2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure

Daniel Kapellmann
Cyber-Physical Threat Intelligence
Senior Analyst
FireEye
Reston, VA, USA
danielkapellmann.z@fireeye.com

Rhyner Washburn
National Consortium for the Study of
Terrorism and Responses to Terrorism
(START)
Research Affiliate
University of Maryland
College Park, MD, USA
rhynerwashburn@gmail.com

Abstract: Vulnerability management remains a significant challenge for organizations that handle critical infrastructure worldwide. Hallmark cyber-physical incidents with disruptive and destructive capabilities like Stuxnet (2010) and Triton (2017) have exploited known vulnerabilities in information technology (IT) and operational technology (OT) assets throughout the attack lifecycle. However, the global critical infrastructure security community is still nascent in the field of industrial control systems (ICS) vulnerability management, especially in information-sharing. While their counterparts in IT security have spent years elaborating multiple resources to track and disseminate information about known vulnerabilities, the ICS community lacks specialized mechanisms for knowledge-sharing. Multiple challenges exist when addressing this issue: a general lack of awareness about ICS cybersecurity, the need to consider multiple industry sectors and unique network architectures, and the need to find a balance between protecting and releasing sensitive information regarding critical infrastructure organizations or proprietary vendor knowledge.

* Opinions and findings from this paper are solely the authors' and do not necessarily reflect the views of their organizations.

Through a multiphase research initiative based on the user-centered design process, we intend to test and evaluate the feasibility and effectiveness of various information-sharing platform designs for streamlining the discussion of ICS vulnerabilities. In the first phase of this research, we surveyed ICS and critical infrastructure security stakeholders to gain insight into the range of cogent, shared, and divergent views of the community relating to the need for specialized resources to share information about ICS vulnerabilities. We then evaluated what these different perspectives imply for the adoption and success of certain information-sharing platform frameworks. Finally, utilizing these insights, we demonstrated possible alternative paths forward for addressing the challenge of sharing information about ICS vulnerabilities to keep critical infrastructure safe.

Keywords: *Vulnerability management, critical infrastructure, industrial control systems (ICS), norms and standards, cyber-physical, information-sharing*

1. INTRODUCTION

On December 2017, the US National Cybersecurity and Communications Integration Center (NCCIC) publicly released an in-depth analysis of the TRITON/HatMan malware framework [1]. For the first time, the industrial control systems (ICS) community learned about threat actors developing malware specifically to compromise safety instrumented systems (SIS) from critical infrastructure facilities, with potentially disruptive or even destructive implications. According to the report, two vulnerabilities in the Schneider Electric Triconex Tricon were exploited during the incident [1]. This was, however, not the first time that known vulnerabilities in ICS had been leveraged as tools during major cybersecurity incidents. In 2010, threat actors exploited vulnerabilities in Siemens S7 and WinCC during the Stuxnet attack lifecycle, resulting in the disruption of Iranian centrifuges [2]. In 2016, a denial-of-service (DoS) vulnerability in Siemens SPIROTEC products was exploited in Ukraine's power grid to render devices unresponsive and generate a power outage [3].

Industrial control systems are used to monitor and control physical processes for industrial production. They are a key component of critical infrastructure organizations, which are characterized for their importance to the national economic security, public health, and safety of a country [4]. Compromises of ICS are usually not the product of the exploitation of single vulnerabilities: they require threat actors to combine multiple techniques, tactics and procedures (TTPs) to move laterally across networks, and normally involve multilevel exploits at different points of an organization's

network architecture [5]. However, single ICS vulnerability exploitation can also result in harm to critical infrastructure or industrial environments. This is mainly true in the case of internet-connected ICS that contain off-the-shelf embedded software. Multiple open source tools such as the Industrial Exploitation Framework (ISF) and Immunity Canvas Gleg Packs have been released to exploit vulnerabilities in ICS components. [6, 7] Following this premise, vulnerability management represents a key component of a defense-in-depth security approach as it enables organizations to address known weaknesses in key operational technology (OT) assets. Asset managers are challenged to perform timely vulnerability assessments and implement patches, updates or compensating controls to address vulnerabilities that are publicly disclosed (even to threat actors) in multiple open source repositories.

Despite the increase in the complexity of adversaries targeting ICS in critical infrastructure, the community continues to struggle to enforce standards that enable efficient information-sharing, which can help organizations implement vulnerability management programs. Most current mechanisms are based on solutions designed to address the needs of the information technology (IT) community, which responds to different priorities. In the IT domain, the cybersecurity priorities are the confidentiality, integrity, and availability of data. In contrast, critical infrastructure organizations prioritize the safety of people and equipment, and the reliability of physical processes [8]. Additionally, the identification and mitigation of vulnerabilities in IT systems is normally achieved leveraging automated tools and scanners [9]. In the case of ICS, organizations require thorough planning to establish vulnerability assessment methodologies, because failed attempts to mitigate weaknesses can cause instability, performance issues, or even a system crash [10]. Strategies to patch vulnerabilities in ICS are highly complex, due to the need to consider factors such as system architecture, configurations, costs and benefits of downtime, bandwidth limitations of legacy devices, equipment that is insecure by design, and vendor interoperability. As a result, the ICS cybersecurity community requires solutions that are tailored to address their specific information needs for ICS vulnerability management.

This paper is the foundation for a multiphase project. We apply the user-centered design process to test and evaluate the feasibility and effectiveness of different information-sharing platform designs for streamlining access to data about ICS vulnerabilities. In the first phase of this research, we distributed a survey to ICS security stakeholders to gain insight into the range of cogent, shared, and divergent views of the community relating to the need for specialized resources to share information about ICS vulnerabilities. We then evaluated what these different perspectives implied for the adoption and success of certain information-sharing platform frameworks. Finally, utilizing these insights, we demonstrated possible alternative paths forward. We highlight that, to the authors' knowledge, there is no pre-existing literature addressing

the challenge of information-sharing for vulnerabilities from the ICS perspective.

