ENHANCING RESILIENCE THROUGH CYBER INCIDENT DATA SHARING AND ANALYSIS

This document identifies perceived obstacles to voluntary cyber incident data sharing and offers potential approaches to overcoming those obstacles. It is the third in a series of white papers.

Overcoming Perceived Obstacles to Sharing into a Cyber Incident Data Repository

December 2015

Table of Contents

Executive Summary

This white paper is the result of a series of discussions among insurers, chief information security officers (CISOs), and other cybersecurity professionals on perceived obstacles to the voluntary and anonymized sharing of cyber incident data into a trusted repository. These deliberations were conducted within the framework of the Cyber Incident Data and Analysis Working Group (CIDAWG) and facilitated by the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD). The CIDAWG's findings build upon the ideas and recommendations contained in the group's previous white papers:

- "*Enhancing Resilience Through Cyber Incident Data Sharing and Analysis: the Value Proposition for a Cyber Incident Data Repository,*" published in June 2015; and
- "*Enhancing Resilience Through Cyber Incident Data Sharing and Analysis: Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository,*" published in September 2015.

This white paper: (1) identifies eight perceived obstacles to the voluntary sharing of cyber incident data; (2) describes ways in which each obstacle might manifest in terms of questions or concerns that repository participants might have; (3) suggests approaches to addressing those questions and concerns in order to overcome each obstacle; and (4) identifies possible stakeholders and subject matter experts who could help develop and implement those approaches.

The identified obstacles focus primarily on assured privacy and anonymization, data security, and technical design challenges. Approaches to address these issues involve process and communications strategies and technical best practices that should inform any future repository implementation. This latter category includes effective input mechanisms for sharing cyber incident data into a repository – specifically, mechanisms that are easy to use, consistent with all applicable privacy and anonymization mandates, and relevant to stakeholders who will both contribute to the repository and utilize aggregated repository data for cyber risk analysis.

This white paper specifically elaborates on the following eight categories of information sharing obstacles identified by the CIDAWG:

1. **Assuring Anonymization**
2. **Ensuring Data Security**
3. **Cultural Challenges/Regional Differences**
4. **Perceived Commercial Disadvantage**
5. **Internal Process Hurdles**
6. **Perceived Value**
7. **Assuring Appropriate, Adequate and Equitable Participation**
8. **Technical Design Issues**

The group's follow-on efforts will focus on how a repository should be structured during an initial operating stage in order to support the kinds of analysis that cybersecurity stakeholders require to improve their cyber risk management practices.

Introduction

Since October 2012, the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) has convened a diverse group of private and public sector stakeholders – including insurers, risk managers, chief information security officers (CISOs), critical infrastructure owners, and social scientists – to examine the state of the cybersecurity insurance market and how to best advance its capacity to incentivize better cyber risk management.

These stakeholders have expressed strong support for the creation of a trusted and anonymized cyber incident data repository. As envisioned, the repository would store, aggregate, and analyze cyber incident data relevant to the cyber risk management community, including risk mitigation experts (CISOs, cybersecurity solutions providers); risk transfer experts (insurers); and other cybersecurity subject matter experts (the academic and scientific communities).

Enterprise risk owners could use the repository to anonymously share sensitive cyber incident data that then could be aggregated and analyzed – resulting in increased awareness about current cyber risk conditions and longer-term cyber risk trends. New analytics products, rooted in rich repository data, in turn could help inform more effective cyber risk management investments by both private and public sector organizations. An anonymized cyber incident data repository accordingly could make a major contribution to driving the Administration's critical infrastructure protection and national resilience goals.

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, and identifying 16 data categories needed to attain that value, the CIDAWG turned its attention to identifying and describing perceived obstacles to the voluntary sharing of cyber incident data and potential approaches to overcoming those obstacles. They are the subject of this white paper. As a next step in this dialogue, the CIDAWG will deliberate on how a cyber incident data 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.

Opinions expressed in this white paper are not necessarily reflective of the opinions of NPPD, DHS, the United States government, or any specific entity or person involved in the discussions leading to this paper.

