MIS Quarterly Executive

Volume 24 | Issue 1 Article 4

March 2025

Promoting Cybersecurity Information Sharing Across the Extended Value Chain

Olga Biedova

Lakshmi Goel

Justin Zhang

Steven A. Williamson

Blake Ives

MIS Quarterly Executive

Promoting Cybersecurity Information Sharing Across the Extended Value Chain

As cyberthreats become more targeted and complex, industries that rely on interconnected information and operational technologies (IT/OT) face unique vulnerabilities. Addressing these risks requires innovative approaches to cybersecurity. This article focuses on an alternative information-sharing forum centered on the extended value chain of a single company in the forest and paper products industry. The article explores the forum's design, execution and challenges, and offers recommendations to guide similar company-specific collaborations aimed at enhancing cybersecurity resilience across interconnected value chains.[1,2]

Olga Biedova
College of Charleston (U.S.)

Lakshmi Goel
Al Akhawayn University in Ifrane (Morocco)

Justin Zhang
University of North Florida (U.S.)

Steven A. Williamson
University of North Florida (U.S.)

Blake Ives
College of Charleston (U.S.)

The Need for Cybersecurity Information Sharing

Between 2021 and 2022, the number of data breach victims worldwide surged from an estimated 294 million to 422 million, with 83% of these breaches attributed to external actors. As cyberrisks escalate rapidly, government agencies are increasingly calling for enhanced cybersecurity information sharing, particularly among organizations in essential industries such as banking, water, waste management, food distribution, energy, telecommunications, drug manufacturing and forest products. Despite these calls, interorganizational information sharing remains sporadic.

In the U.S., Europe and beyond, various government initiatives have encouraged voluntary information sharing among companies. For instance, in the E.U., the Network and Information Security Directive (NIS2) aims to improve cybersecurity resilience across member states. At the same time, the General Data Protection Regulation (GDPR) introduces additional obligations

1 Stuart Madnick is the senior accepting editor for this article.
2 The article contributes to the December 2024 Special Issue on "Cybersecurity and Digital Risk."

DOI: 10.17705/2msqe.00109

for companies handling personal data breaches and emphasizes the need for coordinated cybersecurity practices.

Both NIS2 and GDPR underscore the growing importance of cybersecurity information sharing within Europe, complementing efforts like the U.S.'s Cybersecurity Information Sharing Act (CISA).[3] However, because no mandatory regulations require private-sector firms to share cybersecurity information with each other, many organizations still resist sharing cybersecurity information due to concerns over competitiveness, confidentiality and fears of regulatory repercussions. In addition to these concerns, trust remains a significant barrier. Research indicates that organizations often hesitate to disclose sensitive information due to fears about how other entities may use it.[4]

Despite concerted efforts to facilitate information sharing through initiatives like the National Council of Information Sharing and Analysis Centers (ISACs), the benefits of participation in sector-based ISACs can be limited, particularly for specific industries such as forest products.[5]

For organizations that are hesitant to join their sector's ISAC or that seek alternative channels for information sharing, there is the option of organizing a custom-tailored cybersecurity information-sharing forum, such as the forest products forum we describe here. A focused forum can be designed as a single meeting or series of meetings, specifically targeting business partners as participants and with topics deemed relevant by the organizer. This gives an organizing company the power to bring out cybersecurity topics that are especially relevant to their operations, partners and threats. As a participant in a custom-tailored forum noted: "I go to [cybersecurity] forums. I see the same people in the events, but most of these are very broad. This [cybersecurity forum] was very focused."

By inviting only extended value-chain partners, organizations can foster a more trusting and relevant environment for sharing information. Moreover, invitations from a business partner are likely to be accepted, given the desire to maintain good business relationships.[6]

The urgency of cybersecurity information sharing among forest products firms became starkly evident when a company in the industry was hacked and held up for ransom. The organizer described the forum as having been jump-started by that incident and "a rush of [other] material breaches, especially in the North American sector."

