrastructure sectors and functions and insurance companies.
- The CIDAWG conducted biweekly meetings to:
  - Develop the Value Proposition
  - Identify Repository Data Points
  - Identify Information Sharing Challenges and solutions
- CIDAWG white papers were published on DHS's website:  
<https://www.dhs.gov/publication/cyber-incident-data-and-analysis-working-group-white-papers>

# Cyber Incident Data and Analysis Repository

## Data Points

- Type of Incident
- Timeline
- Contributing Causes
- Use of Cyber Security Framework
- DATA POINTS

- ❖ Federal and SLTT governments and private sector data
- ❖ Comprehensive (volume, variety, quality)
- ❖ Advances actuarial data
- ❖ Free – contributing data is the “cost of admission”
- ❖ Non-government hosted, voluntary, secure and anonymized

## Benefits

- Top Risks and Effective Controls
- Peer-to-Peer Benchmarking
- ROI
- Sector Differentiation
- Forecasting, Trending and Modeling



# Value Proposition



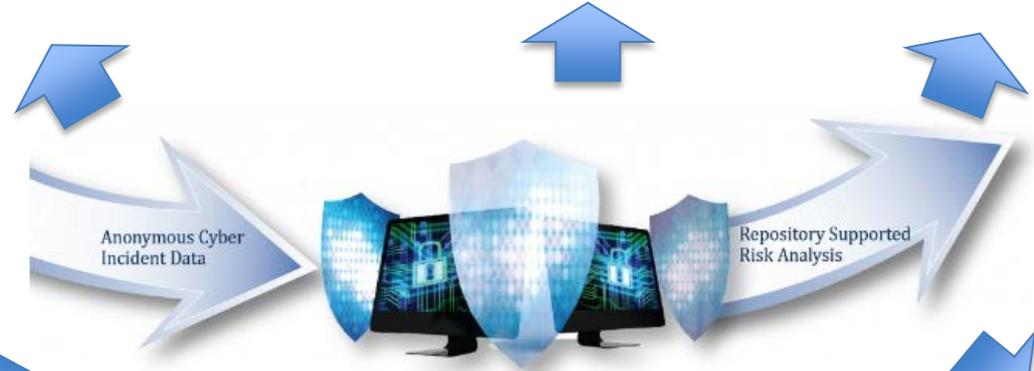
**Identifying Top Risks and Effective Controls**



**Informing Peer-to-Peer Benchmarking**



**Showing Return on Investment**



**Allowing for Sector Differentiation**



**Supporting Forecasting, Trending, and Modeling**



**Advancing Risk Management Culture**



## Challenges

## Solutions

### Legal/Policy

- Non-Disclosure Agreements
- Terms of Service
- Safe Harbor Legislation

### Design

- Sequential or randomized alphanumeric identifier
- Two-server System
- Validations/Background checks
- ISO 27001-like compliance Requirements
- Architecture/database/OS Security reviews
- Response Plans

### Making The Business Case

- Engage ISACs, ISAOs, USG, existing info sharing platforms
- Executive summaries, technical presentations, training workshops, and public statements with targeted messaging by early adopters
- Internal outreach campaign
- Process tools, frameworks, guiding principles



# The 16 Data Points

## Data Points

Type of Incident

Severity of Incident

Use of a cyber security framework

Timeline

Apparent Goal

Contributing Causes

Security Control Decay

Assets Affected

Type of Impact

Incident Detection Techniques

Incident Response TTPs

Internal Skill Sufficiency

Mitigation Prevention Measures

Costs

Vendor Incident Support

Related Events



**Objective:** To identify cyber incident data categories that could be used to perform trend and other analyses by enterprise risk owners and insurers

*What data points would achieve the collective benefits identified in the Value Proposition?*

- Participants identified, developed, evaluated and consolidated more than 30 candidate data categories into 16, each tied to three or more of the six value proposition categories
- Language and priorities differ between communities—many compromises were agreed to in order to arrive at a single list
- Throughout, members balanced privacy needs, ease of data collection/reporting, and value of the data for analysis by both cybersecurity professionals and insurance underwriters

**Quantifying aggregate risk, primarily in terms of direct and indirect financial costs, and actions that might reduce those costs.**

- **“Impacts”** of a cyber incident include **losses and/or compromises** of various types.  
**“What was harmed?”**
- **“Severity”** of a cyber incident addresses the **relative scale or scope** of an incident within the context of the incident contributor’s industry and circumstances. This category captures the **scale/breadth of those impacts** relative to an organization’s capacity.  
**“How bad was the harm?”**
- **“Costs”** of a cyber incident represent the **quantifiable pay-outs** by the incident victims, insurers, suppliers, etc., required to “fix” those impacts  
**“What did it cost to identify, detect, respond, and recover from the incident, including costs incurred to protect against future recurrences?”**

- Focus on data categories that enable them to identify and prevent attacks
  - Avoid oversimplification of data categories
  
- Rejected a “Cybersecurity Maturity Indicator Index” data category
  - Lack of standardization across industry sectors
  - Self-assessments are time and labor intensive post – incident
  - Maturity does not correlate with ability to ward off attacks
  
- Data categories are framed as much as possible in information security terminology where feasible in order to help ensure standardization for better analysis.

