ENHANCING RESILIENCE THROUGH CYBER INCIDENT DATA SHARING AND ANALYSIS

This document enumerates and evaluates consensus data categories that enterprise risk owners and insurers could use to assess risks, identify effective controls, and improve cybersecurity culture and practice.
It is the second in a series of white papers.

Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository

September 2015

Table of Contents

Executive Summary 1
Introduction 3

Cyber Incident Data Categories 3
Contextual Data 4
Data Category #1: Type of Incident 6
Data Category #2: Severity of Incident 7
Data Category #3: Use of a Cyber Risk Management Framework 9
Data Category #4: Timeline 10
Data Category #5: Apparent Goal 12
Data Category #6: Contributing Cause(s) 13
Data Category #7: Specific Control Failure(s) 15
Data Category #8: Assets Compromised or Affected 16
Data Category #9: Type of Impact(s) 18
Data Category #10: Incident Detection Techniques 20
Data Category #11: Incident Response Playbook 21
Data Category #12: Internal Skills Sufficiency 22
Data Category #13: Mitigation/Prevention Measures 24
Data Category #14: Costs 25
Data Category #15: Vendor Incident Support 26
Data Category #16: Related Events 28
Excluded Data Categories: Maturity Indicator Index, Threat Attribution 29

Conclusion 30
Appendix A: Consolidated Data Categories and Values Table 31
Appendix B: Notional Cyber Incident Use Cases 46
Case #1: Machinery Meltdown 46
Case #2: Direct Deposit Profit 47
Case #3: Not-So-Random Ransom 48
Case #4: Confidence Lost 49
Case #5: Disaster Averted (Cyber Near Miss) 50

Executive Summary

The Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) has continued to facilitate discussions on the concept of a trusted cyber incident data repository among insurers, chief information security officers (CISOs), and other cybersecurity professionals within the framework of the Cyber Incident Data and Analysis Working Group (CIDAWG). After ascertaining the benefits of such a repository, captured in the recently published white paper titled, "*Enhancing Resilience Through Cyber Incident Data Sharing and Analysis: the Value Proposition for a Cyber Incident Data Repository,*" [1] the group identified a set of cyber incident data categories that could help deliver those benefits. Over the course of two months, the CIDAWG participants identified, developed, evaluated and consolidated nearly 30 candidate data categories into a concise list of 16, which notionally would form the basis of a future repository development effort.

This paper outlines each of those data categories that, if anonymously shared into a repository, could be used to perform trend and other analyses by enterprise risk owners and insurers. Such repository-supported analyses, conducted in strict accordance with all applicable legal and privacy requirements, could help both private and public sector organizations better assess cyber risks, identify effective controls, and improve their cyber risk management practices.

<u>The 16 data categories consist of:</u>

1. **Type of Incident** - High-level descriptor or "tag" (e.g., "Ransomware") to differentiate the incident for ease of reference, leaving the capture of specific technical details about the incident to other data categories.
2. **Severity of Incident** - The relative scale or scope of an incident within the context of the incident contributor's industry and circumstances.
3. **Use of Information Security Standards and Best Practices** - The cyber risk management practices, procedures, and standards compliance approaches that an organization had in place at the time of an incident.
4. **Timeline** - The date of detection of a cyber incident and the date of effective control.
5. **Apparent Goals** - The assets apparently targeted, implying their financial, reputational, and operational value to an attacker.
6. **Contributing Causes** - People, process, and/or technology failures contributing or otherwise relevant to an incident.
7. **Security Control Decay** - A set of circumstances where a security control, although present, did not operate effectively enough to withstand an incident.
8. **Assets Compromised/Affected** - The points in a network and/or business where an incident took place.
9. **Type of Impact(s)** - The specific effects of an incident on all affected parties.
10. **Incident Detection Techniques** - The techniques used to identify an incident, and their effectiveness.
11. **Incident Response Playbook** - The actions, methods, procedures, and tools used to respond to an incident and to bring it to a close, and their effectiveness.

[1] Department of Homeland Security, "Enhancing Resilience Through Cyber Incident Data Sharing and Analysis: The Value Proposition for a Cyber Incident Data Repository," (June 2015), *available at*: http://www.dhs.gov/cybersecurity-insurance.

12. **Internal Skill Sufficiency** - Availability and sufficiency of an organization's skills and capacity to quickly address and resolve incidents.
13. **Mitigation/Prevention Measures** - Actions taken to stop incidents and to prevent similar future occurrences.
14. **Costs** - Financial and other quantifiable costs incurred as a result of an incident.
15. **Vendor Incident Support** - Vendor behavior during the assessment and resolution of a cyber incident.
16. **Related Events** - Related activities that provide incident context.

In addition to the above, the notional repository would allow for the capture of generic information about a contributing organization in order to preserve its anonymity and privacy. It would capture, for example, the organization's industry sector and size as well as the dates of an incident report and any incident report updates submitted by the contributing organization.

This document builds on the value proposition white paper, which discussed six core benefits likely to arise from the voluntary sharing of data about both intentional and accidental cyber incidents. The CIDAWG has identified and aligned each of the 16 data categories to the six core values of an ideal repository, which include: (1) Identifying Top Risks and Effective Controls; (2) Informing Peer-to-Peer Benchmarking; (3) Showing Return on Investment; (4) Allowing for Sector Differentiation; (5) Supporting Forecasting, Trending, and Modeling; and (6) Advancing Risk Management Culture.

The CIDAWG's follow-on efforts will focus on the legal and privacy protections, anonymization approaches, and other characteristics that a trusted repository must have in order to establish it as a safe information sharing space. The CIDAWG also will address how a repository should be structured during an initial operating stage in order to support the kinds of analysis that cybersecurity stakeholders need to improve their cybersecurity postures.

Introduction

The probability of significant and frequent cyber incidents targeting businesses and industry has become more widely accepted in the wake of recent large-scale and highly publicized cyber attacks on several well-known retailers and industry sector giants. A systemic lack of actionable cyber incident data, however, has hindered efforts by insurers, CISOs, and other cybersecurity professionals to anticipate and address these cyber risks effectively through more informed cybersecurity insurance underwriting and organization-appropriate cyber risk mitigation investment.

Last year, insurance experts concluded that there would be significant value in establishing a legally-compliant, privacy-respecting, and trusted cyber incident data repository that enabled participants to conduct various kinds of cyber risk analysis.[2] They explained that this analysis could support better cyber risk assessments, enhanced cyber incident modeling and prediction, and more cost-effective and dynamic cybersecurity programs.

NPPD is committed to helping address the call for such a repository. In February 2015, it established the CIDAWG, in partnership with the Critical Manufacturing Sector Coordination Council, under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC). The group consists of insurers, CISOs, and other cybersecurity professionals representing a wide range of critical infrastructure sectors. After establishing six major value propositions for a repository, the CIDAWG turned its attention to the specific cyber incident data categories needed to attain that value. Those 16 data categories are the subject of this white paper.

Cyber Incident Data Categories

Over the period of two months, CIDAWG participants discussed specific data categories that are essential for meaningful analysis of a wide range of cyber incidents. As the result of several meetings, the working group:

- identified each data category by name;
- defined the intent of each data category;
- developed consistent input fields for each data category; and
- deliberated on how data within each category, if shared, aggregated, and analyzed, would be useful for improving cyber risk management practices.

The input fields included in this report are for illustrative purposes only. They are not comprehensive and are intended only to clarify the kinds of data points that each data category would likely encompass. Based on public feedback to this report, the CIDAWG will flesh out the input fields through additional and modified entries, as necessary, as part of its future discussion about how a repository should be structured to function effectively during an "alpha" stage of operations.

CIDAWG participants also identified potential conceptual overlaps between the "impacts," severity," and "costs" data categories. They attempted to resolve these overlaps by clarifying the definitions of those categories as follows:

- **"Impacts"** of a cyber incident include **losses and/or compromises** of various types (e.g., lives, system integrity/function, reputation, money, Intellectual Property (IP)/Personally Identifiable Information (PII) data) attributable to the incident – in short, the incident's immediate and

[2] *See* U.S. Department of Homeland Security Cybersecurity Insurance webpage and Cybersecurity Insurance Workshop Readout Reports, *available at* http://www.dhs.gov/publication/cybersecurity-insurance.

cascading consequences. The "impacts" data category asks contributors to explain, "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. While the specific types of impact (e.g., financial, environmental, or humanitarian losses) will vary by industry and circumstance, this category captures the **scale/breadth of those impacts** (e.g., on a scale of 1-5) relative to an organization's capacity. The "severity" data category asks contributors, "How bad was the harm?"

- **"Costs"** of a cyber incident represent the money required to "fix" those impacts (e.g., remediation, liability, other types of compensation (lost wages/profits), reconstruction, manpower, notification and monitoring, forensics). Stated differently, these costs include quantifiable pay-outs by the incident victims, insurers, and suppliers. The "costs" data category asks contributors, "What did it cost to identify, detect, respond, and recover from the event, including costs incurred to establish mechanisms to protect against future recurrences?"

Regarding these and other data categories pertaining to the evolution of a cyber incident, CIDAWG participants repeatedly identified the need for a mechanism through which a contributing company could supplement an original cyber incident report. They explained that most cyber incidents evolve over weeks or months through a series of phases and steps. Moreover, evidence from forensic back-tracking and analysis often emerges over time, as may the full consequences or impacts of an event. New information accordingly may require periodic updates to several categories of contributed information, such as an incident's assessed severity and costs.

Finally, in addition to these 16 data categories, the CIDAWG also carefully considered including a "Cybersecurity Maturity Indicator Index" data category for sharing into a repository. CIDAWG participants ultimately decided to exclude such a data category at this time. Their concerns included the lack of standardization across industry sectors in sector-mandated maturity models; the time-and labor-intensive nature of a detailed self-assessment in a post-incident environment; and the observation that maturity does not necessarily correlate with a company's ability to ward off attacks – particularly given the fact that large, well-resourced and mature companies are precisely those that are likely to be targeted by the most sophisticated attacks. CIDAWG participants concluded that the perceived value of a "maturity" data category instead could be achieved through careful development of other data categories, such as internal skill sufficiency, use of cybersecurity best practices and detection/response timelines and techniques. The discussions surrounding these categories are summarized in greater detail in this white paper.

Contextual Data: "Who Else Might Look Like the Affected Organization?"

Definition:

Background information about the contributing organization intended to facilitate comparative analytics while preserving anonymity and privacy.

This data category captures generic information about a contributing organization in order to preserve the anonymity and privacy of the organization. It captures, for example, an organization's industry sector and size as well as the date of an incident report and any updates submitted by the contributing organization. Because repository participation would be voluntary, a contributing organization could decline to contribute any contextual data that it considered "identifying."

Consistent Input Field Examples:

What is your main industry sector?

- ☐ Defense Industry
- ☐ Financial Services
- ☐ Healthcare
- ☐ Biotech/Pharmaceutical
- ☐ Food Production/Distribution
- ☐ Utilities (water, power, etc.)
- ☐ Transportation/port services
- ☐ Technology
- ☐ Energy Production (oil, natural gas, etc.)
- ☐ R&D/University
- ☐ Manufacturing
- ☐ Other _____

Does your organization consider itself to be a small, small-medium, medium-sized, or large business?

- ☐ Small Business (less than 100 employees)
- ☐ Small-Medium Business (100-999 employees)
- ☐ Medium-sized Business (1,000-9,999 employees)
- ☐ Large Business (10,000 employees or more)
- ☐ Decline to Answer

How long has your organization been dedicating resources to cybersecurity?

- ☐ Started within the last year
- ☐ 1-3 years
- ☐ 3-5 years
- ☐ More than 5 years

Does your organization have someone responsible for cybersecurity/information security, such as a CISO (Chief Information Security Officer) or Chief Security Officer (CSO)? (Yes / No)

Did your organization have someone responsible for cybersecurity/information security, such as a CISO (Chief Information Security Officer) or Chief Security Officer (CSO), at the time of the incident? (Yes / No)

Value Discussion:

CIDAWG participants noted that the desired cross-industry nature of a cyber incident data repository, combined with the commitment by all parties to privacy and anonymization, creates a need for non-identifying contextual data about the organizations that contribute incident reports. This basic contextual information will:

- Allow for “apples-to-apples” comparisons across organizations that could help them draw analytical conclusions relevant to their own risks;
- Facilitate data searches and analysis on a sector-by-sector or other characteristic basis; and
- Support cyber incident trend modeling that could inform cyber risk forecasts.