Multiple large companies within, or related to, the forest products industry agreed to participate in a meeting where their senior information security leadership could discuss threats and mitigation approaches. The resulting forum generated valuable lessons for both the organizing firm and other attendees. The forum's initial discussions primarily focused on addressing best practices and procedures to enhance overall cybersecurity, rather than targeting specific system vulnerabilities.[7] While the insights are particularly relevant for sensitive industries facing critical risks—such as ports, transportation and energy infrastructure—any organization with valuable assets is a potential target and can benefit from these lessons. As one forum organizer emphasized, "It's not a matter of if a cyber incident will happen, but when."

Based on our research (see Appendix C), we highlight three key considerations for businesses planning cybersecurity collaborations with their extended value chain partners: the perceived value and potential of such initiatives, the inherent challenges and risks involved, and the logistical aspects of organizing effective events. We explore specific issues within these areas, including the types of information exchanged, the roles of the organizing entity and legal counsel, and the potential involvement of government agencies. Our discussion and recommendations are foremost intended for information security leaders, compliance officers and organizational

3 See Appendix A for more details on CISA, NIS2 and other cybersecurity acts from different nations.

4 Goles, T., White, G. B., and Dietrich, G. "Dark Screen: An Exercise in Cyber Security," *MIS Quarterly Executive* (4:2), 2008.

5 A more in-depth examination of the challenges associated with ISAC membership and alternative information-sharing approaches is available in Appendix B.

6 We use the term "extended value chain" to emphasize that the forum included a range of participants that extend beyond the forest products industry—such as distributors, corporate customers and logistics providers.

7 According to CISA, two critical types of cybersecurity information sharing include: (1) cyberthreat indicators, such as incidents, vulnerabilities and threats and (2) defensive measures, encompassing mitigations, situational awareness, best practices and strategic analysis. The forum covered the second type of information sharing.

executives tasked with developing, implementing or maintaining cybersecurity strategies.

Safeguarding Operations Technology in the Forest Products Industry

In March 2020, the forest product industry was recognized by the U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency as "critical infrastructure."[8] The designation highlighted the fact that companies in the industry are an attractive target for cyber gangs, especially those backed by foreign states. Further recognition of that threat comes from a global cybersecurity manager for process industries at engineering firm ABB: "The pulp and paper sector traditionally holds a very low inventory, given there is no value in keeping a year's worth of tissue/boxes. Hacking just one tissue supplier could take out 22 percent of the capacity."[9]

The industry's infrastructure includes a mix of often very old paper-making machines and far more recent computer and communications networks. One forum participant explained: "While the formula for making paper and paper products has largely remained unchanged for centuries, the pace of change within the industry has accelerated, driven by imperatives in digital transformations and global sustainability."

The forest and paper products industry relies heavily on manufacturing and production processes that frequently involve operational technology (OT), or "hardware and software that detects or causes a change, through the direct monitoring and control of industrial equipment, assets, processes, and events."[10] At the same time, information technology (IT) increasingly connects the extended value chain of suppliers, distributors, transportation and logistics suppliers, channel partners and customers. IT also enhances support activities—such as accounting, payroll, and research and development—and is critical to sales and operations-planning systems.

Old OT now plays a pivotal role in this increasingly integrated extended value chain, where the boundaries between OT and IT continue to blur. As one forum participant described it: "The traditional operating technologies—characterized by individual paper-making machines and mills—are now part of an end-to-end extended value chain from fiber to end-product and associated data. Information technology extends the value chain in terms of functionality and channels, such as e-commerce."

The cybersecurity defenses for OT technologies are extremely uneven. While the IT sector benefits from a well-developed marketplace of security tools, forum participants expressed concerns that OT security has fallen significantly behind. As one participant noted:

> *"Cybersecurity management tools often don't do as well in the OT space. The [OT cybersecurity] market has not caught up. We found that we had to partner in development with vendors who play very robustly in the IT space, but don't have the same capabilities in the OT space."*

Another forum participant described with frustration an unsatisfactory OT security heritage: "Historically, we have not considered OT security to be critical. We did not have a single pane of glass for transparency in OT." The forest and paper products industry is, of course, hardly unique in both its increasing reliance on—and challenges with—the integration of legacy OT and IT. Legacy machines and systems were not built for a connected world that is under constant risk of cyberthreats, both unintentional and malicious.