Perceived Obstacles to Voluntary Sharing of Cyber Incident Data

Obstacle 1: Assuring Anonymization

This obstacle concerns challenges with assuring the privacy and anonymity of repository contributors while providing sufficient cyber incident details for effective and insightful analysis.

Perceived Concerns:

- Despite assurances of specific data being "non-attributable," the aggregation and analysis of cyber incident data, as detailed in the white paper titled, "*Enhancing Resilience Through Cyber Incident Data Sharing and Analysis: Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository*," could have unintended consequences in terms of sector-wide insurance rates. For example, aggregated data that shows the cascading consequences and total costs or impacts of certain types of incidents to certain industries could make some of the most common cyber incidents uninsurable or prohibitively expensive to insure.
- Large scale cyber incidents might make it possible to connect a particular exploit with a contributing company or companies, undermining the anonymity of the repository.
- A robust anonymization protocol that can withstand attempts at malicious disclosure could lead to a situation where the obfuscation of the data source renders shared incident data unverifiable. This "unverifiability" could undermine the repository's value because it might complicate efforts to assure the reliability of contributed data.

Possible Approaches:

The single most effective way to address these obstacles is effective trust-building. Potential mechanisms for promoting trust include:

- Non-Disclosure Agreements;
- Confidentiality Agreements;
- Terms of Service;
- Legal frameworks focused on compliance (duty to defend) and confidentiality, with provisions that protect information from being linked in any way to a contributor; and
- "Safe Harbor" legislation that protects repository contributors from subpoenas or liability on the basis of their anonymous contributions.

Beyond these policy approaches, protective technical measures could include using a sequential or randomized alphanumeric identifier that ensures that shared data can only be associated with an incident and not a contributor. Although the mechanism of entering data can create an association in system logs with the contributor's IP address, a two-server system with a manual transfer between them could better obfuscate data from malicious hackers to protect anonymity. Using such an approach, system administrators would be responsible for:

- Securely transferring the data between the input system and the system of record;
- Keeping an independent and separate correlation between the alphanumeric identifier and the contributing company should a reason later arise to connect them;

- Validating the legitimacy of the contributor (via background check); and
- Destroying original records as required by repository policy or by participants.

The success of the above policy and technical approaches would depend upon the competence and integrity of system administrators. In addition, a realistic balance between anonymity and verifiability will have to be carefully maintained in order to assure the value of the repository and its data to participating organizations.

Solution Stakeholders:

The CIDAWG membership could be a good starting point for engaging the appropriate mix of stakeholders and subject matter experts to develop anonymization policies and processes that maximize both trust in and value of a repository. These stakeholders could include a combination of insurers, CISOs, other cybersecurity professionals, industry sector representatives, privacy experts, and possibly audit firms with experience in validating policy implementation. In addition, any entity or organization that decides to host a future repository would be integral to the development and enforcement of its actual anonymization policies and processes.

Obstacle 2: Ensuring Data Security

This obstacle addresses the need to assure the integrity and confidentiality of both submitted data and system contributors, including the desire of contributors to retain control over their data and how it is used.

Perceived Concerns:

In addition to the importance of maximizing the security of the repository, contributing organizations would need to understand who will see their data and how they will use it. Specifically, repository contributors would want to know:

- That data access is limited in accordance with repository agreements/policy;
- That information is not disseminated to outside (unvetted) parties;
- How the data will be protected (e.g., will it be encrypted?);
- How the data will be managed (e.g., record retention policies, whether metadata would be retained for trending, whether contributors could modify or delete their own data, etc.); and
- The extent of third party (e.g., non-contributor, other contributor, and government) insight into the contributors' identity and data.

Possible Approaches:

The approaches for overcoming or mitigating this obstacle generally involve cybersecurity best practice guidelines for designed-in security, such as:

- ISO 27001-like compliance requirements – including people, process, and technology controls – as well as governance;
- Architecture/Database/Operating System Security Reviews;
- Continuous monitoring/authentication (this may be at odds with the twin goal of data anonymization);

- Response plans in the event of a breach;
- System and user behavior monitoring and analytics; and
- Operational procedures: access controls and usage monitoring.