Data Category #1: Type of Incident – "Major Category: DDOS? SCADA Attack?"

Definition:

A high-level descriptor or "tag" (e.g., "Ransomware" or "SCADA attack," as opposed to "Malware"), to differentiate the incident for ease of reference, leaving the capture of specific technical details about the incident to other data categories.

This data category is intended as a plain language descriptor or "tag" that differentiates the incident and helps other organizations determine its applicability to their own situations. It is not intended to be technically precise, but to provide "at-a-glance" summary insight into the nature of the incident. More technically precise taxonomies pertaining to specific incident attributes such as attack targets and methods are captured in separate data categories below.

Consistent Input Field Examples:

Please identify the major category description that best fits this incident. Check all that apply:

- ☐ Distributed Denial of Service (DDOS)
- ☐ Destructive WORM
- ☐ Ransomware/Extortion
- ☐ Data Theft
  - ☐ Intellectual Property (IP)
  - ☐ Personally Identifiable Information (PII)
  - ☐ Financial Data
  - ☐ Health Records
  - ☐ Other type of data _____
  - ☐ Unknown
- ☐ Web page defacement
- ☐ Malware

  (Variant, if known_____)
- ☐ Zero-Day Malware Attack
- ☐ SCADA or Industrial Control System Attack
- ☐ Accident/Human Error
- ☐ System Failure
- ☐ Natural or Man-made (Physical) Disaster
- ☐ Storage/Back-up Failure
- ☐ Network Intrusion
- ☐ Third-Party Event
- ☐ Phishing
- ☐ Industrial Espionage
- ☐ Physical Sabotage
- ☐ Configuration Error
- ☐ Insider Attack
- ☐ Lost Device
- ☐ Outage
- ☐ Other
- ☐ *Additional Entry . . .*

Value Discussion:

- By cross referencing incident type against additional data (e.g., industry sector, geographic area, end target, connection to third parties), underwriters could assess whether correlations or trends exist with regard to types of incidents in or across industry sectors. This information could help underwriters identify those sectors that have high versus low hazard exposure – knowledge that is the "fundamental currency" of the insurance market.
- Along with other incident factors, CISOs and other cybersecurity professionals could draw inferences from individual attack scenarios to help them track attacker tactics, techniques, and procedures (TTPs) within an industry sector.
- Aggregated over time, "Type of Incident" data could help highlight trends in the evolving attack landscape and possibly help associate a pattern of attacks with a larger "campaign" – e.g., a broad effort by a crime syndicate to acquire data that could be used to perpetuate credit fraud.
- Analysis that indicates an increased likelihood of particular types of incidents in a given industry sector could help companies take appropriate preventative measures. For example, it might be valuable for organizations experiencing a DDOS attack to know that such attacks often are used as cover for another, more destructive, attack. Such understanding could prompt organizations to look more closely at other parts of their operations that might be targeted.
- Awareness of attack trends could help CISOs and other cybersecurity professionals focus their organizations' internal risk awareness training – for instance, by issuing timely alerts about and examples of spear phishing emails.

Data Category #2: Severity of Incident – "On a Scale of 1 to X, How Bad Was the Harm?"

Definition:

The relative scale or scope of an incident within the context of the incident contributor's industry and circumstances.

While the specific types of impact (e.g., financial, environmental, or humanitarian losses) will vary by industry and circumstance, this data category captures the magnitude of those impacts (e.g., on a scale of 1-5) relative to an organization's capacity. Whereas other data categories specify what was harmed, the "Severity of Incident" data category asks, "How bad was the incident?"

This data category is envisioned as a single scalar input field such as 1-5, Low-Medium-High, or Mild-Moderate-Catastrophic. Because "severity" is an inherently subjective value based on the industry, relative size, and other circumstances of the contributing organization, the CIDAWG recommended that sample severity scales be made available – for instance, as "pull-down tables" specific to particular industries/business categories – in order to help contributors determine the appropriate input value. The tables below are drawn from examples used in particular industries, and are intended to be merely representative of the kinds of tables contributors could access in order to determine the severity input value appropriate to their incident and circumstance.

Industry-Specific Severity Scale Examples:

Example 1

Consequence									
	Risk area								
	Business continuity planning		Information security			Industrial operation safety		Environmental safety	National impact
Category	Manufacturing outage at one site	Manufacturing outage at multiple sites	Cost (million USD)	Legal	Public confidence	People – on-site	People – off-site	Environment	Infrastructure and services
A (high)	> 7 days	> 1 day	> 500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional or national agency or long-term significant damage over large area	Impacts multiple business sectors or disrupts community services in a major way
B (medium)	> 2 days	> 1 hour	> 5	Misdemeanor criminal offense	Loss of customer confidence	Loss of workday or major injury	Complaints or local community impact	Citation by local agency	Potential to impact a business sector at a level beyond that of a single company. Potential to impact services of a community
C (low)	< 1 day	< 1 hour	< 5	None	None	First aid or recordable injury	No complaints	Small, contained release below reportable limits	Little to no impact to business sectors beyond the individual company. Little to no impact on community services

Example 2

Impact	Financial or Asset Loss	Time-to-Market Delay	Product Quality	Environment	Health & Safety	Legal
5	> 20% sales or >$10M	6 months	• Potential severe effect on health and safety • Global product recall	• Environmental disaster • Chronic/ Perm-anent damage	• Fatality or adverse permanent health effects	• Potential imprisonment • Huge fines • Prolonged/multiple litigations
4	11% - 20% sales, or $1M - $10M	3 months	• Potential significant health/safety effects • National product recall	• Significant environmental damage > 1 yr	• Injury or illness causing prolonged impairment	• Potential criminal prosecution • Significant fines • Litigation
3	6% - 10% sales, or $100K-$1M	1 month	• Potential minor effect on health and safety • Product recall from more than one market	• Temporary / Recoverable environmental damage < 1 yr	• Injury or illness requiring medical attention and lost time/job restriction	• Investigations • Fines • Possible litigation
2	1% - 5% sales or $10K-100K	1 week	• Possible effect on health and safety • Product recall from single market	• Limited, Localized environmental damage	• Injury or illness requiring medical attention but no lost time	• Inquiries • Potential fines • Individual civil actions
1	< 1% sales or <$10K	1 day	• No effect on health or safety • No product recall	• Negligible or no environmental effect	• No effect on health or safety	• Minimal legal issues • No fines • No actions

Value Discussion:

Severity forecasting – encompassing data loss, environmental impacts, operational impacts, and physical hazards – is a key aspect of cyber risk underwriting. In conjunction with other data, this information could:

- Help insurers design and differentiate kinds and amounts of meaningful cybersecurity insurance for an industry sector by cross referencing the severity of impacts from specific types of events that the sector experiences with those experienced by other sectors;
- Assist CISOs and other cybersecurity professionals in making cost-benefit cases for cybersecurity investments to senior leaders – specifically, by helping them frame the value of those investments in terms of impact to key business areas as informed by the experiences of similarly situated organizations; and
- Raise awareness of cybersecurity risks as enterprise risks.

Data Category #3: Use of a Cyber Risk Management Framework – "Generally Speaking, How Was an Organization Postured Before an Incident?"

Definition:

The cyber risk management practices, procedures, and regulations and standards compliance approaches that an organization had in place at the time of an incident.

This data category could include consistent input boxes that list the best practices, procedures, regulations and standards compliance approaches – and any overarching frameworks – that an organization has implemented and their corresponding dates of first implementation.

Consistent Input Field Examples:

- Does your organization use a cyber risk management framework, best practice, regulation or standard as part of its cyber risk management activities? ☐ Yes ☐ ☐ No

  If Yes, please identify: _____

- If you are required to be certified compliant with a technical regulation or standard, how are you assessed?

  ☐ Self-Assessed

  ☐ Self-Assessed with Third-Party Validation

  ☐ Third-Party Assessment and Validation

  ☐ Post-Market Surveillance

  ☐ N/A: Not Required

- Are your organization's risk management practices formally approved and expressed as policy?

  ☐ Yes ☐ No

- Are your organization's cybersecurity practices regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape? ☐ Yes ☐ No

- Is cybersecurity integrated into your organization's enterprise risk management? ☐ Yes ☐ No

Does your organization define risk-informed policies, processes, and procedures?
Yes ☐ No ☐

- If Yes, are they implemented as intended ☐ Yes ☐ No
- Are they reviewed? ☐ Yes ☐ No

- Does your organization have methods in place to respond effectively to changes in risk?
  ☐ Yes ☐ No
- Do your organization's personnel possess the knowledge and skills to perform their appointed roles and responsibilities? ☐ Yes ☐ No
- Does your organization understand its dependencies and partners and receive information from partners that enable collaboration and risk-based management decisions within your organization in response to events? ☐ Yes ☐ No

Value Discussion:

While several CIDAWG participants expressed interest in determining whether adherence to a particular framework's best practices, procedures, and standards correlates with decreased cybersecurity risks, many were concerned about standardization: several industry sectors mandate their own framework, and certain common ones are not acceptable to foreign company owners, investors, or regulators. Other participants explained that for small companies that don't already adhere to certain best practices, procedures, regulations, or standards, being required to do so in order to obtain insurance could be both burdensome and prohibitively expensive. This might lead them to accept the risk of remaining uninsured. After considerable discussion, however, the CIDAWG concurred that the potential value of the analysis that this data category could support warranted its inclusion – so long as the needed information is captured through a series of high-level checkboxes. Participants agreed that the sharing, aggregation, and analysis of this information could:

- Enable "apples-to-apples" comparisons among different types of organizations using the same framework or similar organizations using different frameworks;
- Help identify the effectiveness of a particular framework's best practices, procedures, regulations, and standards as implemented by organizations within specific sectors;
- Over time, help forecast when an effective framework is about to become obsolete; and
- Encourage organizations to utilize "proven" frameworks as components of their broader enterprise risk management efforts.

Data Category #4: Timeline – "How Did the Incident Progress?"

Definition:

The date of detection of a cyber incident and the date of effective control.

This data category would capture retroactive timelines of incident phases and steps if they can be established. Because information about the full profile of a sophisticated attack tends to emerge over time, this data category will accordingly require that a repository include a mechanism through which contributing organizations can access and update their original timeline submissions – without compromising their anonymity or privacy – as incident investigations progress. This data category

likewise relates directly to Data Category 6, "Contributing Causes." The incident progression steps identified in that data category could not only help illuminate evolving attack methodologies of concern there but also provide "Timeline" information relevant here.

Consistent Input Field Examples:

What is the interval between initial cyber intrusion to target or significant system compromise (including data records compromise)?

- ☐ Less than 4 hours (almost immediate)
- ☐ 4-24 hours (less than a day)
- ☐ 2-7 days (less than a week)
- ☐ 7-30 days (more than a week, but less than a month)
- ☐ 30-180 days (between 1 and 6 months)
- ☐ 180 days-365 days (6 months to a year)
- ☐ More than a year
- ☐ Unknown (initial date of intrusion, and/or system compromise undetermined

What is the interval between *compromise* and *detection* of the incident's effects?

<Similar time interval options>

What is the interval between *detection* of the incident and *containment/mitigation*?