One big challenge is the need to coordinate cybersecurity strategies between IT and OT teams effectively. A recent study found that 76% of manufacturers agree that the boundary between IT and OT presents significant intrinsic risk.[11] For instance, a recent ransomware attack on the state-run Belarusian Railways, established in the

8 *Forest Products Industry Deemed Critical Infrastructure*, Society of American Foresters, March 25, 2020, available at https://www.eforester.org/Main/SAF_News/2020/Forest_Products_Industry_Deemed_Critical_Infrastructure.aspx.

9 Ray, A. *Protecting Pulp and Paper Mills from Ransomware Attacks*, ABB, available at https://new.abb.com/pulp-paper/abb-in-pulp-and-paper/articles/protecting-pulp-and-paper-mills-from-ransomware-attacks.

10 *Risk Management Framework for Information Systems and Organizations*, National Institute of Standards and Technology, available at https://doi.org/10.6028/NIST.SP.800-37r2.

11 *Manufacturers Ramp up Cyber Defenses as Supply-Chain Bottlenecks—and Vulnerabilities—Deepen*, PWC, 2022, available at https://www.pwc.com/us/en/industries/industrial-products/library/cyber-supply-chain.html.

late 1800s, exemplifies the vulnerability of legacy infrastructures in industries such as electric power, communications and transportation that rely on operational technologies built years ago.[12] In another case, in the recent cyberattack on five water utilities in the U.S., the attackers focused on a specific brand of programmable logic controller, one widely used in "energy, food and beverage manufacturing and healthcare."[13]

Creating the 2021 Cybersecurity Forum

Recognizing such risks, Company A partnered with the PAPER Institute, affiliated with the University of North Florida, to facilitate the Forest Products Industry Forum on Cybersecurity.[14] The objective was to engage major forest products companies and their extended value-chain partners in addressing cyberthreats and developing best practices to mitigate those risks.

Structuring the Forum

In 2019, a business partner of Company A suffered a severe ransomware attack, resulting in costly ransom payments, security upgrades and employee cybersecurity training. To strengthen its defenses, the company enlisted the PAPER Institute to assess its cyberresilience and the effectiveness of its training program. As part of this evaluation, the team interviewed three partners, including Company A.

Two years later, Company A, recognizing both its own cybersecurity vulnerabilities and those of its business partners, took action. They asked the PAPER Institute to facilitate a forum for sharing cybersecurity knowledge and experience within its extended value chain. Company A's chief information officer (CIO) described the motivation: "We remember what [the Paper Institute] did in 2019. It was very helpful for us to talk about this and to hear other companies' views. We want to have that same conversation with the companies in our value chain."

In September 2021, Company A's CIO sent out forum invitations to 16 companies, each a large global player comparable in size to the organizing company. The invitation described the objective as: "… for the forest products industry to become stronger regarding cybersecurity threats. We believe by fostering an open dialog and information sharing we can all learn from one another and help protect industry value."[15]

All 16 invitees expressed initial interest, and 11 subsequently participated in at least one session of the forum, as shown in Table 1. Originally planned as a single two-hour session for November 2021, the forum expanded into four online meetings over six weeks, each lasting 90 to 120 minutes. Two of the authors moderated the discussions, with antitrust legal counsel present and an antitrust warning issued at the start of each meeting.

The Participants

Also present at the first meeting were seven representatives from the 11 companies, holding titles ranging from CIO to manager of IT security. The forum invitation included a brief description of the ideal attendee: "The ideal participant for this forum would be the person that informs the security strategy for his/her organization and not the security practitioner."

The organizing company targeted organizations of similar size in its extended value chain and with an international presence. Participants were selected for their direct involvement in cybersecurity and their decision-making authority in security matters. This approach was intended to ensure that the insights gathered would be both practical and strategic, coming from professionals familiar with cybersecurity challenges, and empowered to implement solutions. However, the participants' specific roles varied across companies, reflecting the diverse structures and responsibilities within each organization.

Participating companies connected to the organizing company as suppliers, distributors and/or customers. While most, like Company A, were in the forest products industry—an industry

12 Roth, A. "Cyberpartisans' hack Belarusian railway to disrupt Russian buildup," *The Guardian*, January 25, 2022, available at https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildupsburgh.