Repository administrators should make judicious use of transparency mechanisms in order to reassure contributors about the security measures in place to protect the data they share. They should do so, moreover, in a way that does not provide a roadmap for malicious actors who might want to obtain and exploit that shared data. Finally, to address peer contributor vetting and access concerns, repository administrators should develop a pre-registration process that includes a background check based on appropriate criteria. Such a check would allow a repository's governing body, such as a board, to approve or disapprove the participation of particular entities.

Solution Stakeholders:

During any future repository planning effort, a legal working group would need to collaborate with a technical working group to establish and review needed legal protections. Both groups would need to engage subject matter experts responsible for developing the repository's data security and access policies and processes.

Obstacle 3: Cultural Challenges/Regional Differences

This obstacle is focused on the unique aspects of various cultures, countries, or regions that may affect voluntary cyber incident data sharing.

Perceived Concerns:

Many U.S. corporations have international ownership, presence, or significant overseas operations which may create several challenges for a repository, including the following:

- Some countries in which participating companies operate are reluctant to expose a weakness/vulnerability by reporting a problem. As a result, repository-identified cyber incident trends may be distorted because they may not include accurate information regarding incidents that local workforces are reluctant to report.
- Privacy laws or other local regulations in some countries may create difficulties in reporting.
- U.S. relationships or reputation in some regions or countries could affect participation. For example, some entities are reluctant to store data on systems in the U.S., based on the Snowden disclosures. Companies with an international board or other stakeholders accordingly may not be comfortable sharing data within a U.S.-hosted repository.
- Some sectors may be more eager/reluctant to participate than others, depending on their relationships with suppliers, consumers, and competitors, which could skew data analysis by over- or under-representing incidents in certain areas.

Possible Approaches:

Contextual information about an incident, such as what region the input comes from (e.g., U.S. or non-U.S.) may help analysts assess the reliability of the data. Several CIDAWG members suggest, however, that participation in a repository should exclude non-U.S. entities, at least during a proof-of-concept phase. Not only is it legally and technically complex to address disparate information sharing laws and customs, but also basing a prototype on a U.S.-only contributor base may help identify issues that would

need to be resolved prior to expanding beyond the initial implementation and participation group. The CIDAWG therefore recommended using a prototype phase to develop trust and prove the concept with U.S. participants, prior to expanding to non-U.S. entities.

Additional ideas for overcoming cultural reluctance to participation include:

- Repository contributions from hacked U.S. government agencies that are legally permitted and willing to share their breach and other cyber incident data could help enhance the perceived value of shared threat information. Such contributions also could help assure that information sharing between the government and the private sector is bi-directional and mutually beneficial.
- Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) could be engaged to educate, build awareness, encourage participation, and leverage existing trust relationships within specific sectors that are reluctant to contribute.

Solution Stakeholders:

The participation of ISAC and ISAO representatives in a repository proof-of-concept might encourage particular sectors to share cyber incident data. Appropriate contributions from hacked U.S. government agencies, as described above, may also make proof-of-concept participation more attractive.

Obstacle 4: Perceived Commercial Disadvantage

This obstacle addresses the likely concern by some companies that sharing cyber incident information could have negative business repercussions.

Perceived Concerns:

- Contributors to a cyber incident data repository might find it difficult to abandon the long-standing practice of keeping company data in house – particularly, incident information that either had damaging impact on a company or, if it has weathered an incident well, could damage competitors. In addition, companies may not want to devote the internal resources necessary to participate in a repository – especially if their competitors are not incurring those same overhead costs.
- Repository contributors must be able to trust that their sharing would not open them to liability, exposure, and/or otherwise negatively affect their business.