<Similar time interval options>

Value Discussion:

Time-to-detection data may be uninformative at best and misleading at worst for cyber risk management purposes. Many cyber attacks are clumsy and sometimes targeted organizations get lucky in detection. Conversely, even very competent cybersecurity operations can fail to detect a sophisticated attack. Furthermore, many cyber attacks develop over weeks or months, and the date of the original compromise may never be established. The CIDAWG participants nevertheless concurred that a timeline of the entire course of an attack would be useful, if it can be determined, because:

- The ability or inability of an organization to quickly get an incident under control once discovered can highlight the effectiveness or ineffectiveness of its controls, including its key processes;
- In conjunction with other factors gleaned from detection methods and attack patterns, time-to-control data can indicate the sophistication of an attack and the relative maturity of the impacted organization;
- Consistent variations in time-to-control data among industry sectors can highlight sector-specific cybersecurity strengths and weaknesses such as might be introduced by sector-unique SCADA and other industrial control systems; and
- Cyber attacks aimed at collecting data over an extended period of time often are the "larger" events when it comes to intellectual property theft or other espionage – categories of loss into which insurers often lack visibility. This data could potentially help insurers develop new or expanded insurance coverage options.

Data Category #5: Apparent Goal – "What Were the Attackers After?"

Definition:

The assets apparently targeted, implying their financial, reputational, and operational value to an attacker.

This data category identifies the assets that appear to have been targeted for destruction, disruption, theft, disclosure, or other action contrary to an organization's interests – that is, an attacker's apparent motivation or desired outcome for the attack. While theft of private or intellectual property data has featured prominently in many well-publicized attacks, attacker motives may also include disruption of system or service availability, harm to company reputation (through exposure or defacement), extortion (as with ransomware), or physical destruction. This data category accordingly could include consistent input fields such as "Disruption of System/Service Availability," "Degradation of Reputation," and "Acquisition/Theft (e.g., theft of IP or PII)".

Consistent Input Field Examples:

What was the attacker's apparent end-state goal? Check all that apply.

- ☐ Acquisition/Theft – Illicit acquisition of valuable assets for resale or extortion in a way that preserves the assets' integrity but may incidentally damage other items in the process.
- ☐ Business Advantage – Increased ability to compete in a market with a given set of products. The goal is to acquire business processes or assets.
- ☐ Technical Advantage – Illicit improvement of a specific product or production capability. The primary goal is to acquire production processes or assets rather than a business process.
- ☐ Damage to Property – Injury to the target organization's physical/electronic assets, or intellectual property.
- ☐ Bodily Injury/Death – Injury to or death of the target organization's personnel.
- ☐ Denial – Prevent the target organization from accessing necessary data or processes.
- ☐ Disruption of System/Service Availability – Interference with or degradation of the target organization's legitimate business transactions.
- ☐ Production Loss – Reduction or halting of the target organization's ability to create goods and services by damaging or destroying its means of production.
- ☐ Environmental Harm – Adverse impact to land, air, or water resources.
- ☐ Degradation of Reputation – Public portrayal of the target organization in an unflattering light, causing it to lose influence, credibility, competitiveness, or stock value.
- ☐ Unknown – Intent of the attack is not known.
- ☐ Not Applicable – Attack does not appear to have been an intentional/hostile incident.
- ☐ *Additional Entry . . .*

Value Discussion:

An attacker's motivation sometimes will be evident or even stated. When this is not the case, the type and volume of data compromised, and what is done with it afterward (e.g., sold, used for espionage, released to the public, used in future attack), can imply the attacker's goals. Understanding those goals:

- Helps organizations better assess their risks by determining whether their assets align with the apparent goals of attackers targeting their sector;
- Helps insurers identify not only the risks that may be unique or common to a particular industry sector but also what controls are or are not effective in mitigating those risks;
- In combination with Data Category 1, "Type of Incident," and Data Category 16, "Related Events," helps organizations forecast increased risk of attacks – and potentially the methodologies of those attacks – on the basis of circumstances such as policy announcements, corporate organizational changes, or shifting political/media focus pertinent to a particular sector; and
- Improves corporate cybersecurity culture through timely alerts and training tailored to rising threats, reinforced with analysis that draws on the examples of similarly situated peers.

Data Category #6: Contributing Cause(s) – "How Did the Incident Happen" or "How Did the Attacker Do It?"

Definition:

People, process, and/or technology failures contributing or otherwise relevant to an incident.

This data category seeks to identify the multiple contributing causes that, over the course of several cyber incidents, could reveal attack patterns that could inform cybersecurity risk assessments. It should include consistent input fields for both contributing organization and related third-party provider control failures during each step of an incident's progression such as "Insider," "Poor Training," "Unpatched System," "Misconfigured Control," and "Zero-Day Exploit." The inclusion of time interval information via drop-down menus for each step, similar to what is used in Data Category 4, "Timeline," could further illuminate incident progression as well as provide additional insight into Data Category 4, "Timeline." Such notional pull-down interval menus are denoted in the table below by boxes.

Consistent Input Field Examples:

Incident Progression		Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Contributing Cause/Control Failure	Intentionally caused or conducted by third party vendor	☐	☐	☐	☐	☐	☐
	Unintentionally/negligently introduced through third party information sharing partner (e.g., link to an infected site, or poor protection of shared materials)	☐	☐	☐	☐	☐	☐
	Third party vendor infrastructure (e.g., remote access connection)	☐	☐	☐	☐	☐	☐
	Third party vendor account credentials	☐	☐	☐	☐	☐	☐
	Data was under third party control when compromised	☐	☐	☐	☐	☐	☐
	Direct access by Insider	☐	☐	☐	☐	☐	☐
	Physical access by unauthorized personnel	☐	☐	☐	☐	☐	☐

	Spear phishing email attachment	☐	☐	☐	☐	☐	☐
	Spear phishing email link	☐	☐	☐	☐	☐	☐
	Poor Passwords	☐	☐	☐	☐	☐	☐
	Stolen Authorized Credentials	☐	☐	☐	☐	☐	☐
	Employee Human Error in authorized procedure (e.g., distracted/multitasking, inadequate training)	☐	☐	☐	☐	☐	☐
	Employee Human Error – unauthorized/reckless activity (system or authorization misuse, benign shortcuts, etc.).	☐	☐	☐	☐	☐	☐
	Improper sensor tuning	☐	☐	☐	☐	☐	☐
	Malicious Insider Activity	☐	☐	☐	☐	☐	☐
	Unauthorized Device (e.g., personal laptop)	☐	☐	☐	☐	☐	☐
	Misconfigured Device (firewall, router, switch)	☐	☐	☐	☐	☐	☐
	Compromised mobile media (e.g. USB)	☐	☐	☐	☐	☐	☐
	Compromised firmware	☐	☐	☐	☐	☐	☐
	Known vulnerability not patched	☐	☐	☐	☐	☐	☐
	Previously unknown vulnerability	☐	☐	☐	☐	☐	☐
	Brute Force attack	☐	☐	☐	☐	☐	☐
	Virus w/ A/V	☐	☐	☐	☐	☐	☐
	Virus - No A/V	☐	☐	☐	☐	☐	☐
	Zero-Day	☐	☐	☐	☐	☐	☐
	Additional Entry…	☐	☐	☐	☐	☐	☐
	Other:						

Value Discussion:

CIDAWG participants repeatedly raised concern about the difficulty in meaningfully identifying all contributing causes of a particular cyber incident. They noted that the ultimate root cause of most attacks is a poor security practice by "the clicker," or user. Once attackers gain an initial foothold, they exploit other weaknesses in the target network architecture. Sometimes, attackers take weeks to compromise one intermediate system after another until they reach their objective. While CIDAWG participants agreed that identifying all incident causes is often difficult, they nevertheless concluded that characterizing the entire attack lifecycle could support extremely valuable analysis that would:

- Help identify new attack methodologies and, in conjunction with Data Control 7, "Specific Control Failure(s)," highlight what controls are or have become ineffective;
- Identify all the various points in an architecture that different types of attacks exploit;
- Help illuminate cybersecurity concerns associated with third-party providers;
- Help CISOs and other cybersecurity professionals make a case for return on specific cybersecurity investments by reinforcing the merits of various cybersecurity protections that an organization has in place and, conversely, the increased risks an organization may face if it foregoes upgrading to more appropriate controls;

- Identify sector-unique concerns associated with particular classes of systems;
- Incentivize organizations to employ appropriate risk controls, including investments in internal cybersecurity processes and training; and
- Help show whether similar attacks on multiple organizations are connected by enabling the identification of attack patterns. Framing an attack in light of a broader campaign can be enlightening to a company's leadership, spurring investment in more effective controls.

Data Category #7: Specific Control Failure(s) – "Exactly What Failed and How?"

Definition:

A set of circumstances where a security control, although present, did not operate effectively enough to withstand an incident.

For mature cybersecurity organizations especially, successful incidents often reflect not the absence of security controls but instead situations in which in-place defenses that operational experience or industry standards suggest should be adequate nevertheless are circumvented or overwhelmed by a determined attacker. This data category focuses on the ways in which control mechanisms – involving people, processes, and/or technologies – fail.

Consistent Input Field Examples:

Consistent input fields for this data category could include a list of standard security controls, along with various selection options such as "Poor Internal Security Processes," "Approaches/Tools Incompatible with All Platforms," a particular control that "Failed Open," "Improperly Tuned Sensor(s)," "Inadequate Maintenance/Patching Practices," and "Working Control/Failed to Prevent Incident and/or Attack."

Please identify the category of the involved security control as well as descriptors of the failure. Check all that apply:

Type of Security Control:

- ☐ Human
- ☐ Process
- ☐ Technology
- ☐ Environmental (e.g., facility power, cooling, natural disaster, etc.)
- ☐ Third Party

Level of Security Control:

- ☐ Network
- ☐ Business/Process Application
- ☐ System Control (SCADA/ICS)
- ☐ Data

Descriptor of the Failure:

- ☐ Poor Internal Security Processes
- ☐ Approaches/Tool Incompatible with All Platforms
- ☐ Improperly Tuned Sensor(s)
- ☐ Inadequate Maintenance/Patching Practices
- ☐ Working Control Failed to Prevent Incident and/or Attack
- ☐ Other _____
- ☐ *Additional Entry . . .*

Value Discussion:

Repository-supported analysis of this data category could:

- Highlight changes in technology effectiveness over time, which would give CISOs and other cybersecurity professionals time to augment or change security provisions within their organizations and help insurers appropriately incentivize the adoption of more effective controls;
- Identify industry sector-related differences in control effectiveness, boosting underwriter knowledge about risks inherent in particular sectors;
- Help identify candidate technologies and processes that could improve risk management by facilitating comparisons of controls among sectors with similar deployed technologies (e.g., SCADA and other industrial control systems);
- In those situations in which a control failure is based on improper employment –
    - Help insurers assess the relative security maturity of a particular industry sector and incentivize improvements; and
    - Support CISOs and other cybersecurity professionals in addressing internal process and training shortfalls;
- Help promote the forecasting of control "lifecycles" that could inform the work of not only insurers, CISOs, and other cybersecurity professionals but also cybersecurity product developers. For example, objective analysis that shows that existing technology is "aging out" could enable CISOs to make the business case to their leaders for spending on technology upgrades; and
- Along with cost and impact data, demonstrate return on cybersecurity investment in terms of loss avoidance by highlighting cyber risk management failures within similarly situated organizations.

Data Category #8: Assets Compromised or Affected – "What Got Hit?"

Definition:

The points in a network and/or business where an incident took place.

This data category focuses on what assets were implicated, and how, during a cyber incident. Potential points of compromise could encompass people, processes, and/or technologies and may include cascading compromises to secondary, incidental, and third-party assets. The goal of this data category is to capture aggregate exposure and not impact (defined below as harm), because assets compromised during an incident might not experience actual harm.

Consistent Input Field Examples:

This data category could include a combination of consistent input fields regarding where an incident took place – such as a SCADA or other industrial control system, database, individual account(s), business application server, or third-party system. They could include short narrative spaces that contributors could use to describe specific compromise(s) pertaining to the affected asset.