13 Bajak, F. and Levy, M. "Breaches by Iran-affiliated hackers spanned multiple U.S. states, federal agencies say," Associated Press, December 2, 2023, available at https://www.wtae.com/article/aliquip-pa-water-authority-hack-us-breach-cisa/46016776.

14 The companies participating in the forum requested anonymity to facilitate open discussions and protect sensitive information. Additionally, anonymization helps mitigate potential reputational risks for both the participating and organizing companies.

15 The full text of the invitation can be found in Appendix C, with identifiable information of Company A retracted.

Table 1: Companies Participating in the Forum

Company	Role	Employees	Relationship to Organizer	Industry
A	Group CIO; CIO North America	10,000-25,000	Organizer	Forest and paper products
B	Sr. Director Corporate IT Shared Services and Security	5,000-10,000	Supplier	Forest and paper products
C	Director – Information Security	10,000-25,000	Supplier	Transportation and logistics
D	Manager – Cybersecurity; VP and Controller	1,000-5,000	Supplier	Pulp producer and solid wood products
E	Director – Global Information Security	10,000-25,000	Customer	Packaging manufacturer
F	VP IT – Information Security; Director IT – Security	10,000-25,000	Supplier	Water and process management
G	Manager – IT Security	5,000-10,000	Supplier	Forest and paper products
H	N.A.	5,000-10,000	Supplier	Producer of industrial minerals
I	N.A.	25,000-50,000	Customer	Materials science and manufacturing company: design and manufacture of labeling and functional materials
J	N.A.	1,000 - 5,000	Supplier	Chemical-materials solutions provider
K	N.A.	1,000 - 5,000	Distributor	Sales, marketing and distribution of pulp, paper, tissue, packaging, wood products and metals

encompassing activities such as the growing, harvesting and processing of wood and fiber, as well as the manufacturing of pulp, paper, and wood products[16]—some represented other key sectors in the broader value chain (e.g., trucking). Given that most participating companies were conglomerates with many subsidiaries, these relationships could be complex; for instance, a company might simultaneously serve as a supplier, customer and, in certain product lines, a competitor.

Discussion Topics

Two PAPER Institute faculty members, all among the authors, collaborated with an executive from Company A to organize and facilitate the forum. Semi-structured questions, based on themes partially derived from a prior project on cybersecurity,[17] guided the list construction. The list had been shared with participants before the first Zoom call. Here are the initial topics (see Appendix D for specific descriptions):

- Technical
- Trends
- Awareness training
- Emergency response/preparedness
- Governance/support
- Value-chain collaborations
- Cyber maturity

In planning for subsequent meetings, topics suggested by participants were:

16 Forest Products, United States Environmental Protection Agency, available at https://archive.epa.gov/sectors/web/html/forest.html.

17 That project involved interviews with top executives from four companies (including Company A) that were implementing security-awareness training programs in their organizations.

- Manufacturing protection/network segmentation
- Incident response process/crisis management
- Cloud security
- Nation-state attacks

Other topics discussed included:

- Segmentation strategy implementation
- Hardening systems access interfaces
- Protecting OT/manufacturing assets
- Self-evaluation of defenses and response capabilities
- Rapid threat identification
- Education and training of stakeholders
- Security-data analytics
- Scorecards (e.g., key performance indicators)
- Importance of visibility/transparency
- Overcoming breach shame/stigma
- Government agency reporting (e.g., SEC)
- Certification vs. testing (red team/blue team)
- Cyber readiness as key supplier evaluation criteria
- IT vs. OT dichotomy
- Remediation (e.g., restoring a supplier after an incident)
- Senior management involvement
    - Fostering a security imperative
    - Culture (e.g., transparency)
- Assessing risk
    - Insurance
    - Blast radius (extent of damage)
    - Corporate security culture
    - Partner trust scores
    - Trust vs. zero trust
    - Real-time assessment

Assessing Forum Value

Each session ended with a questionnaire to gauge the forum's value and participants' willingness to engage in future sessions. Feedback indicated that the sessions were well-received and helped to shape subsequent discussions.

Two years later, we followed up with three participants. We asked about their overall experience, any actions they took as a result of the forum and their willingness to participate again. The representative of the organizing company recalled a key takeaway.