2. INFORMATION-SHARING PLATFORMS

In 2013, Luc Dandurand and Oscar Serrano discussed the need of the cybersecurity community to develop tools to facilitate information-sharing and automation, in order to efficiently handle information about vulnerabilities, threats, and incidents. The authors identified that at the time most information-sharing mechanisms lacked interoperable standards, data quality validation, and mechanisms to govern and control the use of sensitive information. To address these challenges, they defined the Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) concept, with the objectives of facilitating information-sharing, enabling automation, and fostering interorganizational collaboration [11]. The paper was focused on IT vulnerabilities, and preceded a series of improvements over the years for cybersecurity information-sharing. However, it did not evaluate sources pertaining to ICS vulnerabilities present in critical infrastructure.

The International Association of Crime Analysts (IACA) defines an information platform as a

> centralized computer system that allows authenticated users to collect, manage, share, and discover structured and unstructured datasets from a variety of sources. It is designed to facilitate two-way communication between users … serve as a channel for official and unofficial communication to facilitate top-down, bottom-up, and lateral communication.

The design of information-sharing platforms is based on multiple considerations, which include but are not limited to the types of entities sharing information, membership diversity, the types of exchanged information, the models used to access information, and the users' needs [12, 13, 14, 15].

Information-sharing platforms are intended to provide people or organizations from specific communities with the ability to access historic information, generate knowledge, and define future insights [12]. According to the European Network and Information Security Agency (ENISA), the main incentives for information exchange are economic benefits stemming from cost savings, and benefits from the quality, value, and use of shared data. Information-sharing mechanisms are economically valuable for organizations to streamline decision-making processes and define resource allocation. However, a key challenge to information-sharing is addressing

misaligned economic incentives, given the reputational risks it poses for companies disclosing information [16].

Multi-stakeholder collaboration promotes the creation of quality data by concentrating multiple sources of information. However, high quality data requires the fulfillment of certain conditions, including timeliness, specificity, relevance to address the participants' concerns, and a suitable level of granularity [16]. Further research identifies quality and trustworthiness of data as key requirements for inter-organizational information-sharing. The author suggests four main considerations for trustworthiness: the perceived competence of other parties sharing information, openness, trust issues between parties, and reliability/consistency with which information is released [17]. In the next section, we present the landscape of information-sharing, specifically in the case of ICS vulnerabilities.

3. EVOLUTION OF ICS VULNERABILITIES INFORMATION-SHARING

Information-sharing is currently a controversial topic for ICS stakeholders. The community traditionally relied on a model known as "security by obscurity", where industrial networks relied on proprietary assets and were isolated from business networks [18]. Information about systems architecture and characteristics of ICS assets was exposed only to small groups of people to hide vulnerabilities from adversaries. However, "security by obscurity" is no longer appropriate for ICS, given the increasing integration between corporate IT and modern control system architectures [19]. The ICS community is divided between those who believe information about threats and vulnerabilities should not be shared, and those who believe that greater communication between organizations would improve preparedness against adversaries. Other considerations concern whether information-sharing would divert efforts from other more essential security controls, or whether the quality of shared contents and misinterpretations might generate adverse impacts [20].

Interest in ICS cybersecurity began to proliferate in 2010, parallel to the publication of "Protecting Industrial Control Systems from Electronic Threats" by Joe Weiss. Among other topics, the author elaborated on the lack of significant data to demonstrate ICS cybersecurity cases to executives, given the unwillingness of organizations to share information about incidents. He suggested the need for an ICS Computer Emergency Response Team (CERT) to centralize information from multiple stakeholders, process it and share insights with the community [5]. In 2011, the Stuxnet incident targeting Iranian critical infrastructure was publicly recognized. This caught the attention of the international cybersecurity community and drove a significant increase in ICS-

specific vulnerability disclosures [21]. The incident highlighted the relevance of ICS cybersecurity as a key component of national security.

While information about threats and incidents against ICS is still handled discreetly, data related to vulnerabilities in assets is already commonly shared by public and private organizations in different platforms. However, private organizations have highlighted the low quality and integrity of public advisories [22]. Some of the most common platforms are vulnerability repositories, Information-Sharing and Analysis Centers/Information-Sharing Analysis Organizations (ISACs/ISAOs), and ICS vendor advisories. Other sources that are not further discussed in this paper include researcher websites and private industry services. Specialized online forums, such as the SANS ICS community, provide a platform for discussions among ICS cybersecurity practitioners, although none of these forums specifically addresses vulnerabilities. Furthermore, international regulation, such as the European Network and Information Security Directive (NIS), currently stresses the need for information-sharing about threats, incidents and vulnerabilities between different stakeholders [23].

A. Vulnerability Repositories

Online repositories are the most common information-sharing platforms for vulnerabilities. Information from the Vulnerability Database Catalog of the Forum of Incident Response and Security Teams (FIRST) indicates there were at least 22 officially recognized vulnerability databases by March 2016 [24]. Data about weaknesses in electronic components is abundant, as reflected by the United States National Vulnerability Database (NVD) which disclosed more than 15,000 vulnerabilities in 2018; however, the number of repositories releasing specialized information about ICS vulnerabilities is very low [25]. The most recognized repository for ICS vulnerabilities is ICS-CERT, which was created in 2009 and placed under the command of the US NCCIC in 2018 [26]. ICS-CERT not only releases information about ICS vulnerabilities, but also collaborates with vendors and researchers to coordinate the process of responsible disclosure. While ICS-CERT advisories are tailored for the ICS community and provide a higher granularity of data than other repositories, the platform still faces significant challenges.