Please identify all assets that were affected by the compromise. Check all that apply:

- ☐ SCADA/ Industrial Control Systems (ICS)
- ☐ Databases
- ☐ Individual Accounts
- ☐ Business Application Servers
- ☐ Third Party Systems
- ☐ Websites (e.g., defacement)
- ☐ Structured Data (e.g., application/relational databases)
- ☐ Unstructured Data (e.g., office/individual's files, PDFs, blueprints)
- ☐ Transactional Systems
- ☐ Decision Support Systems (including data warehouses)
- ☐ Building Management Systems
- ☐ Peripheral (e.g., USB, external hard drive)
- ☐ End-User Device (e.g., stolen iPad, phone, laptops)
- ☐ Data Center/Office Device (e.g., server, storage array, printer)
- ☐ Printed Hardcopy
- ☐ Other
- ☐ *Additional Entry . . .*

Value Discussion:

This data category could prove essential for enhancing understanding of both the immediate and long-term effects of cyber incidents, and informing appropriate responsive cyber risk management investments, by:

- Identifying what assets within network architectures are typically compromised, and how, in order to better identify appropriate controls;
- Modeling critical dependencies in real-world cyber events. Such dependencies are of particular concern to insurers because they may cover more than one party affected by a given cyber event (e.g., when partnering companies merge multiple supply chains, or when one application vendor supports several insured clients that each have their own customer databases);
- Boosting the insurer case for incentivizing supplier and vendor cybersecurity controls – such as segmentation, encryption, or secure vendor interfaces – by showing the cascading effects from a particular kind of cyber incident to be a frequent and/or likely occurrence within a particular industry sector;
- Helping CISOs and other cybersecurity professionals explain cyber incident "chains of events." For example, analysis of affected asset information, together with Data Category 4, "Timeline," and Data Category 6, "Contributing Causes," information, could show how hackers in a particular instance (1) compromised an administrator account to steal credentials; (2) used the credentials to compromise financial records on a vendor application server; and then (3) stole bank account information in a public cloud database; and
- Encouraging corporate discussions about cybersecurity risks inherent in particular business decisions, such as the selection of third-party provider applications.

Data Category #9: Type of Impact(s) – "What Was Harmed?"

Definition:

The specific effects of an incident on all affected parties.

Whereas Data Category 8, the "Assets Compromised or Affected," focuses on what assets were affected, this data category addresses how they were affected – in short, the actual harm incurred by the victim(s) during each step of an incident. This data category extends beyond impacted or targeted organizations to include third-party providers as well as downstream parties such as employees and customers. The consistent input fields for this data category should include the generic identities of affected parties by category (e.g., the organization contributing the incident report and its Infrastructure- and Software-as-a-Service (IaaS/SaaS could and application provider)); the impacts they suffered (e.g., "Production Loss," "Damage to Property," "Bodily Injury/Death," and "Environmental Harm"); and the step of the incident when those impacts occurred. The goal of this data category is to further illuminate aggregate risk by identifying aggregate effect.

Consistent Input Field Examples:

Check all that apply:

What is the cybersecurity industry category affected? Check all that apply:

- ☐ Loss of confidentiality
- ☐ Loss of integrity
- ☐ Loss of availability

What is the amount of data compromised?

- ☐ 0-100,000 records/documents
- ☐ 100,001-500,000 records/documents
- ☐ 500,001-1,000,000 records/documents
- ☐ Over 1,000,000 records/documents
- ☐ Not Applicable

What is the duration of the experienced business interruption and/or outage?

- ☐ Less than one hour
- ☐ 1-3 hours
- ☐ 3-10 hours
- ☐ 10-24 hours
- ☐ 1-3 days
- ☐ 3-6 days
- ☐ Greater than one week

What is the sensitivity of the data involved? Check all that apply:

- ☐ Personally Identifiable Information (PII)
- ☐ Protected Health Information (PHI)
- ☐ Intellectual Property (IP)
- ☐ Credit Card Data
- ☐ Consumer Financial Data
- ☐ Employee Data
- ☐ Business Process Data (e.g., logistics information, trade secrets)
- ☐ Biometric Data
- ☐ Corporate Confidential Information
- ☐ Personal Confidential Information (e.g., an individual's emails)
- ☐ Other _____
- ☐ Not Applicable
- ☐ *Additional Entry . . .*

What was the actual outcome of the attack? Check all that apply:

- ☐ Acquisition/Theft – Illicit acquisition of valuable assets for resale or extortion.
- ☐ Business Advantage – Increased ability to compete in a market with a given set of products.
- ☐ Technical Advantage – Illicit improvement of a specific product or production capability.
- ☐ Damage to Property – Injury to the target organization's physical or electronic assets, or intellectual property.
- ☐ Bodily Injury/Death – Injury to or death of the target organization's personnel.
- ☐ Denial – Prevention of the target organization's access to necessary data or processes.
- ☐ Disruption of System/Service Availability – Interference with or degradation of the target organization's legitimate business transactions.
- ☐ Production Loss – Reduction or halting of the target organization's ability to create goods and services by damaging or destroying its means of production.
- ☐ Environmental Harm – Adverse impact to land, air, or water resources.
- ☐ Degradation of Reputation – Public portrayal of the target organization in an unflattering light, causing it to lose influence, credibility, competitiveness, or stock value.
- ☐ No Apparent Impact – No impact has been detected or it is confirmed that the attack had no impact.
- ☐ *Additional Entry . . .*

Value Discussion:

A single cyber incident can have multiple types of effects at different steps in its evolution – for instance, service interruptions at one point in an ecosystem network; data loss or destruction elsewhere; and financial losses in yet another area. Characterizing these effects, and how they propagate or "cascade" across organizational and functional boundaries, could:

- Help establish the range of potential cascading impacts from a particular type of cyber incident within a certain industry sector by benchmarking impact data across peer organizations;
- Support cybersecurity budget and investment recommendations, when analyzed in conjunction with Data Category 7, "Specific Control Failure(s)," and Data Control 10, "Incident Detection Techniques";
- Help insurers design and differentiate the kinds and amounts of cybersecurity insurance coverage that they could or should offer across different industry sectors and circumstances;
- Inform analysis that helps organizations evaluate business decisions that give rise to aggregate risk – for instance, when they contemplate shifting portions of their operations to the cloud; and
- Provide a broad corporate context that empowers cybersecurity professionals to frame cybersecurity as an inherent part of enterprise risk management.

Data Category #10: Incident Detection Techniques – "How Did the Affected Organization Find Out?"

Definition:

The techniques used to identify an incident, and their effectiveness.

This data category could include input fields for internal detection techniques such as "Tool/Process Intrusion Prevention System (IPS)," "Custom Script," and "Analytics." It likewise could include input fields for describing external detection and notification such as by the "FBI, United States Secret Service, Other Law Enforcement Entity," "Attacker" (in extortion situations), "Outsourced Security," and/or "IaaS/SaaS Provider." This data category also could include input fields that address the scale of detection technique effectiveness, such as "Not Detected Prior to Completion or Success of Incident and/or Attack."

Consistent Input Field Examples (adapted from VERIS):

If the incident was detected externally, how was the organization notified? Check all that apply:

- ☐ Not Applicable (Detected Internally)
- ☐ Disclosed by threat agent (e.g., extortion, public bragging)
- ☐ Compliance Audit
- ☐ Security/Vulnerability scan
- ☐ Emergency Response Team (e.g., ICS-CERT)
- ☐ Found Documents
- ☐ Fraud Detection (e.g., CPP)
- ☐ Notified while investigating separate incident
- ☐ Notified by law enforcement or government agency (what agency? _____)
- ☐ Report of suspicious traffic
- ☐ Notified by partner/provider organization (select below)
  - ☐ Antivirus Company (not AV product)
  - ☐ Audit Service
  - ☐ Monitoring Service
  - ☐ Other _____
- ☐ *Additional Entry . . .*

If the incident was detected internally, how was it detected? Check all that apply:

- ☐ Not applicable (Detected Externally)
- ☐ Host IDS or file integrity monitoring
- ☐ Informal IT review
- ☐ Network IDS or IPS alert
- ☐ Antivirus alert
- ☐ Vulnerability scan
- ☐ Data loss prevention software
- ☐ Financial audit/reconciliation process
- ☐ Analytics
- ☐ Fraud detection mechanism
- ☐ Discovered while responding to another (separate) incident
- ☐ Infrastructure monitoring
- ☐ External Threat Feed
- ☐ Log review process or SIEM
- ☐ Reported by employee who saw something odd
- ☐ Physical security system alarm
- ☐ Unknown
- ☐ *Additional Entry . . .*

Value Discussion:

Whether an incident was detected internally or externally, and how, can shed light not only on the event itself but also on the effectiveness of a contributing organization's capabilities. Analysis of this data could:

- Help identify what detection techniques are effective against the kinds of attacks prevalent in a given industry sector – for example, "Organizations using this TTP were 37% less likely to be successfully attacked," or "No difference was found between companies that use antivirus and those that do not";
- Promote, through peer-to-peer comparisons, greater awareness about the capabilities in which industry sector peer organizations invest and the effectiveness of those capabilities;
- Help CISOs and other cybersecurity professionals validate their cybersecurity activities – specifically, by supporting cost-benefit analyses that demonstrate return on investment for technology, training, and other cyber risk management measures; and
- In conjunction with Data Category 1, "Type of Incident," Data Category 4, "Timeline," and Data Category 12, "Internal Skill Sufficiency," information, provide insurers with valuable proxy indicators of an organization's cyber risk management maturity.

Data Category #11: Incident Response Playbook – "How Did the Organization Respond, and Did the Response Work?"

Definition:

The actions, methods, procedures, and tools used to respond to an incident and to bring it to a close, and their effectiveness.

Whereas Data Category 13, "Mitigation/Prevention," seeks to establish long-term "get well" actions, this data category is focused on the immediate cyber risk management actions taken to "stop the bleeding" and reestablish control.

Consistent Input Field Examples:

Please identify the tactics, techniques and procedures used to respond to the incident. Check all that apply:

- ☐ Blocking
- ☐ Install/update patch
- ☐ Change passwords
- ☐ Honeypot
- ☐ Sinkhole
- ☐ Isolation/segregation in the DMZ
- ☐ Disconnection
- ☐ Employ custom scripts for hunting
- ☐ Reconfigure network devices
- ☐ Direct personnel actions
- ☐ Re-tune Technical Controls
- ☐ Patch Management
- ☐ Other _____
- ☐ *Additional Entry . . .*

Value Discussion:

The CIDAWG participants described this data category as essential for identifying what processes, tools, and other techniques are effective or ineffective in response to particular incidents and where they should be employed within an enterprise. Analysis of this information could help:

- Identify what cybersecurity controls – including processes – are effective when working to "stop the bleeding" during an incident;
- Validate return on cybersecurity investments, including investments in people, processes, and/or technologies, by demonstrating their effectiveness when used (or not used) by peer organizations;
- Provide trending insights that indicate:
  - Whether certain industry sectors and/or technologies are better at preventing attacks, in turn informing how coverage for a sector that often experiences certain incidents should be priced; and
  - What particular tools and techniques should be required as a condition for coverage within a particular industry sector and accordingly incentivized through the "reward" of more coverage at reduced rates;
- Promote the development of "Lessons Learned" and incident "playbooks" – i.e., libraries of responses that defenders can use in different scenarios to bring an incident to an effective close or to defeat a cyber attack – based on demonstrated success across peer organizations; and
- Identify cultural or technology strengths or shortcomings in particular industry sectors with regard to cyber incident response that could be used to establish incentives or adjust insurance policy pricing.

Data Category #12: Internal Skills Sufficiency – "Did You Have What You Needed to Respond to the Incident?"

Definition:

Availability and sufficiency of an organization's internal capacity and skills to quickly address and resolve incidents.

This data category is focused on identifying the types and availability of skills needed over the course of an incident regarding event detection, characterization, response, and recovery.