> *"While we had a robust security strategy in place, we saw what others were doing and learned from it. We learned something in every discussion. We learned how others managed third-party level risks. From those observations, we refined our approach. It's hard to get your mind around what you should be doing until you hear what others are doing."*

Other responses included the observation that sharing tended to make everyone more realistic about their own level of preparedness: "If participants had been asked to rate themselves on a security rating of maturity scale of 1 to 5, even a '3' is probably much better than most companies really are, as companies tend to overrate themselves." Because participants included companies in other industries (e.g., trucking), "the forum helped us to understand how the paper industry compared to other industries."

Of particular value was a discussion with a participating company that had endured a ransomware attack. As one participant described, "they [the victimized company] admitted the material breach and were willing to have follow-up conversations about it. It was impactful to hear their story." The forum also fostered cross-company relationships that extended beyond the scheduled sessions and encouraged greater information sharing among participants. As one attendee's offer illustrates: "We have a PowerPoint template we use to report on any breaches we have. We share this with our partners. We are willing to share the presentation with y'all."

Participants also identified specific tools (e.g., for deep-web analysis, recorded future and insights) and shared policies. One such policy is used for managing portable storage devices.

> *"Use, where possible, endpoint controls to prevent sneaker attacks. Use a policy that prevents unidentified storage devices from being mounted on high-priority networks. Require secure remote storage only, limited to certain vendors and even certain serial numbers of devices."*

According to a representative from the organizing company, the forum's greatest achievement was opening up discussions on

topics that many had previously been reluctant to address: "The forum conversations shifted the dynamic to organizations being more open."

For another participant, a key lesson was the impact on their company's senior management.

> *"The consensus from the forum was that tone from the top is key. It is not IT; it is the executive committee. This is not an IT decision. We have now heavily engaged executive leadership support in our cyber initiatives. We have a contracted company that conducts red team/blue team exercises. The results are reported to our senior management. Our CFO was in touch during the whole exercise to get updates."*

Recommendations

Attendees overwhelmingly regarded the forum as a success. Below, we summarize the key recommendations that we believe contributed to that success, divided into two categories: (1) those related to the execution of the forum and (2) key cybersecurity takeaways from the discussions.

Forum Execution

Invite the right people: It is in a company's best interest for all firms in its extended value chain to maintain strong cybersecurity defenses. The organizing company benefits by tailoring the invitation list to its own extended value chain and in seeding the initial discussion topics and questions. By listening carefully to the discussion, the company gains awareness—and, ideally, reassurance—regarding its business partners' cybersecurity defenses.

Before issuing invitations, the organizing company should critically assess its extended value chain. For instance, companies in the forest product industry have complex extended value chains that need careful consideration.[18] To promote balanced participation, invitations could, as in this forum, be limited to partners of similar size. However, controlling who ultimately attends can be challenging, if not impossible. In this case, while all participants shared security responsibilities, their titles and specific duties varied.

A potential concern is that the diverse companies in the industry, each with a unique extended value chain, could result in an individual company's chief cybersecurity officer being faced with the challenge of selecting among numerous potential invitations. What about competitors? In this forum, while the participating companies were primarily suppliers, distributors and customers, some firms did compete in certain markets. This made it necessary to have legal counsel present to ensure antitrust compliance. The attorney was appointed by the organizing company, a decision that all participants agreed upon. External facilitators, meanwhile, can help in structuring the sessions, keeping participants focused and organizing the findings. The lead facilitator described her role: "My job was to lead and continue to prompt the discussion and to make sure that everybody had an opportunity to express their perspective."

Government agencies were not included in this forum. One participant worried that "government agencies [would] add another layer of complexity to the legal approval process." Nevertheless, that same executive recognized the importance of establishing relationships with agencies: "If we are targeted by a nation-state actor, we are not going to have the resources to prevent that attack. But what can we do to mitigate it? Who are our friends? Do we have the right relationships with law enforcement?" An executive from the organizing company felt that if a government agency is invited "the same ground rules must apply to them, with a precondition that they too must bring value and transparency to the other participants."

Select the right format and timeframe: There are benefits to meeting face-to-face, particularly for establishing personal networks. But for this kind of sensitive collaboration, we recommend an online forum. Among the challenges of meeting face-to-face, one attendee described "being spread thin and the ever-present worry of urgent issues suddenly arising."