Three main challenges are: concentrating information about ICS vulnerabilities from multiple sources using different data structures; elaborating practical mitigation recommendations that satisfy the needs of the ICS community; and organizing information in accessible and consumable formats [27, 28]. Other recognized repositories that contained information about ICS vulnerabilities were owned by Critical Intelligence [29] and the Open Source Vulnerability Database (OSVDB) [30]. Both databases disappeared between 2015 and 2016 due to the intense manual input

required to concentrate the information, and low returns on investment. More recently, the Zero Day Initiative was launched by a private sector organization to reward researchers for vulnerability disclosure. While it does not contain only ICS-tailored information, it has encouraged collaboration with researchers for the disclosure of vulnerabilities.

B. ISACs and ISAOs

ISACs are mechanisms formed by critical infrastructure owners and operators to gather, analyze, sanitize and disseminate information between public and private stakeholders. These organizations are crucial for public-private collaboration in sharing information about vulnerabilities, threats, intrusions and anomalies, mostly in critical infrastructure sectors [31]. The value of ISACs depends on the collective consensus of the members and their willingness to share information. Some examples of ISACs from different sectors are: Electricity (E-ISAC), Oil and Natural Gas (ONG-ISAC), Mining and Metals (MM-ISAC), Maritime (Maritime-ISAC), and the Industrial Control Systems (ICS-ISAC) [29]. In 2015, the Obama administration issued an Executive Order introducing ISAOs as an alternative to address some of the information-sharing limitations of ISACs. These organizations seek to "encourage the formation of communities that share information across a region or in response to a specific emerging cyber threat." [32] Information shared within the ISACs is only communicated among members, limiting their value to the external community.

C. ICS Vendor Advisories

The disclosure of ICS vulnerabilities is highly reliant on the collaboration of commercial product vendors and service providers. While it is not in the scope of this paper to discuss the process of coordinated and responsible disclosure, ICS vendor advisories remain one of the most in-depth sources of information about vulnerabilities. Some of the main vendors of ICS products have invested in developing specialized platforms for sharing information. For example, both Schneider Electric's Cybersecurity Support Portal, and Siemens ProductCERT release regular vulnerability advisories [33, 34].

D. New Media

In 2016, a report from FireEye defining critical lessons from 15 years of ICS vulnerabilities indicated that "media coverage of significant events in ICS security, either attacks or research, will likely continue to fuel the vulnerability disclosure rate." [21] While there is no formal research published about the role of media in sharing information about ICS vulnerabilities, some specialized news outlets regularly share this information. An example is Security Week, which regularly releases notes expanding on the information released in vendor advisories and publications from vulnerability repositories [35]. Social media has also been a tool used by reputable

ICS organizations and experts: for example, ICS-CERT releases regular advisory notifications [36].

4. RESEARCH DESIGN AND METHODOLOGY

Despite the variety of information-sharing platforms available, it remains unclear to what extent they meet the needs of the ICS security community. To address this lack of assessment on information sources supporting ICS vulnerability management and ascertaining what information the ICS community values, we elected to design a subject matter: expert elicitation. Our primary tool for elicitation was a web-based survey, which we distributed among ICS stakeholders in the private, public, academic, and non-profit sectors. The survey was mainly shared on recognized community forums and remained open for one month. It consisted of 22 questions focused on participant background, access to ICS vulnerability data, information needs, and ideal methods for collecting or sharing such information. The seventh question filtered respondents who did not access information about known ICS vulnerabilities. The full questionnaire is available in Appendix A.

For this survey, we attempted to recruit across multiple professional domains and industries. To this end, instead of individually identifying participants, we sent the survey to specialized ICS forums including SANS-ICS community, the Industrial Control Systems Joint Working Group (ICSJWG), and the International Society of Automation (ISA). We also reached out to a select few individuals who are thought leaders or experienced in the ICS and critical infrastructure community, to further spread the survey. Even though convenience sampling implies an intrinsic risk of volunteer bias, we chose this method to identify individuals who were particularly interested or experienced in ICS vulnerabilities. This was mainly relevant to reach a representative sample despite the small size of the population with expertise on this topic.

There are currently no official estimates of the size of the ICS cybersecurity community, for multiple reasons. ICS cybersecurity is a young discipline, spread through diverse industries, that requires skills from multiple disciplines, and has only recently begun to be defined as a knowledge field. After exhaustive research, we decided to adopt as an estimate the number of members present in SANS ICS invitation-only forum, which is 6,300 [37]. However, we recognize that the forum does not only include members actively participating in ICS vulnerability management. Members range from security analysts and ICS owners, to sales representatives, managers, and anyone who has learned the basics about ICS security. As we were unable to capture data of how many people the survey did reach, we could not ascertain an accurate survey response rate.

The first section of the survey contained questions about the previous experience and demographics of the sample. The second section began by asking participants about their habits for accessing information pertaining to ICS vulnerabilities, then identified the main challenges they faced in using this information, and finally asked about their information needs. We added an additional field for comments and invited participants to provide their emails for follow-up interviews during the next phases of the research initiative. We employed descriptive statistics and exploratory data analysis to draw understanding from the participants' responses.

In 2015, Hollifield and Perez released a White Paper showing how designing usable human-machine interface (HMI) displays that fulfilled the needs of operators could improve their capacity to manage physical processes [38]. Our methodology seeks to adopt a similar approach for the design of ICS information-sharing platforms, recognizing that what currently exists follows patterns set by the IT community and does not meet the unique needs of ICS users. In the following section, we present an initial survey of users' needs and preferences to guide the creation of prototype tools for ICS vulnerability information-sharing.