Consistent Input Field Examples:

Were internal skills sufficient? Yes ☐ No ☐

What internal skills were employed? Check all that apply:

- ☐ Incident response coordination
- ☐ Forensics/investigations
- ☐ Response strategy development
- ☐ Technical skills
- ☐ Chain of custody/evidence management
- ☐ Systems analysis (e.g., correlation, event detection, log analyses)
- ☐ Enterprise architecture design
- ☐ Business impact assessment
- ☐ Malware analysis/reverse engineering
- ☐ Other _____
- ☐ *Additional Entry . . .*

Does your organization outsource skills? **Yes ☐ No ☐**

If yes, did the outsourcing work? Yes ☐ No ☐

What external skills were employed? Check all that apply:

- ☐ Expert witness
- ☐ Incident response coordination
- ☐ Forensics/investigations
- ☐ Response strategy development
- ☐ Technical skills
- ☐ Chain of custody/evidence management
- ☐ Systems analysis (e.g., correlation, event detection, log analyses)
- ☐ Enterprise architecture
- ☐ Business impact assessment
- ☐ Malware analysis/reverse engineering
- ☐ Other _____
- ☐ *Additional Entry . . .*

Does your organization have an incident response (IR) plan? **Yes ☐ No ☐**

Does your organization have internal forensic capabilities? **Yes ☐ No ☐**

Does your organization have a retainer for external forensic capabilities? **Yes ☐ No ☐**

Value Discussion:

The sharing, aggregation, and analysis of information falling within this data category could:

- Help establish benchmarks for assessing a potential insured's cybersecurity capabilities in terms of what mix of skills is appropriate to an organization's risk management profile;
- By indicating what skills are required, assist organizations that outsource segments of their cybersecurity programs so they can screen service providers for those specific skills;
- Suggest, where outsourcing is not appropriate or desired, what skills are needed to address categories of cyber incidents that are endemic to a particular industry sector;
- Help CISOs and other cybersecurity professionals:

- Forecast their manpower and training needs ahead of changing incident and technology trends within the context of their respective industry sectors;
- Identify needed investments in staffing and training changes; and
- Justify the costs of those changes; and

- Identify the characteristics of effective cyber risk management cultures across industry sectors by providing insight into the response capabilities of impacted organizations.

Data Category #13: Mitigation/Prevention Measures – "What Was the 'Final' Fix?"

Definition:

Long-term actions taken to stop incidents and to prevent similar future occurrences.

Consistent Input Field Examples:

Please identify which actions were taken to stop incidents and to prevent similar future occurrences. Check all that apply:

- ☐ Implemented New Policies/Procedures
- ☐ Conducted Training
- ☐ Performed Patch Management
- ☐ Corrected Configurations
- ☐ Installed Additional Authentication Measures
- ☐ Security Communications Program
- ☐ Revised Security Responsibilities. Check all that apply:
  - ☐ Implemented new policies and procedures
  - ☐ Formalized responsibility for security controls (e.g., documented and assigned)
  - ☐ Added additional security solution to portfolio
  - ☐ Engaged outside provider to support internal skill sets
  - ☐ Other _____
  - ☐ *Additional Entry . . .*
- ☐ Purchased Cybersecurity Insurance
- ☐ Engaged with a Third-party Vendor
- ☐ Deployed New Technology
- ☐ Captured Lessons Learned
- ☐ *Additional Entry . . .*

Value Discussion:

Analysis of information falling within this data category is essential for:

- Benchmarking and justifying long-term cybersecurity investments by showing senior leaders that a given approach has been proven effective for similarly situated organizations; and

- In conjunction with Data Category 1, "Type of Incident," Data Category 4, "Timeline," and Data Category 16, "Related Events," information, helping the cybersecurity community identify "Lessons Learned" and develop incident "playbooks."

Data Category #14: Costs – "How Much Did It Cost to Clean Up, in Total?"

Definition:

Financial and other *quantifiable* costs incurred as a result of an incident.

This data category focuses on the resources required to "fix" the issues created by a cyber incident. It asks repository contributors, "What were the total costs involved in responding to and recovering from the incident, to include establishing mechanisms to protect against future recurrences?" This data category should include all quantifiable "pay outs" by the victim, insurers, and affected third parties as well as profit loss and reputation loss (to the extent it can be estimated). This data category thus could include input fields for the quantifiable costs associated with, for example, "Business Downtime," "Additional Manpower for Remediation," "Liability," "Lost Wages/Profits," "Reconstruction," "Notification and Monitoring," and "Forensics."

Consistent Input Field Examples:

COST CATEGORY	COST ($$$)
Direct Losses to Theft (e.g., Diverted Funds)	
Liability Claims/ Restitution	
Production Equipment Replacement	
System Administrator Overtime	
Third Party Assistance Costs (e.g., Investigation, Forensics)	
Staff Augmentation During Response	
Hardware/Equip (Replacement)	
Hardware/Equip (New, as in additional sensors/controls)	
System/ Software Installation	
Production Delays	
Backup Restoral	
Business Interruption/Lost Transactions	
Lost Wages/Lost Profits	
Public Relations/Reputation	
Victim Notification	
Credit Monitoring	
Legal Costs	

PCI & Regulatory Fines/ Assessments	
Other _____	
Additional Entry . . .	
TOTAL COSTS	

Decline to Answer ☐

Value Discussion:

While understanding costs incurred during and after a cyber incident is central to the insurance process, analysis of this data could have a multitude of potential cyber risk management benefits, including the following:

- Benchmarking costs associated with typical incidents that occur in a given industry sector could enable repository participants to draw inferences about the cost-effectiveness of various controls;
- Data on costs incurred by similarly situated peers could help justify otherwise prohibitively expensive investments. For example, repository-supported analysis might reveal that a good but pricey disaster recovery capability would almost completely alleviate the costs of an otherwise extremely costly incident;
- Comparisons between the cost of effective controls (risk mitigation) versus the cost of insurance (risk transfer) – for example, during a cyber "accident" – could help organizations better balance their cyber risk management investments;
- Showing the breadth of non-IT business costs associated with cyber incidents could help organizations frame cybersecurity within their respective enterprise risk management models;
- Comparisons of organization cyber incident costs within and across industry sectors could support pay-out forecasting and consequence modeling on a sector-by-sector basis. For instance, if an insurer covers all of a cloud service providers' clients, every one of those clients will have business interruption costs on top of the provider's own mitigation and reconstitution costs, which may also be insured; and
- Capturing the total costs incurred in various cyber incident scenarios might uncover intimidating numbers that many cybersecurity insurance stakeholders do not yet fully understand. Such awareness could advance cybersecurity awareness and foster wiser business decisions and strategies.

Data Category #15: Vendor Incident Support – "Were Other Involved Parties Helpful?"

Definition:

Vendor behavior during the assessment and resolution of a cyber incident.

CIDAWG participants advised that while the importance of third-party vendors to an organization's cybersecurity is increasingly recognized, CISOs and other cybersecurity professionals have only limited access to information that can help them objectively determine the quality of vendor support when cyber events happen. This data category is intended to capture information on a consistent basis that could provide that insight. The approach could be either scalar or include input fields describing vendor

behavior in commonly understood and used terms such as "Unknowledgeable," "Indifferent," "Cooperative," "Actively Helpful," and "Hostile/Combative."

Consistent Input Field Examples:

For each vendor/service provider you contacted for assistance, indicate their role and their helpfulness in resolving the incident:

Vendor Type	**1** **Difficult to Source**	**2** **Hostile / Combative**	***3*** ***Not Knowledgeable***	**4** **Indifferent / Unhelpful**	**5** **Cooperative**	**6** **Reasonably Helpful**	**7** **Actively Helpful**
Telco							
IaaS Provider							
Business Services Partner							
Merchandise Supplier							
Business App Provider / Host							
POS System Provider							
Utility (power, HVAC, etc.)							
Forensic							
Software							
Hardware							
Insurer							
Additional Entry . . .							

If you filed an insurance claim, was it accepted or denied? Accepted ☐ Denied ☐

Value Discussion:

The sharing, aggregation, and analysis of information falling within this data category could help organizations:

- Identify and mitigate specific risks associated with data/application hosting, software services, and product suppliers;
- Better understand how vendors in particular industry sectors engage in the cyber incident resolution process;

- Inform decision making about the degree to which an organization should rely upon third parties (and under what circumstances) by capturing information about how vendors respond to requests for assistance;
- Determine what kinds of support clauses to write into vendor contracts; and
- Reveal categories of vendors with patterns of poor support in order to encourage organizations to:
  - Invest in secure interfaces and isolation processes; and
  - Make incident response support a routine part of supplier relationships.

Data Category #16: Related Events – "Was Anything Relevant Happening at the Time of the Incident?"

Definition:

Related activities that provide incident context.

This data category is intended to provide incident-specific context to a given report shared into a repository that could – if aggregated and analyzed – discern broader contexts that could help similarly-situated organizations in the future. Such broader contexts could reveal, for example, that when organizations within a particular industry sector announce an unpopular kind of policy, they see an uptick in hacktivist attacks. Specific context input fields that might provide this insight could include "SaaS Provider Change," "Upcoming Merger Discussions," "Corporate Policy Publicity," "Product Launch," and "High Shopping/Transaction Period."

Consistent Input Field Examples:

Has your organization experienced any recent events that may be related to the incident? Check all that apply:

- ☐ New Data Host (IaaS or SaaS Provider)
- ☐ New Software/Application Provider
- ☐ Corporate Merger/ Acquisition
- ☐ Corporate Lay-Offs / Downsizing
- ☐ Seasonal / Cyclical Event
- ☐ Geopolitical / Regional Event
- ☐ Disgruntled Employee(s)/Strike
- ☐ Industry Sector-Wide Attacks
- ☐ New Product Release/Pre-Release
- ☐ Recent Event/Bad Publicity (e.g., Environmental Impact, Scandal)
- ☐ New Corporate Policy Release (i.e., with Social/Economic Implications)
- ☐ Natural Disasters
- ☐ Operation / Campaign
- ☐ C-Suite Level Public Remarks

Additional Entry . . .

Value Discussion:

The CIDAWG participants identified several areas where repository-supported analysis of related events information could help advance the cause of more effective cyber risk management:

- Organizations anticipating similar circumstances could use this information – in conjunction with Data Point #1, "Type of Incident," information – in order to increase their vigilance against not only

hacktivist activity generally but also the particular attack model deployed by their injured peer organization;

- For companies employing point-of-sale systems or moving into a new international market, analysis of this kind of data could help identify periods such as holiday or tourist seasons – as well as other local or periodic triggers – that may warrant additional staffing, more frequent patching, or other preventive actions;
- In the aggregate, this data could highlight the kinds of events in various industry sectors (or contexts) that drive cyber attacks. This could enable insurers to forecast attack cycles, adjust pricing, alert clients, and take other actions as appropriate; and
- Framing cyber incidents within a broader business operations context could help CISOs and other cybersecurity professionals advance cybersecurity awareness by making their senior leadership more cognizant of cybersecurity risks as a core component of effective enterprise risk management.

Excluded Data Categories: Maturity Indicator Index, Threat Attribution

Cybersecurity Maturity Indicator Index

The CIDAWG discussed but ultimately chose to reject the inclusion of a data category that would have involved organizational self-assessment using some approved maturity scale (e.g., 1-5), such as the SANS capacity/maturity index, the Cybersecurity Capability Maturity Model (C2M2), or the Building Security in Maturity Model (BSIMM). CIDAWG participants expressed concerns about: (1) incompatible industry sector-mandated assessments; (2) CISO willingness to provide a retroactive self-assessment in the wake of an incident; (3) the accuracy and actuarial value of subjective self-assessments; and (4) the observation that maturity – even when objectively evaluated – does not necessarily correlate with an ability to ward off attacks. To this last point, they noted that some large, well-resourced and mature companies are precisely those likely to be targeted by the most sophisticated threat actors – such as nation states, organized crime, or well-resourced hacktivists – simply because of the nature and scope of the data those companies own, and/or their greater social/economic visibility. Ultimately, the CIDAWG opted to exclude this data category as a stand-alone item in favor of garnering comparable information through other data categories, including skills, point of failure, detection/ mitigation techniques, response timelines, and framework usage.

Attribution

The CIDAWG also considered including but opted against a separate "Threat Actor/Attribution" data category. While CIDAWG participants agreed that organizations – and insurers – are interested in understanding who initiated a cyber attack, they concluded that today's attribution capabilities and methods lack sufficient precision to accurately identify attackers with a reasonable degree of confidence. Although attribution could be helpful in terms of blocking certain suspect IP ranges, for example, the CIDAWG participants noted serious drawbacks with this approach. One CISO asked, "Does that mean that if I'm doing business in China, all my traffic will be flagged as an attack on its recipient? That's a big disincentive to international companies." Others noted that identifying the proximate attacker may just point an organization to a hacker-for-hire. Put simply, the entity responsible for conducting the attack may not be the one who ordered it. Some sophisticated threat actors, moreover, maintain servers in unwitting nations just to further muddy the attribution waters and create deniability.