Possible Approaches:

- Despite the overall concerns regarding information sharing of sensitive data, repository developers should clearly communicate to potential contributors how repository data and resulting analysis could help illuminate the business case for particular cybersecurity investments in new technologies, people and processes. They should also emphasize that incident data sharing could help promote benchmarking against peer organizations that in turn would increase commercial competitiveness.
- Appropriate safe harbor legislation that shields companies from subpoenas and/or liability could help create the conditions necessary to incentivize sustained voluntary sharing into a repository.
- Future repository developers should engage organizations that already operate voluntary information sharing systems about the kinds of legal protections that they have in place to foster trusted information sharing environments. The Aviation Safety Information Analysis and

Sharing (ASIAS) database and Computer Emergency Response Team (CERT) are just two examples of potential models.

Solution Stakeholders:

Chief Risk Officers, CISOs, chief information officers (CIOs), company financial experts, and CEOs would be key solution stakeholders to overcome this obstacle.

Obstacle 5: Internal Process Hurdles

This obstacle concerns cultural and procedural challenges that may exist within contributing companies that could make information sharing difficult.

Perceived Concerns:

Many companies have internal processes governing the ability of their cybersecurity staff to participate in a voluntary cyber incident data sharing repository. Some examples include:

- Internal privacy regulations, legal reviews, and corporate information release/approval processes can be prohibitive when it comes to effective information sharing. They often involve the equities of many different offices whose cultural paradigms typically may not align well with an effort intended to rapidly release detailed information – albeit anonymously – regarding a cyber incident that may have serious corporate implications.
- Companies with limited resources may not want to engage in non-mandatory activities that create overhead burdens or otherwise tie up manpower.
- Certain sectors – for instance, the health services industry – may have specific legal obligations that could conflict with voluntary sharing.

Possible Approaches:

Several strategies for overcoming these challenges include:

- Appropriate "safe harbor" legislation that protects repository contributors from liability pertaining to the shared information could help overcome internal resistance.
- Communities participating in a cyber incident data repository, and the host/operator of the repository, could undertake an outreach or marketing campaign to overcome any reluctance to share. One model might be the DHS "See Something? Say Something!" campaign used by the Transportation Security Administration to detect and report possible criminal or terrorist activities affecting public safety at airports and other transportation nodes.
- Incentivizing companies to incorporate incident data reporting into their standard operating procedures (SOPs), such as benchmarking data sharing as a best practice, could help overcome this barrier.
- Transparency with regard to security and privacy, as well as demonstrated value to participating companies, will be crucial to normalizing voluntary reporting.
- Providing process tools, frameworks, guiding principles, and/or education and training about a repository and its purpose and value – in a way similar to how NIST introduced and developed the concept of its Cybersecurity Framework – may help overcome internal process hurdles, particularly for small or medium-sized companies that are inexperienced at gathering or making use of cyber incident data.

Solution Stakeholders:

Compliance and claims experts, privacy officers, general counsels, risk committees, and CISOs (for developing SOPs) are all important to overcoming likely internal hurdles to sharing. Most important, however, is leadership buy-in. Even the most entrenched internal obstacles can dissolve quickly if company leadership embraces the need for repository participation.

Obstacle 6: Perceived Value

This obstacle concerns the return on investment (ROI) from participating in a trusted and anonymized cyber incident data repository.

Perceived Concerns:

Building on the internal hurdles discussion pertaining to leadership buy-in, the CIDAWG discussed the need to constantly and clearly communicate the risk management advantages to companies that elect to voluntarily share cyber incident data into a trusted repository. In other words, repository proponents must be prepared to answer, with concrete examples, how repository contributors can expect to derive a return on investment (ROI) from their participation. In particular, members suggested that the specific value that a particular contributor might expect to gain from participation in the repository (i.e., through incident data sharing) must be made clear.

Possible Approaches:

The specific questions, "what does a contributor gain" and "what is the return on investment" are addressed at length in the CIDAWG's Value Proposition white paper. The renewed discussion about incentivizing repository participation, however, highlights the need for further consideration of this question – specifically, how to personalize the value of that participation so individual contributors can see a direct correlation between participation in cyber incident data sharing and received benefit. In addition to the six core value propositions listed in the CIDAWG's Value Proposition white paper, therefore, participation in the repository must demonstrate value specific to each company. In order to clearly convey such advantages, consideration should be given to several strategies:

- Companies are more likely to adopt risk management approaches that their peers claim are useful. Early adopters (and/or the developer) of a repository accordingly could publish white papers to advertise its benefits. One successful model for such "marketing" information could be the use cases developed by companies after the release of NIST's Cybersecurity Framework that showed the value of adopting that framework.