5. FINDINGS AND DISCUSSION

A. Sample Description

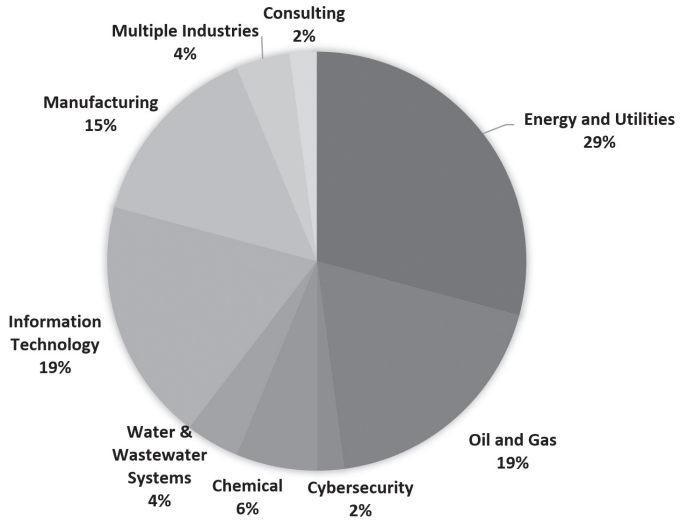
The survey captured 48 responses, of which four remained incomplete given that it was designed to exclude non-ICS stakeholders. While a bigger sample would provide higher statistical confidence, we consider that the present survey still provides highly valuable insights: as one of the first systematic efforts to identify the habits, challenges and needs of ICS stakeholders regarding ICS vulnerabilities present in critical infrastructure.

The survey was distributed in forums frequented by stakeholders from different backgrounds. Close to 98% of the individuals who elected to participate stated that they had technical backgrounds in areas such as engineering and computing science. More than 80% of the participants were employed in the private sector, but we also received responses from government, academia, and non-profit professionals. Close to 71% of the participants were currently occupied in the field of cybersecurity, followed by 15% from ICS engineering.

The main strengths of the sample were: a highly diverse group of participants from 15 different industries, with most participation from energy and utilities, oil and gas, information technology and manufacturing (as shown in Figure 1); and a reported

medium to high confidence level in cybersecurity expertise from 94% of participants. The main limitation was the small size of the sample. This can be explained mainly by two factors: the previously discussed small size of the ICS cybersecurity community, and some individuals declining to participate due to concerns about sharing information. It is also possible that the lack of active discussion and interest impacted our response rate.

FIGURE 1. DISTRIBUTION OF THE SAMPLE BY INDUSTRY.



B. Habits, Challenges and Needs Pertaining to Information-Sharing for ICS Vulnerabilities

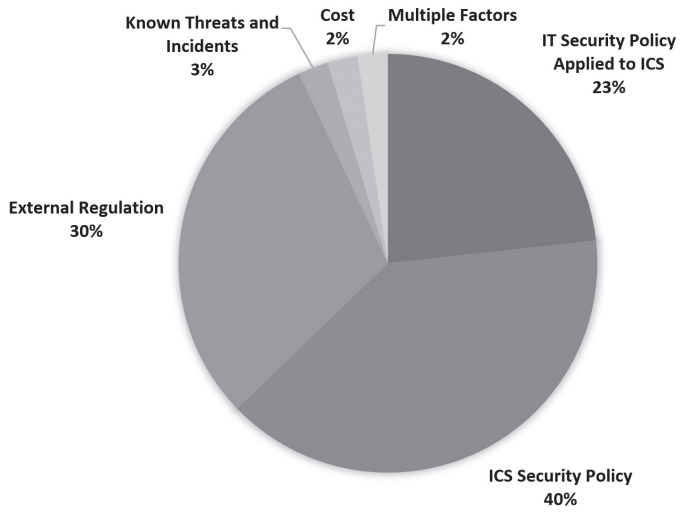
We categorized survey questions into three sections, to explore the current habits of the ICS community, the challenges they face, and their preferred mechanisms for fulfilling their ICS vulnerability information needs. An additional section is provided to share insights presented by survey responders beyond questionnaire requirements.

1) Habits

Most respondents were intensive consumers of information about ICS vulnerabilities. At least 61% accessed this information daily or weekly, and 20% monthly. The most common purposes for access were general awareness (learning about trends and new threats), research, vulnerability management, risk management and compliance with regulations. Figure 2 shows that despite the unique needs of ICS security, only 40% of the respondents considered ICS security policy to be the main factor driving ICS vulnerability management in their organization. In contrast, 30% considered it was

mostly driven by government regulations, and 23% expressed it as IT security policy applied to ICS. This highlights the common adoption of IT resources to facilitate ICS cyber security, and the strong role of government regulations in vulnerability management.

FIGURE 2. MAIN FACTOR THAT DRIVES ICS VULNERABILITY MANAGEMENT IN RESPONDENTS' ORGANIZATIONS.



The primary avenues used by participants to access information about ICS vulnerabilities were ICS/US-CERT (77%), ICS vendor websites (57%), news and media (52%), and the NVD (39%). Participants demonstrated interest in multiple sources of information. Figure 3 illustrates the co-occurrence of source usage. The most common combinations included ICS/US-CERT, vendor websites, and the NVD. We highlight the prevalence of news and media as a source of information, given that a higher quality of information is regularly expected from validated sources such as CERTs and vendor websites. ICS/US-CERT and vendor websites both offer detailed vulnerability advisories, but lack support for checking multiple vulnerabilities at once. Finally, though the NVD contains the most information about vulnerabilities, identifying specific ICS vulnerabilities remains a challenge. Two survey participants noted limitations with this database, including improper association between vulnerabilities, product names as they are known by engineers in the field, and misrepresented risk ratings. These limitations result from the repository's original intention to share information about IT vulnerabilities. ICS products commonly have multiple components of firmware, hardware and software, which makes their naming more complex. In the case of risk ratings, most repositories utilize the CVSS,

which does not account for damage caused by vulnerabilities to processes, people or equipment [39].