The CIDAWG noted two potential positives that could arise from the sharing of attribution information: (1) the identification of clearly known attackers, such as insiders and extortionists; and (2) the discernment of similarities to known threat campaigns by sophisticated or notorious threat actors within and across sectors. With regard to this latter benefit, CIDAWG participants stated that aggregate data collected under type, causes, timelines, and apparent goals – along with contextual information about the incident, such as sector – could be used to extrapolate this information and correlate an individual or series of incidents with known modus operandi of particular threat groups.

Conclusion

The data categories and associated discussion presented in this paper addresses the second topic – the type and scope of appropriate data that should be shared into a repository – of a four-topic dialogue about how a legally-compliant, privacy-respecting, and trusted cyber incident data repository could be leveraged to improve the overall cyber risk management practices of private and public sector organizations. The CIDAWG has engaged in this dialogue over the course of several months in order to bring deep subject-matter expertise to the task of evaluating the proposition that cybersecurity incident data, anonymized and shared into a repository, could support analysis that informs:

- Day-to-day risk mitigation strategies of CISOs and other cybersecurity professionals and the investments that their organizations make to address their unique cyber risk profiles;
- Research initiatives and related product and service development plans of forward-looking cybersecurity solutions providers; and
- Insurer efforts to scope, price, and deliver existing and new cybersecurity insurance policies that effectively transfer cyber risk by drawing upon new streams of actuarially relevant information.

Executive Orders 13636 and 13691 make clear that enhanced information sharing that facilitates effective cyber risk management across industry sectors is a national (and economic) security imperative. As the CIDAWG's conversation develops through future discussions, NPPD's goal continues to be answering three key questions:

- Do existing repositories meet the cyber incident data needs of cybersecurity stakeholder groups?
- Are owners and operators of existing repositories open to leveraging the knowledge that the CIDAWG develops – regarding needed cyber incident data and analysis and the best ways of sharing it – and incorporating it into their existing structures?
- If not, should a new cyber incident data repository be developed?

As the number, scale, and sophistication of cyber incidents around the globe continue to mount, the importance of facilitating and incentivizing more informed cyber risk management and investment through enhanced information sharing becomes ever more pronounced. The first two steps in this inquiry – determining the value of a trusted cyber data incident repository and defining the data categories that can deliver on that value – will be followed in the coming months by further CIDAWG discussions addressing the legal and privacy protections, anonymization approaches, and other characteristics that a trusted repository must incorporate in order to make it a safe information sharing space. That conversation, in turn, will inform a future dialogue about how a repository notionally should be scoped and structured during an initial operating stage in order to support the kinds of analysis that cybersecurity stakeholders across every sector need in order to enhance their cyber risk management practices.

Appendix A: Consolidated Data Categories and Values Table

#	DP Title	Provenance of Consolidated DP	Submitter	Revised Definition (CISO + Insurer)	Value	How is Value Achieved?
	Incident Context	***Note: aggregation of several comments over multiple discussions - necessary for apples-to-apples comparison/analysis of data.***	N/A	**Background information about the contributing organization intended to facilitate comparative analytics while preserving anonymity.** ***"Who else might look like the affected organization?"*** *This input field captures generic information about a contributing organization in order to preserve the anonymity/privacy of the organization. It captures, for example, an organization's industry sector and size as well as the date of an incident report and of any incident report updates submitted by the contributing organization.*	***2. Peer-to-Peer Benchmarking*** ***4. Sector Differentiation*** ***5. Forecasting, Trending, Modeling***	- Allow apples-to-apples comparisons - Facilitate data searches/analyses by sector or other characteristics - Support trend modeling by sector

1	**Type of Incident**	*Modification of* ***Insurer DP#1.*** Modified to conform to cybersecurity industry taxonomies (e.g., incident "type" vs "payload"). **Checkboxes recommended.**	Insurers/ CISOs	**A high-level descriptor or "tag" (e.g., "Ransomware" or "SCADA attack" as opposed to "Malware"), to differentiate the incident for ease of reference, leaving the capture of specific technical details about the incident to other data categories.** ***"Was it a DDOS, exploitation, destructive WORM, etc.?"*** *This data category could include input boxes such as Physical Disaster, System Failure, DDOS, Exploitation/Espionage, Extortion/Ransomware, Destructive WORM, etc.*	***1. Identify Risks & Effective Controls*** ***4. Sector Differentiation*** ***5. Forecasting, Trending, Modeling*** ***6. Advance Risk Mgmt. Culture***	- Identify evolving attack tactics, techniques, and procedures (TTPs) - Track different TTPs by sector - Help predict attacks in similar companies/sectors - Support internal risk awareness/training with specific alerts (e.g., spear phishing)

2	**Severity of Incident**	*Merger of **Insurer DP#5** and **CISO DP#9**, both addressing Severity.* Note: In addition to an objective incident severity scale (one national-level scale is being developed by NIST and the National Security Staff), will require short narrative due to variations in impacts by industry ($, lives, downtime, chemical measurements, etc.). **Checkboxes will facilitate consistency, but a narrative will also likely be needed to account for variations in metrics.**	Insurers/ CISOs	**The relative scale or scope of an incident within the context of the incident contributor's industry and circumstances.** ***"How bad was it? Really bad, bad, or pretty minor?"*** *This data category could include scalar input fields such as Low-Medium-High, 1-5, Mild-Catastrophic, along with Short Narrative Descriptions (e.g., for Environmental Harms, spill and emissions levels), the specific values (e.g., 100K records, or 1M gallons spilled) dependent upon the type of impact incurred. As described in Data Category 9, "Type of Impact," those impacts could include Production Loss/Time to Market Delay, Equipment Damage, Death or Injuries, and Environmental Harms.*	**3. Show Return on Investment** **4. Sector Differentiation** **5. Forecasting, Trending, Modeling** **6. Advance Risk Mgmt. Culture**	- Helps insurers determine appropriate coverage by sector - Helps CISOs make cost-benefit cases in terms of loss avoidance based on similarly situated companies - Helps predict/model potential costs - Raises awareness of cyber risks as enterprise risks

3	**Use of a Cyber-security Framework**	***CISO DP#7*** Dozens of frameworks available. In order to standardize inputs, **checkboxes** will be required.	CISOs	**<u>The cyber risk management practices, procedures, regulations and standards that an organization had in place at the time of an incident.</u>** ***"Generally speaking, how was an organization postured before the incident and/or attack?"*** *This data category could include input boxes/fields that list the best practices, procedures, regulations, and standards -- and any related, overarching frameworks -- that an organization has implemented and their corresponding dates of first implementation.*	**1. Identify Risks & Effective Controls** **4. Sector Differentiation** **5. Forecasting, Trending, Modeling** **6. Advance Risk Mgmt. Culture**	- May help determine whether compliance with a framework is helpful in minimizing successful attacks - If a variety of frameworks are used, helps identify which ones work - Can help forecast when a previously effective framework is becoming obsolete - May encourage adoption of a cybersecurity framework as a component of ERM

4	**Timeline**	*This is a merger of **Insurer DP#9** "Timeline of discovery/reporting," **Insurer DP#10**, "Timeline for detecting/stopping attack," **Insurer DP#11**, "Date of Initial Attack" (often indeterminable) and **Insurer DP#14** "Success in Detection" (detection is assumed a pre-requisite for reporting)* Consolidated to eliminate redundancies, and to address CISO concerns. Original submission included time between initial attack and detection, but several CISOs noted that (a) sophisticated attacks are unlikely to be detected regardless of effective security controls in place; (b) quick detection may indicate a clumsy attack rather than good security; and (c) in an attack with a series of steps, the original compromise point/date may not be determinable. **This revised DP shifts focus from Time-to-Detect, to Time-to-Respond.** Retroactive timeline establishing initial attack date is included, *if that can be determined.*	Insurers	**<u>The date of detection of a cyber incident and the date of effective control.</u>** ***"How did the incident and/or attack progress?"*** *If they can be established, this data category should capture retroactive timelines of incident and/or attack phases and steps. Given its dynamic nature, this data category requires that a repository include a mechanism by which contributing organizations can access and update their original timeline submission, without compromising their anonymity, as incident and/or attack investigations progress.*	**1. Identify Risks & Effective Controls** **2. Peer-to-Peer Benchmarking** **3. Show Return on Investment** **4. Sector Differentiation**	- The ability/inability to quickly get an incident under control can highlight the effectiveness/ ineffectiveness of controls used - Time to respond can indicate the maturity and effectiveness of a cybersecurity function - Time to control may indicate the maturity of the targeted organization and/or the sophistication of the attack - Variations across sectors can highlight sector-specific strengths and weaknesses - Knowing the response time will be noted may help CISOs get the resources they need to respond quickly and effectively.

5	**Apparent Goal**	*Modification of **Insurer DP#3**, "Attack Goals/Targets."* Modified in response to CISO observations that many attacks will have several intermediate targets, and goals may not be known but only inferred from the type of attack, e.g., disrupt services (DDOS), disrupt physical operations (SCADA/ICS), theft (PII data breach), industrial espionage (IP data/system breach), punishment or extortion of an individual (specific accounts/files compromised), or Hacktivism/degrade corporate reputation/affect corporate policy (defaced web sites, publicized information, etc.). **Checkboxes Suggested.**	Insurers	**The assets apparently targeted, implying their financial, reputational, and operational value to an attacker**. ***"What was the attacker after?"*** *This data category identifies the assets that appear to have been targeted for destruction, disruption, theft, disclosure or other action contrary to the organization's interests. It could include input boxes/fields such as System/Service Availability, Reputation, Theft of Intellectual Property (IP), and Theft of Personally Identifiable Information (PII).*	**1. Identify Risks & Effective Controls** **4. Sector Differentiation** **5. Forecasting, Trending, Modeling** **6. Advance Risk Mgmt. Culture**	- Identify Adversary targets and TTPs by sector - Identify evolving attack trends - Help identify the value of particular assets to attackers to help organizations better assess their risks

6	**Contributing Causes**	*Consolidation of **Insurer DP#2**, "Incident Causes," **Insurer DP #12**, "Vendor Involvement" (which included supply chain root causes), and aspects of **CISO DP#3**, "Control Decay Situations."* Modified definition to conform to cybersecurity industry taxonomies. Strong CISO support for this DP. **Recommend "Check All That Apply," plus "Other" narrative option.**	Insurers/ CISOs	**People, process, and/or technology failures contributing or otherwise relevant to an incident and/or attack.** ***"How did the incident happen/how did the attacker do it? What people/process/technology was involved/exploited?"*** *This data category should include input boxes/fields for both contributing organization and related third party vendor/supplier control failures such as Misconfiguration, Malicious Insider, and Poor Training, and Zero-Day Exploit.*	**1. Identify Risks & Effective Controls** **3. Show Return on Investment** **4. Sector Differentiation** **5. Forecasting, Trending, Modeling** **6. Advance Risk Mgmt. Culture**	- Identifies what controls are effective and which are ineffective or losing effectiveness - Helps illuminate cybersecurity concerns associated with third party providers - Helps CISOs justify investments in replacing/upgrading controls shown to be deficient - Helps identify sector-unique control issues - Supports attacker TTP trending - Supports internal process/training improvements

7	**Security Control Decay**	***CISO DP#3.*** **Checkboxes recommended** for common taxonomy of controls (including TTPs) and failures (e.g., failed open, unpatched, in-tune/operating but still failed).	CISOs	**A set of circumstances where a security control, although present, did not operate effectively enough to withstand an incident and/or attack.** ***"What controls failed and how?"*** *This data category assesses why, where, and how a particular security control failed. It could include input boxes/fields that identify the category of the involved security control as well as descriptors of the failure, such as Failed Open, Unpatched, Improperly Applied/Configured, and In-Tune and Operating/Still Failed.*	**1. Identify Risks & Effective Controls** **3. Show Return on Investment** **4. Sector Differentiation** **5. Forecasting, Trending, Modeling**	- Identifying what controls are failing can give CISOs warning in time to augment or change those controls in their enterprise - Sufficient control failure data over time may allow forecasting of control "lifecycles" - Helps CISOs justify technology upgrades with data showing existing technology is aging out - Helps identify sector-specific controls that are or are not effective. Helps similarly situated companies realistically assess risk