- Future repository developers should conduct an educational campaign that consists of executive summaries, technical presentations, training workshops, and public statements. Targeted messaging to different groups could highlight particular value that might appeal to their members. Developers could offer workshops and webinars to help companies understand how to "use" a repository and why participation in a repository is valuable, in a way similar to how NIST introduced the Cybersecurity Framework to industry.

Solution Stakeholders:

In addition to technical and corporate stakeholders mentioned in previous solutions, marketing teams should be involved at both the developer/administrator and company participant level. Their participation would help ensure that repository contributors remain aware of and committed to the value gained from the voluntary sharing, aggregation, and analysis of cyber incident data.

Obstacle 7: Assuring Appropriate, Adequate and Equitable Participation

This obstacle concerns the effect that the participation of others might have on the value of a repository. There are three aspects to this obstacle: (1) assuring appropriate participation, which is related to access control; (2) garnering adequate participation, to ensure the volume and variety of data is sufficient to achieve envisioned value; and (3) overcoming concerns about insufficient and inequitable participation by other contributors.

Perceived Concerns:

1. Appropriate Participation

- Repository contributors will want to know that other participants in a repository are peer organizations, or are in other ways comparable to their own (e.g., members of the same industry sector). This will help ensure that cyber incident data contributed by those peer organizations can support meaningful analysis when aggregated with their own.
- Because of the specific types of information that the kind of repository envisioned here would hold, some of which might have regulatory implications, participants likely will insist that it not be owned, operated, or controlled by the Federal government. In addition, participants likely will seek assurances that government access to aggregate information is explicitly approved by a governing body of repository contributors.

2. Adequate Participation

During its initial operations, a future repository might experience low participation rates occasioned by reluctance to be "first" and/or potential stigma associated with early adoption.

3. Equitable Participation

If only a handful of companies contribute the vast majority of data into a repository, they might conclude that they effectively are being "penalized" for sharing – in other words, they give more than they get. This "free rider" problem may lead some contributors to stop participating.

Possible Approaches:

- A future repository likely will need to be developed and hosted by a non-government entity(ies) and/or organization(s), with the extent and nature of Federal government engagement to be determined and approved by the repository's governing body.
- In order to encourage participation through benchmarking, a repository could employ some kind of "tag," recognition, or other benefit to individual organizations that would accrue only after they share incident data.
- Participation rates could be obfuscated during the early phase of implementation when participation by relatively few users might create a false impression that the repository "isn't working" or is not valuable to its contributors.
- Repository administrators could make data contribution the "price of admission," which would address both the appropriate participation and "free rider" problems. Only those organizations that are (1) vetted; and (2) share information could take advantage of the information shared by others. This would increase the perceived value of a repository by assuring contributors that their peer participants are equally invested in sharing data to inform cyber risk management practices. However, as some members observed, such a provision would limit the ability of

legitimate but non-contributing entities, such as researchers, to take advantage of a unique opportunity to analyze aggregated cyber incident information. A compromise approach might be to require that entities desiring access to repository data be vetted by the repository membership or some designated authority. This would allow participants to require participation in return for access for commercial peers, yet allow access on a case-by-case basis to other interested parties based on rules that a repository's governing body determines.

Solution Stakeholders:

In developing solutions to these obstacles, CIDAWG members suggested involving academic institutions, Computer Emergency Response Teams (CERTs), Federally Funded Research and Development Centers (FFRDCs), legislators/lobbyists, and General Counsels.

Obstacle 8: Technical Design Issues

This obstacle includes a combination of several related concerns about the actual functioning of a repository – specifically, how that functioning affects voluntary information sharing. These concerns are grouped under Ease of Process and Data Input and Display.