# CIDAR Data Points Summary

#	Title	Submitter	Description
0	Incident Context	N/A	Generic (to protect privacy) company and incident information (industry sector, size, date of report, etc.) <b>Who else might look like you?</b>
1	Type of Incident	Insurers/ CISOs	Major category of attack in industry terms <b>What Happened? DDOS, ransomware, destructive WORM, etc.</b>
2	Severity of Incident	Insurers/ CISOs	Difficulty in stopping/controlling incident (e.g., Low-Med-High, 1-5, Mild-Catastrophic, etc) <b>How bad was it? Really bad, or pretty minor?</b>
3	Use of Cyber-Security Framework	CISOs	Does the affected organization use a cybersecurity framework? If so, how, and to what effect? <b>Generally speaking, how were you postured before the incident?</b>
4	Timeline	Insurers	Date of detection, date of effective control. Retroactive timeline of attack steps (if it can be established). <b>How did the incident/attack progress?</b>
5	Apparent Goal	Insurers	Financial, reputational, and operational value of assets <u>to attackers</u> . <b>What were the attackers after?</b>
6	Contributing Causes	Insurers/ CISOs	People/Processes/Technology failures relevant to incident (e.g., misconfiguration, insider, poor training, etc.). Includes 3d parties. <b>How did they get in? What weaknesses were exploited?</b>

# CIDAR Data Point Summary (cont'd)

#	Title	Submitter	Description
7	<b>Security Control Decay</b>	CISOs	If a relevant security control was present, why/how was it not effective? Assesses how security controls break down. <b>Specifically what controls failed and how?</b>
8	<b>Assets Affected</b>	Insurers	Points in the network and/or the business that were compromised (e.g., SCADA/ICS, business sys servers, 3d party systems, websites). <b>What did they hit?</b>
9	<b>Type of Impact</b>	Insurers/ CISOs	Total impacts on all affected, including 3d parties (e.g., infrastructure/cloud/application service providers, the target organization, suppliers, customers, employees). Identifies Aggregate Risk. <b>What were the effects?</b>
10	<b>Incident Detection Techniques</b>	CISOs	How was the compromise identified? E.g., Internally by IPS, custom script, analytics, etc., or Externally, by FBI, the attacker (extortion), outsourced security, IaaS/SaaS provider, etc.? <b>How did you find out?</b>
11	<b>Incident Response TTPs</b>	CISOs	What techniques were used to stop the attack? Were they effective? <b>How did you respond? Did that work?</b>



#	Title	Submitter	Description
12	<b>Internal Skill Sufficiency</b>	CISOs	Availability/sufficiency of in-house skills to quickly address incidents <b>Did you have what you needed to respond?</b>
13	<b>Mitigation/Prevention Measures</b>	Insurers/ CISOs	Actions taken to stop incident and prevent future occurrences. <b>What was the “final” fix?</b>
14	<b>Costs</b>	Insurers	Financial and other quantifiable costs incurred as a result of an incident, including mitigation, recovery, liability, and profit loss. <b>How much did it cost to clean up, in total?</b>
15	<b>Vendor Incident Support</b>	CISOs	Vendor behavior in assessing/resolving incidents, e.g.: unknowledgeable, indifferent, cooperative, helpful, hostile) <b>Were other involved parties helpful?</b>
16	<b>Related Events</b>	Insurers	Related activities that provide incident context (e.g., upcoming merger discussions, corporate policy publicity, product launch). <b>Was anything relevant going on at the time?</b>

One of the biggest challenges for repositories is the development of correct metrics and measurements that incentivize a broad array of stakeholders to make contributions. Break-out sessions will consider:

- What are the underlying data points in each data category?
- What cyber incident data points do organizations already track;
  - What additional data points should they be tracking for the purposes of the repository; and what would be the additional cost of tracking those new data points?
- Which data points are the easiest to automate and operationalize?
- Do the 16 data categories identified by the CIDAWG accurately reflect the needed data, which if anonymously shared into a repository, could be used to perform trend and other analyses by enterprise risk owners and insurers?

# Breakout Session Groups

## General Incident Information

- **Type of Incident** - High-level descriptor/“tag”
- **Apparent Goals** – Attacker motivation as suggested by assets targeted
- **Assets Compromised/Affected** - The points in a network and/or business where an incident and/or attack took place.
- **Related Events** - Related activities/events that may provide context

## Incident Response and Recovery

- **Incident Detection Techniques** - Techniques used to identify an incident and/or attack
- **Mitigation/Prevention Measures** - Actions to stop incidents and prevent future occurrences
- **Timeline** - Detection to effective control.
- **Vendor Incident Support** - Vendor behavior during the assessment and resolution of the incident

## Organizational Practices and Maturity

- **Use of Cyber Security Standards & Best Practices** Cyber risk management practices, procedures, and standards in place at the time of the incident
- **Specific Control Failure(s)** – If a security control was present, identifies why/how it was not effective
- **Incident Response Playbook** –The Action, methods, procedures, and tools used to respond
- **Internal Skill Sufficiency** – Availability/sufficiency of in-house skills to quickly address incidents

## Consequences and Impacts

- **Severity of Incident** - The relative scale or scope of an incident within the context of the industry
- **Type of Impact(s)** - Total impacts on all affected, including 3d parties. Identifies Aggregate Risk
- **Costs** - Financial and other quantifiable costs incurred as a result of an incident and/or attack.
- **Contributing Causes** – People/process/technology failures contributing to an incident