8	**Assets Compromised/ Affected**	*Note: **This DP, plus "Type of Impact"** below, **replaces Insurer DP #6:** "Impacts" and Insurer **DP#13**, "3d Party Impacts."* May include multiple assets from different phases of attack--e.g., 3d party system, then, core business system, then PII database…May require a **"Check All That Apply," plus a short "Other" Narrative option.**	Insurers	**<u>The points in the network and/or business where an incident and/or attack took place.</u>** ***"What was impacted by the incident/what did the attacker hit?"*** *The input boxes/fields for this data category should reflect all potential points of compromise -- including people, process, and technology -- and extend to incidental, secondary, and third party assets that either caused or were otherwise affected by the compromise. They could include, for example, SCADA/ Industrial Control Systems (ICS), Databases, Individual Accounts, Business Application Servers, Third Party Systems, and Websites. The goal of this data category is to identify aggregate exposure, not impact (defined in Data Category 9 as "harm"), because compromised assets may not experience actual harm.*	**1. Identify Risks & Effective Controls** **3. Show Return on Investment** **4. Sector Differentiation** **5. Forecasting, Trending, Modeling** **6. Advance Risk Mgmt. Culture**	- Identify target types by sector - Help attribute motive and access points to assess and protect against future risks - Help model particular types of attacks by showing what assets are compromised over the course of particular attacks - Identify/justify areas of investment around known targeted assets in a given sector (e.g., ICS or Point-of-Sale systems)

9	**Type of Impact**	*Merger of **Insurer DP#6** "Impacts to Systems, Including Cascading Effects" and **Insurer DP#13** "3d Party Impacts"* Modified to incorporate CISO concern that only PII, IP and financial losses were covered (in original Insurer definition), and that operational and physical impacts were not adequately addressed (e.g., environmental harm, equipment/physical damage, production loss, service interruption, injury/death, service unavailability, etc.). **Checkboxes Recommended.**	Insurers/ CISOs	**<u>The specific effects of an incident and/or attack on all affected parties.</u>** ***"What were the effects?"*** *This data category addresses the actual harm incurred by the victim(s) at each step of the incident and/or attack and extends beyond the impacted/targeted organization to third party vendors and suppliers, as well as downstream parties such as employees and customers. The input boxes/fields for this data category should include the generic identities of affected parties by category (e.g., contributing organization and its Infrastructure- and Software-as-a-Service (IaaS/SaaS) cloud and application provider); the harms/impacts they suffered (e.g., Production Loss, Equipment Damage, Deaths/Injuries, and Environmental Harm); and the phase or step of the attack and/or incident when those impacts were incurred.*	**2. Peer-to-Peer Benchmarking** **3. Show Return on Investment** **4. Sector Differentiation** **5. Forecasting, Trending, Modeling** **6. Advance Risk Mgmt. Culture**	- Supports insurer aggregate risk estimates - Facilitates consequence modeling for insurers in a particular sector, or using a particular service, such as cloud hosting - Capturing the total impact of an incident in a peer organization can help CISOs frame cybersecurity budget/investment recommendations - By highlighting third party impacts, helps frame cybersecurity as inherent in ERM

10	**Incident Detection Techniques**	***CISO DP#5*** **Checkboxes suggested**. Include option for "not detected prior to attack success/completion".	CISOs	**<u>The techniques used to identify an incident and/or attack, and their effectiveness.</u>** ***"How did the affected organization find out?"*** *This data category could include input boxes/fields for internal detection techniques such as Tool/Process Intrusion Prevention System (IPS), Custom Script, and Analytics. It likewise could include input boxes/fields for describing external detection/notification such as by FBI, USSS, or Other Law Enforcement Entity; Attacker (extortion situation); Outsourced Security, and IaaS/SaaS Provider. This data category also could include input boxes/fields that address the scale of technique effectiveness such as "not detected prior to attack and/or incident success/completion."*	***1. Identify Risks & Effective Controls*** ***2. Peer-to-Peer Benchmarking*** ***3. Show Return on Investment*** ***4. Sector Differentiation***	- Helps companies remain aware of what capabilities others in their industry are investing in/using, and whether they're effective - Supports cost-benefit analysis and ROI for cybersecurity investments - Identifies methods, including processes, that are effective in detecting attacks; helps justify investments in both technology and manpower/training - May help identify sector-specific controls effective against the kinds of attacks experienced by that sector

11	**Incident Response TTPs**	***CISO DP#6*** Avoid keying on technology, which changes. Focus on process solutions. **Checkboxes** will help ensure consistency of framing, but **narrative** may also be required.	CISOs	**The tools, actions, methods, and procedures used to respond to an incident and/or attack and to bring it to a close, and the effectiveness of those tools, actions, methods, and procedures.** ***"How did the organization respond? Did that work?"***	**1. Identify Risks & Effective Controls** **2. Peer-to-Peer Benchmarking** **3. Show Return on Investment** **4. Sector Differentiation**	- Identifies what response TTPs, including tools and processes, are effective/ineffective in responding to particular attacks - Helps CISOs demonstrate ROI for cybersecurity investments - Helps build Lessons Learned/Playbooks among similarly situated companies - May help identify cultural or technology strengths or shortcomings in particular sectors with regard to cyber incident response

12	**Internal Skill Sufficiency**	***CISO DP#2*** **Checkboxes** for common skills will require accepted taxonomy.	CISOs	**<u>Availability and sufficiency of an organization's skills and capacity to quickly address and resolve incidents and/or attacks.</u>** ***"Did the organization have in place what it needed to respond, or did it have to hire out?"***	**2. Peer-to-Peer Benchmarking** **3. Show Return on Investment** **5. Forecasting, Trending, Modeling**	- P2P benchmarking on in-house skill-sets can help companies decide whether to acquire/train or outsource certain skill areas - Can help companies who outsource parts of their cybersecurity to screen service providers - Helps CISOs identify and justify staffing changes/additions and training - Analyzing required skills over time helps companies forecast manpower and training needs ahead of need, in response to changing attack and technology trends
13	**Mitigation/ Prevention Measures**	*Merger of* ***Insurer DP#16*** *"Preventative Actions" and* ***CISO DP#6*** *"Response Techniques."* CISOs note this may require **Narrative checkboxes.**	Insurers/ CISOs	**<u>Actions taken to stop incidents and/or attacks and to prevent similar future occurrences.</u>** ***"What was the 'final' fix?"***	**1. Identify Risks & Effective Controls** **2. Peer-to-Peer Benchmarking** **3. Show Return on Investment**	- Helps establish what controls, including tools and processes are effective in stopping an incident and/or attack in progress - Helps CISOs justify investment in proven controls - Helps build Lessons Learned/Playbooks

14	**Costs**	***Insurer DP#8.*** NOTE: CISOs strongly recommend not including "IT Spend" prior to event, because (a) companies are not consistent in how they identify security expenditures; and (b) it is not strongly correlated with security for a given company or incident. **Offering checkboxes may help companies bin costs consistently.**	Insurers	**Financial and other quantifiable costs incurred as a result of an incident and/or attack.** ***"What did it cost to clean up, in total?"*** *This data category focuses on the resources required to "fix" the issues created by the incident and/or attack. It should include all quantifiable "pay-outs" by the victim, insurers, and affected third parties as well as profit loss and reputation loss (to the extent it can be estimated). This data category thus could include input boxes/fields for the quantifiable costs associated with, for example, Business Downtime, Additional Manpower for Remediation, Liability, Lost Wages/Profits, Reconstruction, Notification and Monitoring, and Forensics.*	**2. Peer-to-Peer Benchmarking** **3. Show Return on Investment** **4. Sector Differentiation** **5. Forecasting, Trending, Modeling** **6. Advance Risk Mgmt. Culture**	- P2P benchmarking supports cost estimates and consequence modeling for insurers in a particular sector - Capturing the total impact of an incident in a peer organization can help CISOs frame cybersecurity budget/investment recommendations - By highlighting third party impacts, helps frame cybersecurity as inherent in ERM
15	**Vendor Incident Support**	***CISO DP#1*** **Checkboxes suggested** for uniformity of input.	CISOs	**Vendor behavior in assessing/resolving incidents and/or attacks.** ***"Were other involved parties helpful?"*** *This data category could be scalar, or have input boxes describing vendor behavior, such as: Unknowledgeable, Indifferent, Cooperative, Actively Helpful, and Hostile/Combative.*	**2. Peer-to-Peer Benchmarking** **4. Sector Differentiation** **6. Advance Risk Mgmt. Culture**	- Helps companies identify risks associated with third party vendors. Informs decision-making - Can help companies determine what kinds of support clauses to write into vendor contracts - For categories of vendors with a pattern of poor support, encourages investment in secure interfaces and isolation processes

16	**Related Events**	***Insurer DP#15***. CISOs recommend **short Narrative**, **or checkboxes** with write-in "Other" option.	Insurers	**<u>Related activities that provide incident and/or attack context.</u>** ***"Was anything relevant going on at the time of the incident and/or attack?"*** *This data category could include input boxes/fields such as SaaS Provider Change, Upcoming Merger Discussions, Corporate Policy Publicity, Product Launch, and High Shopping/Transaction Period, as well as a short narrative space for "Other."*	**2. Peer-to-Peer Benchmarking** **4. Sector Differentiation** **5. Forecasting, Trending, Modeling** **6. Advance Risk Mgmt. Culture**	- Allows organizations experiencing similar events to identify possible associated cyber risks - Helps identify what kinds of events in various sectors drive cyberattacks - Helps forecast attacks that may be cyclical (such as during holiday shopping periods) or political--enables CISOs to plan additional staff, more aggressive patching, etc. - By framing within the context of larger business operations, can help frame cybersecurity risks as inherent in ERM
	InfoSec Program Maturity **-** **DELETED** **-**	***CISO DP#4*** ***Note:*** *Considerable debate about ability to collect this data, CISO's willingness to provide (time/labor intensive and after-the-fact), and actuarial value.* ***<u>Deleted</u>*** *in favor of combination of other data categories: skills, point of failure, detection/ mitigation techniques, response timelines, and Framework usage.*	CISOs	Self-assessment using some approved maturity scale (i.e., 1-5), such as the SANS capacity/maturity index or NIST.	**2. Peer-to-Peer Benchmarking** **5. Forecasting, Trending, Modeling** **6. Advance Risk Mgmt. Culture**	

Appendix B: Notional Cyber Incident Use Cases

The following Use Cases were developed by CIDAWG participants as representative of different types of prevalent, serious cyber incidents affecting companies today. These scenarios were used in CIDAWG discussions to validate and refine the Data Categories presented in this paper.

Case #1: "Machinery Meltdown" (Industrial Sabotage via Industrial Control System Compromise)

Case #2: "Direct Deposit Profit" (Monetary Theft through financial PII data compromise)

Case #3: "Not-so-Random-Ransom" (Extortion through ransomware - unwitting Third-Party Provider)

Case #4: "Confidence Lost" (Malware injected through Third-Party Systems – Who's responsible?)

Case #5: "Disaster Averted" (Malware from unpatched system)

Case #1: Machinery Meltdown

Attackers gained access to a steel mill's corporate network via a spear phishing campaign. Once inside the network, the attackers pivoted through various computer systems until access to an industrial control system (ICS) was obtained. The corporate network and ICS were separated by a firewall. The attackers prevented the onsite workers from shutting down the blast furnace controlled by the ICS. The blast furnace was driven to melt down, causing significant damage to the steel mill's production facility.