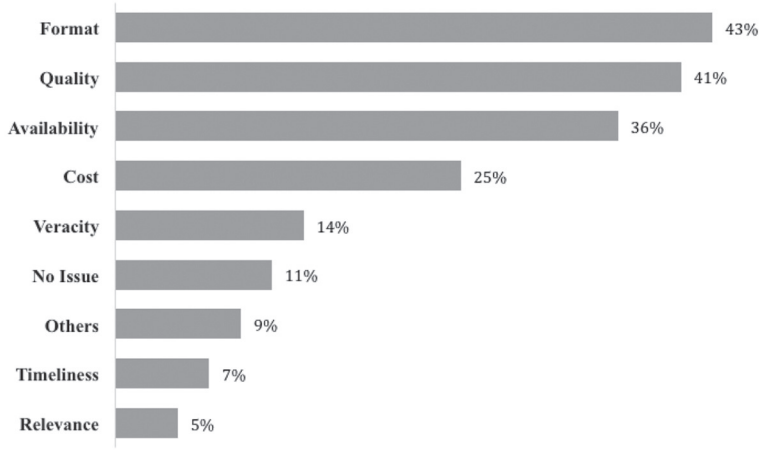
FIGURE 3. CO-OCCURRENCE OF PRIMARY AVENUES USED BY PARTICIPANTS TO ACCESS INFORMATION ABOUT ICS VULNERABILITIES.

	News & Media	ISACs	NVD	ICS/US-CERT	ICS Vendors	Private Industry	Others
News & Media	52%	14%	14%	39%	30%	11%	2%
ISACs	14%	30%	16%	27%	20%	16%	0%
NVD	14%	16%	39%	36%	27%	16%	2%
ICS/US-CERT	39%	27%	36%	77%	43%	23%	2%
ICS Vendors	30%	20%	27%	43%	57%	14%	0%
Private Industry	11%	16%	16%	23%	14%	25%	0%
Others	2%	0%	2%	2%	0%	0%	2%

2) Challenges

Close to 46% of the participants expressed dissatisfaction with the information they obtain through ICS vulnerability resources. At least half of those who expressed dissatisfaction also noted that their ICS security programs were mainly driven by risk management and compliance with regulations. This result can be driven by the high cost and complexity of regulatory requirements. When support from executives is limited, practitioners are challenged to find alternatives for compliance despite this. Figure 4 shows that the main barriers identified by participants in accessing the information they need about ICS vulnerabilities were the data format (43%), quality of information (41%), availability (36%), and cost of good information (25%).

FIGURE 4. MAIN BARRIERS TO FINDING INFORMATION ABOUT ICS VULNERABILITIES.



One of the participants who identified the format of information as one of the main challenges included a comment highlighting the inability of his organization to filter large amounts of data to identify risks pertaining to assets. In fact, the most commonly accessed resources (vendor advisories and ICS/US-CERT) are not accessible in single data repositories that enable analysis of multiple vulnerabilities at the same time. In the case of NVD, the large amount of information from IT vulnerabilities makes it difficult to address specific ICS needs. Interestingly, only 11% of the respondents indicated they found no barriers. This shows that even though 54% of the respondents considered they were satisfied with the information they had access to, 89% believed that information-sharing for ICS vulnerabilities had room for improvements.

3) Needs

The last section of the questionnaire was intended to learn about the needs and preferences of the ICS community to access and share information about known vulnerabilities. Figure 5 illustrates the most popular selections for ideal platform design and co-occurrence of multiple choices. These results highlight possible compatibilities between different platforms to inform the future design of solutions and address information-sharing needs. Participants expressed most interest in vulnerability repositories/databases (68%) and alert feeds/notifications (64%), with 50% expressing interest in both. The findings highlight the demand for an ICS vulnerability repository that provides a consumable format for analyzing multiple vulnerabilities at a time. Access to this repository would be preferred through newsfeeds and alerts (55%), an online dashboard (43.2%), application program interfaces (39%), XML or other markup languages (30%), or text reports (27%). Most participants (86%) prioritized

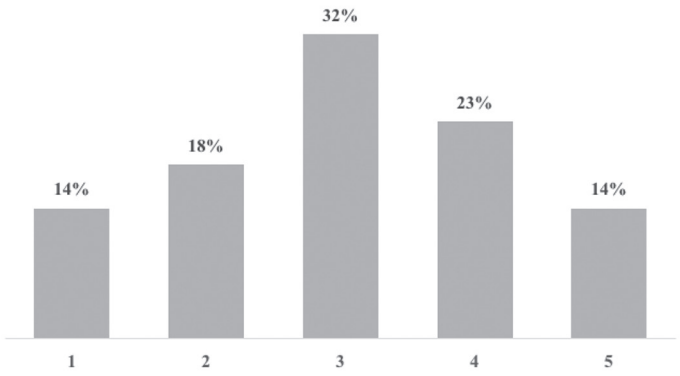
quality of information when selecting information platforms over the design itself. Other factors that drove preferences were usability of the platform (55%), the veracity of sources (50%), and accessibility of the platform (41%). Other popular platforms included regulated forums (45%), and community-driven forums (32%).

FIGURE 5. CO-OCCURRENCE OF PREFERRED TYPES OF PLATFORMS AS EXPRESSED BY PARTICIPANTS.