1. Ease of Process

Perceived Concerns:

A repository might add to a company's reporting or staffing burdens – especially during the response phase of what might be a major cyber incident. The following questions accordingly should be considered during a future repository design phase:

- How easy is it for contributors to access and use repository data?
- How easy is it for contributors to input and change data that they share into a repository?
- What is the level of effort necessary for contributors, within their own organizations, to obtain and to provide data, given the data may come from many different locations?

Possible Approaches:

Repository developers could:

- Design questions for a repository input template that are relevant and easy to understand and to answer – e.g., with hover buttons and pull-down menus;
- Ensure user-friendly human interfaces – e.g., provide parenthetical information to help users understand definitions, the purpose of questions, etc.;
- Consider providing data collection guidance that will allow company leadership to approve release of the information prior to sharing it into a repository. A well-designed repository input template also could help users improve their root cause analysis capabilities by guiding the user to the right functional areas with the right questions; and
- Consider integrating a common forensics reporting tool, such as the STIX/TAXII tool, that allows the inputting of data in common formats for more effective sharing.

2. Data Input and Display

Perceived Concerns:

The CIDAWG also focused on how data inputs should be governed to prevent, for example, double-reporting, and how data should be displayed or accessed after it has been entered. Repository developers must consider the following questions:

- How should a repository verify that each cyber incident has only one reporter – for instance, when incidents affect multiple parties?
- How should access be provided to shared cyber incident data?
- How will repository guidelines or documentation ensure a common lexicon or frame of reference for data elicitation and sharing?
- Will the information be displayed in a way that could potentially violate confidentiality and/or reveal too much about the contributor?
- How should a repository control what can be accessed/downloaded by entities other than the original contributor?

Possible Approaches:

Several of these concerns reflect those expressed in *Obstacle 1: Anonymization*. The CIDAWG agreed that the approaches identified for overcoming that obstacle should be applied as design considerations. Additional approaches might include the following:

- Multiple reports about a single cyber incident that affects several organizations are not only likely but desirable, because part of the value of a repository is the ability to capture cascading effects and total costs/impacts. Therefore, there needs to be a way to indicate when incidents are linked to a single source event, like a regional incident where multiple companies are impacted (e.g., a cloud provider that loses data for 10 companies). Designers should develop a way to separate, on the one hand, identifiers used by organizations to track and access their own data and, on the other, identifiers used for the incident itself.
- Information must be easy to understand. There should be a dictionary of terms, ease of access to the system fields (e.g., through a browser), and effective visualization and data mining tools – in short, the kinds of built-in technical assistance that could help contributors easily conduct analysis.
- In order to protect confidentiality, there should be clear direction, information, and rules about appropriate repository usage, such as prohibitions against downloading all its data or selling aggregated information.
- Designers should consider adopting role-based access control for data display – i.e., academics, insurers, CISOs, and other contributors could have access to different information.
- A means of measuring how well the system is meeting the needs of participants – that is, anonymized metrics assessing the performance of the repository itself – should be included in its design.

Solution Stakeholders:

Solution stakeholders should include IT systems experts, including auditors, Chief Data Officers, data scientists, and a data analytics team. CISOs, Chief Security Officers (CSOs), Directors of Security,

governance representatives, and NIST experts also should participate as security SMEs. Moreover, because CIOs typically own the resources through which participation in a repository would be conducted, they also should be included in design discussions. Their inputs will likely focus, for example, on the resources required to implement and use a given design effectively. Finally, entities with extensive experience in survey design should be included in order to ensure that the questions that a repository uses to elicit shared data do not skew the information provided.

Conclusion

The CIDAWG discussions summarized in this paper address the third topic – *Incentivizing Voluntary Data Sharing* – of a four-topic dialogue about how a trusted and anonymized cyber incident data repository could be leveraged to improve the overall cybersecurity 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 through a repository, could support analysis that informs:

- Day-to-day risk mitigation strategies of CISOs, CSOs, 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.

As a next step in this dialogue, the CIDAWG will deliberate on how a cyber incident data 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.