Timeline & Details

- November 3, 2014 - Attackers send the initial spear phishing email to a network administrator. The email indicates that open enrollment for health care benefits "starts today" and asks the network administrator to click an included link to start the process. When the network administrator clicks the link, the page it loads bears the logo of the steel mill's website and looks reasonable. When the network administrator enters his corporate credentials, however, the page indicates that there was a problem and that he should contact human resources. When he does so, a human resources employee assists him with logging into the real site. The network administrator doesn't think anything of the failed login attempt and proceeds to modify his health care benefits.
- November 4 through November 23 - The attackers slowly explore the corporate network. They work in the evening, but not too late in order to avoid arousing suspicion.
- November 23 - The attackers discover an internal firewall; the DNS name for the firewall is "plant-fw1". The attackers determine that employee computers in the "plant environmental" group have access to control systems that operate the steel mill through this firewall.
    - Plant environmental group employees are not supposed to have this access, but it nevertheless was added last spring when the ICS had to be debugged. The debugging took a few weeks to complete, and the security staff was not notified that the "temporary" access could be decommissioned.
    - Firewall rule reviews are performed annually (just before the auditors arrive) as part of a recertification process to remove rules that are unnecessary.
- November 24 through December 14 - The attackers explore the ICS and determine from the labeling that something called "furnace 1" is available for manipulation.

- December 15 - The attackers change the password to the ICS, locking out the steel mill's staff during the latter part of the second shift. The attackers change the settings for "furnace 1" by deleting the shutdown procedure. This prevents the normal shutdown procedure from automatically taking place. Two hours into the third shift, employees realize that the furnace is still operating when it shouldn't. The emergency shut off is finally activated.
- December 16 - The furnace is shut down and the anomaly is investigated. As a result of the attackers' manipulation, the furnace developed a crack that requires new parts that must be ordered and replaced. The replacement takes six weeks, and costs $2,500,000. At first, the company attributes these events to an unfortunate equipment failure.
- December 17 - The ICS password change is detected and IT Security begins investigating. IT Security successfully reconstructs the events, but by this time the initial spear phishing email has been deleted. The trail ends with a network log entry indicating the network administrator's computer accessed the spear phishing site located on a server in China.
- January 12, 2015 - The incident investigation concludes. Event costs: $2,500,000 to replace the damaged blast furnace parts; $0 for business interruption because the company was able to shift work to other furnaces within 72 hours; and $120,000 for the investigation. Total event costs: $2,620,000.

Case #2: Direct Deposit Profit

A large company has an international presence and employees who regularly travel overseas. A Secure Sockets Layer Virtual Private Network (SSL-VPN) is provided for those employees to connect back to corporate resources. The company uses single sign on technology to reduce the number of passwords that the employees need to remember. All authentications at this company consist of a username and a password.

Through a broad based phishing campaign, attackers compromised a small number of user accounts at the company. The attackers used the compromised accounts to connect to the company's SSL-VPN and logged into the human resources system. They then changed the direct deposit information of ten employees from their actual bank accounts to a bank account in Malaysia. A few days after the next expected pay date, the company received complaints from some of the affected employees regarding their not being paid. The company contacted the FBI to report the complaints in the hope of recovering the stolen funds. By this time, however, the attackers already had cashed out the money from the Malaysian bank.

Timeline & Details

- March 10, 2014 – Attackers send phishing emails to the company's employees indicating that they failed to acknowledge the company's IT security policy during an allotted time period. The emails explain that in order to avoid disciplinary action, the employees must click on a provided link in order to log in and acknowledge the policy.
- March 11 through March 24 - Several employees click the phishing link. When they do so, they are presented with a web page bearing the company's logo and a login box. Upon logging in, the employees are thanked for acknowledging the policy and informed that no further action is required.
- March 25 through April 5 – Using the access that the phishing emails have provided, the attackers connect to the SSL-VPN and explore the company's human resources system. The human resources site was not difficult to find; the company had previously provided a quick link to the site on the SSL-VPN login page in order to assist employees. The attackers discover that

ten of the employees who divulged their passwords also use direct deposit to deposit their paychecks.

- April 6 - The attackers change the banking information for the ten employees to a bank account at a Malaysian bank. Noting the change, the human resources system automatically generates a confirmation email, telling the employees that their bank information has been modified. To avoid detection, the attackers log into the employees' email accounts via another link on the SSL-VPN login page and delete the confirmation email shortly after it is sent.
- April 11 - The paychecks of the ten employees are directly deposited into the foreign bank.
- April 16 - The company receives the first complaint of missing payment from one of the affected employees. The company investigates this first event as an employee error.
- April 17 - The attackers remove the cash from the Malaysian bank.
- April 18 – The company receives additional reports about missing payments from other affected employees, and the attack pattern is finally realized. The company contacts the local police.
- April 21 - The FBI is brought into the investigation.
- April 25 – The last of the ten affected employees, who have been on international travel, report the missing payments to their bank accounts. The company sends an email to its entire workforce instructing them to change their passwords.
- May 16 - The investigation concludes, and two-factor authentication is recommended going forward. The affected employees lost $50,000 to the attackers. The company decides to cover the affected employees' lost wages.
- May 20 - The FBI determines the activity to be part of a crime ring that has attacked several other large companies in a similar fashion over the last few months. The attacks come from computers at Malaysian internet cafes.
- October 1, 2014 – The company introduces two-factor authentication.
- Event costs: $170,000 for the investigation; $50,000 in lost funds; and $200,000 for procuring and implementing the two-factor authentication system.

Case #3: Not-So-Random Ransom

A financial services company hosts an annual off-site meeting for its employees every April. The company has used the same travel service for many years to assist its employees with booking flights, hotels, and local transportation for the meeting. The travel service works directly with individual employees to help them with their travel arrangements and shares relevant information with them through email. Late in the day on the Friday before the meeting, the travel service sent an email to the financial service company's employees indicating that the final agenda for the meeting was attached.

The attachment did include the final agenda, but it also included specially crafted ransomware that attackers had embedded. When the financial service company's employees opened the attachment, the ransomware proceeded to encrypt data files on all their computers. The employees then began receiving ransom payment demands from the attackers in return for an encryption key and to stop the attack. Over the weekend and through the early part of the following week, the employees reported to the company's IT Security team that their computers had stopped functioning and that they had received the ransom demands.

Subsequent investigation determined that the "agenda" email came from a compromised account at the travel service. The attackers had used DNS spoofing to redirect the travel service's web traffic to a fake, "look-alike" travel reservation site in order to obtain the credentials of the travel service's agents – specifically, their usernames and passwords. The investigation revealed that a number of the travel

service's agents had used the same usernames and passwords for the travel reservation site as they did for their corporate site. Using the stolen passwords of those agents, the attackers established the travel service as a convenient platform to launch the ransomware attack.

Timeline & Details

- November 10, 2014 - Attackers use DNS spoofing to redirect the computers of several travel service agents to a fake, "look-alike" travel reservation site that appears to be a legitimate site. When the agents enter their usernames and passwords on the fake site, it sends copies of those credentials to the attackers before connecting the agents to the real site.
- November 11 through November 21 - The attackers collect the travel service agents' usernames and passwords from the fake travel reservation site.
- November 22 - The attackers test those usernames and passwords to see if the same usernames and passwords grant access to the travel service's network. They find several usernames and passwords that grant that access.
- December 2014 through March 2015 - The attackers monitor email in several travel service agent accounts, looking for a worthwhile target. They select the financial services company.
- April 1 - The financial services company sends a copy of the finalized agenda for the off-site meeting to the travel service to distribute to the employee attendees and post to an employee/attendee website. The financial services company instructs the travel service to send out the agenda on Monday, April 6.
- April 3 - The attackers send out a ransomware-laced copy of the agenda to the meeting attendees. At first, the financial services company thinks that the travel service mistakenly sent the message too early. Later that day, the first reports of computers with the ransomware start coming into the financial service company's IT Security team. A ransom of $300,000 is demanded by the attackers to stop the attack. The ransom message is written in broken English and directs the company to contact an anonymous email account for further instructions. The CEO of the financial services company vows to never pay any ransom.
- April 4 through April 6 - Reports of many computers having the ransomware keep surfacing.
- April 6 – The financial services company's annual off-site meeting starts. Most of the company's employee computers are being held for ransom at this point. Remediation is hampered by the large number of employees traveling to the meeting. Confusion is rampant, the meeting is disbanded early, and business grinds to a halt.
- May 4 - The final computer with ransomware is reimaged, and the incident is closed. The financial services company's incident costs include: $20,000 to reimage the damaged computers; $50,000 to recreate lost documents; $100,000 in lost hotel and meeting space costs; and $100,000 for the investigation. The total cost is $270,000. Several of the financial services company's customers discontinue doing business with the company during the following year. Some of the defecting customers vaguely hint at the ransom event as the reason.
- May 5 - The travel service, which does not have an IT Security team, directs all of its agents to reset their corporate passwords. The travel service incident costs include: $500 of lost productivity during the password change and one lawsuit for $5,000,000 brought by the financial services company.

Case #4: Confidence Lost

A vendor provides point of sale (POS) systems to smaller retailers like independent restaurants, bars, and convenience stores. The POS systems don't allow customization beyond the vendor's specialized software. The POS systems process debit and credit cards through the vendor's online service. The

retailer does not pay for the POS hardware; rather they pay a monthly fee to the vendor for the service. Unfortunately, the vendor's POS system is easier to use than their contract. It is unclear who is responsible for security incidents should they arise.

An attacker discovers a weakness in the POS system and installs malware that retains a copy of every debit and credit card processed. The attacker sells the card information to other criminals that commit fraud. One news agency reports that several medium sized restaurant chains have been hacked; while another reports that independent bars have been hacked across several states. An online security news blogger cites anonymous banking sources that implicate a hack of the POS vendor. The POS vendor adamantly denies such a hack, but out of an abundance of caution retains a well-known computer forensics firm to verify there was no hack of the POS vendor's system. The POS vendor will not discuss the events until the forensic firm has finished the investigation.

Meanwhile, the retailers that use the POS system face questions from their customers, news organizations, and government agencies they can't answer. To make matters worse, when the retailers contact the POS vendor for support, the response is the vendor systems are secure and the retailers need to take action to verify their security. Several retailers express frustration and disappointment with the POS vendor's response in interviews. They feel blamed by the POS vendor for something out of their control.

Timeline & Details

- January 7, 2015 – The attacker places malware on hundreds of POS terminals at small businesses. The collection of credit and debit cards commences.
- April 1 – The attacker places a batch of credit and debit cards for sale on underground credit card marketplace. Buyers of card information begin using the cards for fraud.
- April 15 – The banks that issued the credit and debit cards detect the increase of fraud and start reissuing cards. The first news reports of the hacked cards start to circulate.
- April 20 – The security news blogger implicates the POS vendor as target of the hack.
- April 27 – The POS vendor hires the well-known computer forensics firm to investigate and begins spreading a message of "It's not us."

Case #5: Disaster Averted (Cyber Near Miss)

An employee of an auto parts manufacturing firm downloaded malware on his computer. The malware would have used a flaw in a popular computer operating system to spread but was thwarted because the firm's patch management system had patched the rest of the firm's computers. An installation failure had prevented the patch from applying properly to the infected machine. The firm was aware of the installation failure, and the computer had been scheduled for remediation by a technician the following week. The malware, however, got to it first. Once installed, the malware erased the infected computer's local hard drive. No data was lost, however, because the firm stored its data on internal servers. Once the malware was discovered, the IT Security team reimaged the computer and placed it back in service later that day.

Timeline & Details

- February 10, 2015 - The software vendor releases a patch for a security flaw in the popular computer operating system.
- February 26 - IT Security uses their patch management system to apply the security patch. The patch fails to apply to one workstation.

- February 27 – Damaging malware infects the unpatched computer when an employee accidentally downloads it from a website that was hosting a malicious advertisement. Local antivirus does not detect the malware. The employee leaves for the day before the malware triggers its destructive phase.
- March 2 – An IT technician is scheduled to manually patch the workstation early Monday morning. Reimaging commences instead of patching. The computer is reimaged and returned to the user later that day. A temporary computer is available to the user during the reimaging.

Event costs are estimated at $50 for the reimaging effort and lost productivity.