	Public Websites	Regulated Forums	Community-Driven Forums	Education or Training Platform	Vulnerability Repositories/ Databases	Social Media	Alert Feeds/ Notifications
Public Websites	27%	9%	5%	7%	20%	2%	18%
Regulated Forums	9%	45%	18%	9%	27%	2%	25%
Community-Driven Forums	5%	18%	32%	9%	20%	5%	18%
Education or Training Platform	7%	9%	9%	18%	11%	2%	11%
Vulnerability Repositories/ Databases	20%	27%	20%	11%	68%	7%	50%
Social Media	2%	2%	5%	2%	7%	9%	9%
Alert Feeds/ Notifications	18%	25%	18%	11%	50%	9%	64%

An additional finding (illustrated in Figure 6), indicated a normal distribution of participants expressing how comfortable they were sharing information about ICS vulnerabilities outside their organization on a scale from 1 to 5. The distribution corroborates that there is as yet no consensus on the topic among the community; though some members are open to sharing information, others are not. Willingness to share information about vulnerabilities may vary between stakeholders. For example, critical infrastructure organizations and ICS vendors commonly resist sharing information, while governments favor collaboration to improve the security of the community. Any solution that is implemented will require the consideration of both perspectives to become a widely used resource.

FIGURE 6. COMFORT WITH SHARING INFORMATION ABOUT ICS VULNERABILITIES OUTSIDE RESPONDENTS' ORGANIZATIONS RANKED FROM 1 (NOT COMFORTABLE) TO 5 (VERY COMFORTABLE).



4) Additional Highlights

From the 44 participants that completed the full survey, 52% provided their contact information to follow up through the research process. This shows a high level of engagement from participants in support of finding solutions to address the challenges discussed. One participant commented that some private sector products were beginning to offer more information about known vulnerabilities and potential mitigations. However, to the authors' knowledge, the listed solutions rely on comparing asset information with data from public repositories that use the Common Vulnerability Enumeration (CVE) format to identify matches. As a result, improvements in public repositories can result in a spillover to higher quality products for the private sector. Another relevant highlight was that vulnerability management requires a large amount of time and resources that is commonly understated by executives. Better quality information about ICS vulnerabilities may reduce the effort required for vulnerability management, increasing the level of preparedness of organizations against known threats.

6. MOVING FORWARD TO IMPROVE INFORMATION-SHARING FOR ICS VULNERABILITIES

Our survey provided a unique opportunity to gather insights from ICS stakeholders following principles from the user-centered design process to develop solutions that adapt to the needs of the industry. While IT software companies have long relied on user-centered methodologies to develop products and services, the ICS security community could still benefit from knowing what are the habits, challenges, and

needs of this specific population dedicated to protecting critical infrastructure systems. By publicly releasing this information, we hope to promote and formalize conversations about ICS vulnerability platforms, and spark thoughts with regard to design alternatives. We highlight that addressing ICS vulnerabilities is not only relevant for the private industry, but holds value as a key component to safeguard national security by protecting critical infrastructure processes and assets.

In this first paper, part of a series to identify alternatives for ICS vulnerability information-sharing platforms, we performed exploratory user research on members from the ICS community. Our findings corroborated an interest from most participants in improving ICS vulnerability platforms. While the sample was divided into a normal distribution in terms of comfort with sharing information, there was a consensus on the importance of improving the format, quality, and availability of data. An interesting finding was that most participants prioritized quality over other attributes. Therefore, the first challenge is to identify what information is useful for practitioners, and how to obtain this data given limited resources.

The survey also reflected valuable findings to guide the development of such a solution. Results indicated that an ICS vulnerability repository/database would be highly accepted by the community, mainly in combination with alert feeds and notifications. To a certain extent, ICS/US CERT, ICS vendor resources, and some private organizations issue notifications about new vulnerabilities. Next steps should, however, improve the quality of shared information and offer access in multiple formats to fit the needs of different organizations. Another alternative spawning from this paper is the elaboration of hybrid information-sharing platforms combining features from different models. A particularly interesting experiment would be to combine a vulnerability repository with regulated or community-driven forums. Even though there are currently no forums specializing in sharing information about ICS vulnerabilities, these were a popular idea among respondents. This type of interaction could enable participants to discuss alternative mitigations and clarify misconceptions on known vulnerabilities.

This survey was the first step in recognizing and formally documenting the needs of ICS security practitioners with regard to vulnerability sharing. Conclusions may be known to some and novel to others. Regardless of this, it provides a first step in developing tools based on the needs of actual users. We hope this paper motivates the community to develop alternatives with which we can jointly improve our ability to address ICS vulnerabilities.

7. FURTHER RESEARCH

This research paper provides a precedent to invite the ICS community to develop further research on mechanisms and platforms for sharing information about ICS cyber security. We find the results particularly valuable in guiding the implementation of prototype tools and processes to better address the vulnerability management needs of the ICS community. Further research may also explore the challenges of inter-organizational information-sharing for ICS vulnerabilities and define high quality standards for this data. Finally, as expressed by one of the survey participants, we recognize that information-sharing about threats, incidents, and impacts should also be prioritized as a promising field of study.

Acknowledgments

Thanks to the members of the ICS community who responded or distributed the survey. We thank Sean McBride, Nathan Brubaker, Jeffrey Ashcraft, Alicia Bargar, Margaret Morganti, and Ryan Serabian for their support. Rhyner Washburn also thanks Dr. Steve Sin for his guidance.

REFERENCES

[1] NCCIC, "MAR-17-352-01 HatMan-Safety System Targeted Malware (Update A)," *ICS-CERT*, 2018.

[2] E. Byres and S. Howard, "Analysis of the Siemens WinCC / PCS7 'Stuxnet' Malware for Industrial Control System Professionals," *Tofino Security*, 2010.

[3] A. Cherepanov and R. Lipovsky, "Industroyer: Biggest threat to industrial control systems since Stuxnet," 12 June 2017. [Online]. Available: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/. [Accessed 05 December 2018].

[4] Federal Emergency Management Agency, "Critical Infrastructure and Key Resources," [Online]. Available: https://emilms.fema.gov/IS520/PAN0101400text.htm. [Accessed 2 January 2019].

[5] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*, First Edition ed., New York: Momentum Press, 2010, pp. 63-86.

[6] Immunity, "CANVAS," [Online]. Available: https://www.immunityinc.com/products/canvas/gleg-products.html. [Accessed 22 March 2019].

[7] dark-lbp, "Industrial Exploitation Framework," [Online]. Available: https://github.com/dark-lbp/isf. [Accessed 22 March 2019].

[8] A. Ginter, *SCADA Security: What's broken and how to fix it*, Calgary: Abterra Technologies Inc., 2016.

[9] M. Chapple and D. Seidl, *CompTIA CySA+*, Indianapolis: Sybex, 2017.

[10] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Massachusetts: Elsevier, 2015.

[11] L. Dandurand and O. Serrano Serrano, "Towards Improved Cyber Security Information Sharing," in *5th International Conference on Cyber Conflict*, Tallin, 2013.

[12] International Association of Crime Analysts, "Information-Sharing Platforms," International Association of Crime Analysts, Overland Park, 2014.

[13] N. Sardjoe, "The Interrelation of Information Sharing Levels: Intra-organizational and inter-personal influences on inter-organizational information sharing," *TUDelft*, Delft, 2017.

[14] S. V. Sundar and D. E. Mann, "Effective Regional Cyber Threat Information Sharing," *MITRE Corporation*, Bedford, 2016.

[15] R. Krishnan, R. Sandhu, J. Niu and W. H. Winsborough, "A Conceptual Framework for Group-Centric Secure Information Sharing," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, 2009.

[16] N. Robinson and E. Disley, “Incentives and Challenges for Information Sharing in the Context of Network and Information Security,” *European Network and Information Security Agency* (ENISA), Heraklion, 2010.
[17] M. Ibrahim, “Interorganizational Trust and Interorganizational System’s Information Quality,” in *IQ*, 2005.
[18] E. Byres, “The Industrial Cybersecurity Problem,” *International Society of Automation (ISA) Research Triangle Park*, 2013.
[19] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,” *Homeland Security*, 2016.
[20] D. Peterson, “Info Sharing Bubble Burst of Everything Is A Success,” 4 October 2012. [Online]. Available: http://www.digitalbond.com/blog/2012/10/04/info-sharing-bubble-burst-or-everything-is-a-success/. [Accessed 11 November 2018].
[21] FireEye iSIGHT Intelligence, “Overload: Critical Lessons from 15 Years of ICS Vulnerabilities,” *FireEye*, Milpitas, 2016.
[22] Dragos, “Year in Review 2018 - Industrial Controls System Vulnerabilities,” 2018. [Online]. Available: https://dragos.com/wp-content/uploads/yir-ics-vulnerabilities-2018.pdf. [Accessed 18 February 2019].
[23] European Parliament and the Council of the European Union, “Directive (EU) 2016/1148 of the European Parliament and of the Council,” *Official Journal of the European Union*, pp. 6-11, 2016.
[24] FIRST, “Vulnerability Database Catalog,” 17 03 2016. [Online]. Available: https://www.first.org/global/sigs/vrdx/vdb-catalog. [Accessed 20 November 2018].
[25] National Institute of Standards and Technology (NIST), “Statistics Results,” [Online]. Available: https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all. [Accessed 20 November 2018].
[26] ICS-CERT, “About Us,” [Online]. Available: https://ics-cert.us-cert.gov/about-us. [Accessed 20 November 2018].
[27] R. Wightman, “Industrial Control Vulnerabilities: 2017 in Review,” Dragos, Hanover, 2018.
[28] D. Kapellmann, “Vulnerability Assessments in ICS Environments: Lessons Learned and Wishlist of Improvements,” in *Industrial Control Systems Joint Working Group Spring Meeting*, Albuquerque, 2018.
[29] C. E. Bodungen, B. L. Singer, A. Shbeeb, S. Hilt and K. Wilhoit, *Hacking Industrial Control Systems Exposed*, New York: McGraw-Hill Education, 2017.
[30] SCADAhacker, “SCADAhacker,” [Online]. Available: https://www.scadahacker.com/. [Accessed 22 March 2019].
[31] The White House, “Protecting America’s Critical Infrastructures: PDD-63,” Washington DC, 1998.
[32] Cyber Threat Intelligence Network, “ISAOS,” [Online]. Available: https://ctin.us/site/isaos/. [Accessed 23 November 2018].
[33] Schneider Electric, “Cybersecurity Support Portal,” [Online]. Available: https://www.schneider-electric.com/en/work/support/cybersecurity/overview.jsp. [Accessed 22 March 2019].
[34] Siemens, “Siemens ProductCERT and Siemens CERT,” [Online]. Available: https://new.siemens.com/global/en/products/services/cert.html. [Accessed 22 March 2019].
[35] SecurityWeek, “SCADA/ICS,” [Online]. Available: https://www.securityweek.com/scada-ics. [Accessed 22 March 2019].
[36] ICS-CERT, “ICS-CERT,” Twitter, [Online]. Available: https://twitter.com/ICSCERT. [Accessed 22 March 2019].
[37] SANS, “SANS ICS Community,” [Online]. Available: https://ics-community.sans.org/. [Accessed 22 March 2019].
[38] B. Hollifield and H. Perez, “Maximize Operator Effectiveness: High Performance HMI Principles and Best Practices,” PAS, 2015.
[39] I. Barda, “Increase in CVE Reports vs Long Field-Development - How to Manage the Conflict,” in *ICS Cyber Security Conference*, Atlanta, 2018.

APPENDIX A: RESEARCH QUESTIONNAIRE

Information-Sharing for ICS Vulnerabilities.
Thanks for agreeing to take part in this important survey to better understand the needs and preferences of the ICS community related to the quality and availability of information-sharing platforms for ICS vulnerabilities. This survey consists of 21 questions and is designed to gather insights from different types of stakeholders.

1. What do you consider to be your primary background?
   a. Technical (e.g. engineering or computing sciences)
   b. Non-technical (e.g. policy or social sciences)

2. Which of the following options best describes your sector of work?
   a. Academia
   b. Private sector
   c. Government (including military)
   d. Non-profit

3. Which of the following options best fits your industry?
   a. Energy & utilities
   b. Oil & gas
   c. Manufacturing
   d. Chemical
   e. Water & wastewater systems
   f. Retail/commercial
   g. Legal/regulation
   h. Telecommunications
   i. Information technology
   j. Financial
   k. Healthcare

4. Which of the following options best describes your current occupation?
   a. ICS engineering
   b. Policy and regulation
   c. Cybersecurity
   d. Business/management
   e. ICS Equipment vendor

5. Do you consider yourself a stakeholder in the ICS community?
   a. Yes
   b. No

6. Rate your experience in cybersecurity:
    a. 1 – Not familiar
    b. 2
    c. 3
    d. 4 – Very knowledgeable

7. Do you access information about known ICS vulnerabilities?
    a. Yes (Continue to next section)
    b. No (Finish survey)

No Access to ICS Vulnerabilities

1) Why do you not have access to ICS vulnerability information?
    a. Not relevant to my current job
    b. I am unfamiliar with ICS vulnerability resources
    c. My organization has no vulnerability management program
    d. My organization prioritizes other security controls
    e. Lack of resources (time or funding)

2) Do you have any additional comments or recommendations?

Access to ICS Vulnerabilities

1) How often do you access information about known ICS vulnerabilities?
    a. Daily
    b. Weekly
    c. Monthly
    d. Quarterly
    e. Biannually
    f. Yearly
    g. Less than a year

2) For what purpose do you access this information? (Choose all that apply)
    a. General awareness: learning about trends and new threats
    b. Research: analysis, disclosure or assessment of ICS vulnerabilities
    c. Risk management & compliance: performing risk or vulnerability assessments
    d. Vulnerability management: mitigation of vulnerabilities in ICS

3) Based on your experience, what is the main factor that drives ICS vulnerability management in an organization?
   a. External regulation
   b. IT security policy applied to ICS
   c. ICS security policy

4) What are your primary avenues for accessing information about ICS vulnerabilities? (Choose all that apply)
   a. News and media
   b. Information-sharing and analysis centers (ISACs)
   c. National vulnerability database (NVD)
   d. ICS-CERT/US-CERT
   e. ICS vendor websites
   f. Private industry resource

5) Are you satisfied with the information you are getting through those services?
   a. Yes
   b. No

6) What are the main barriers you encounter to find the information you need? (Choose all that apply)
   a. Cost: good information is costly
   b. Availability: I can't find any information
   c. Format: information is not digestible
   d. Quality: information is subpar
   e. Veracity: sources are not trustworthy
   f. No issue: I do not find any barriers

7) What granularity of data would best satisfy your information needs related to ICS vulnerabilities
   a. 1 – Very broad (Only ID, name, description and resources)
   b. 2
   c. 3
   d. 4
   e. 5 – Very specific (In-depth description containing associated source code, scenarios, requirements for exploit, etc.)

8) What type of platforms do you think would best fit your organization to share or access information about known ICS vulnerabilities?
   a. Public websites
   b. Regulated forums
   c. Community-driven forums
   d. Education/training platform
   e. Vulnerability repositories/databases
   f. Social media
   g. Alert feeds/notifications

9) What factors mostly influenced your choice of best information-sharing platforms for ICS vulnerabilities?
   a. Accessibility of the platform
   b. Usability of the platform
   c. Privacy of the data exchange
   d. Quality of information
   e. Veracity of the sources

10) How comfortable are you sharing information about ICS vulnerabilities outside your organization?
   a. 1 – Not comfortable
   b. 2
   c. 3
   d. 4
   e. 5 – Very comfortable

11) What are the parameters you would want to have in an ideal ICS vulnerability repository/database? (Choose all that apply)
   a. Unique identifier (E.G. CVE)
   b. Vendor
   c. Affected products
   d. Affected versions
   e. Common vulnerability scoring system (CVSS)
   f. CVSS vector string
   g. Common weakness enumeration (CWE)
   h. Exploitability
   i. Risk score
   j. Researcher/author
   k. Critical infrastructure/Industry sectors affected
   l. Potential physical impact
   m. Countries/areas product is deployed

n. Vendor country of origin
o. Available patches/updates
p. Alternative mitigations
q. Tools for exploitation
r. References

12) How would you prefer to access information from this ICS vulnerability repository? (Choose up to two answers)
    a. Text reports
    b. Spreadsheets
    c. Newsfeeds or alerts
    d. Application program interface (API)
    e. XL or other markup language
    f. Online dashboard

13) Do you have any additional comments or recommendations?

14) May we contact you in the future to ask for additional insights and share the results from the survey? (If yes, please provide your email)