For the forest products cybersecurity forum, an advantage of hosting the forum remotely was the global distribution of participants' headquarters. But how many meetings should be planned and for how long? One facilitator

18 *Wood Supply Chain Schematic*, Forest Resources Association, November 9, 2021, available at https://forestresources.org/resources/wood-supply-chain-schematic/.

described the challenge: "We planned for one two-hour forum meeting where we went through all of our topics. We touched on maybe 50% of them. We ended up with four sessions."

Establish participation ground rules and foster trust: At the start of each meeting, the organizing company should seek to establish communication norms. "This forum is as useful as participants make it. This is not about just listening. We put forward ground rules up front that encouraged sharing and discouraged passivity." Doing things like emphasizing that participating companies face a common adversary and will be stronger by working together and recognizing that strengthening cybersecurity benefits all extended value-chain partners can foster trust. By addressing vulnerabilities, all participants will emerge more resilient.

If there are competitors in the room, legal counsel oversight can mitigate legal risks. In the forum described, each session started with discussion rules, such as: "Don't say anything that might affect the determination of the price of products in the marketplace." It is also advisable to establish active participation as a ground rule and expectation. Nevertheless, free-riding can become an issue even with agreed-upon ground rules. One participant observed: "While many folks were open and willing to engage in the discussion, others were passive, and not very useful." When sharing is strongly encouraged, those who don't share may be seen as unreliable, lacking in relevant background or, potentially, masking limitations in their organization's security infrastructure or policies.

Participants with similar organizational roles should be invited to minimize free-riding and foster trust. In this forum, differences in participant roles and responsibilities might explain the free-riding that the facilitators and other participants observed. It also makes sense to utilize independent facilitators to reduce the perception of undue influence by the organizing company and to ensure the company is seen as an equal participant alongside the other participants.

The facilitating team should be asked to encourage passive participants to engage more in the discussions. One of the facilitators described her team's role in the forum: "We would call people out if they saw that someone was not talking." Ground rules can also help participants get past the shame they might feel if they have been breached: "Going into the forum, there was a stigma, and no one wanted to acknowledge that they had cyber incidents." In this case, the participant's willingness to describe and answer questions about his company's breach reinforced the expectation of nonjudgmental sharing.

Finally, though logistically challenging, the forum should be spread across multiple meetings to build trust and relationships. As the lead facilitator observed: "With every new forum meeting, people were feeling more comfortable."

Seed initial topics: A predetermined, though adaptable, set of topics and questions can provide helpful initial structure. Topics can be drawn from the experience or interests of the participants or the organizer. The detailed list of cybersecurity topics covered during these meetings, included in Appendix D, can serve as a starting point for drafting the agenda. Many topics are broad and applicable across various industries, while others are more industry-specific (e.g., operational technology).

However, cybersecurity is constantly evolving. Therefore, it's a good idea to seek topics from participants and remain vigilant about new topics that may emerge. Follow-up interviews, conducted two years later, demonstrated how dynamic such a list can be. New potential topics mentioned included: the SEC's tightened rules on cybersecurity disclosures, the perceived heavy-handedness of government oversight, the threat posed by collaborations among cybercriminals, the dual nature of AI as both a threat and an opportunity, the emergence of consolidated data analytics that transcend a single supplier, and the management of cybersecurity culture.

Assess the effectiveness of the forum: Organizing a cybersecurity information-sharing forum is no simple task. The organizing entity can assess the forum's effectiveness and value to determine whether future meetings would be beneficial. As a short-term evaluation, organizers can distribute a follow-up questionnaire to participants, asking about their perceived value from the forum and their interest in attending future sessions and soliciting feedback on the forum's organization. In this case, survey results confirmed participants' willingness to continue

the dialogue, indicating the need for future meetings.

To assess the forum's long-term value, the organizing company could conduct follow-up interviews with participants one or two years later. However, this approach presents challenges, as participants may have transitioned to new roles or moved to different companies.

The two most indicative measures of the forum value for the organizing company are: (1) whether any changes in cybersecurity policies were implemented post-forum as a result of the discussion with participants—during the forum or after (such as changes in the cybersecurity playbook, updated risk metrics and reviewed training materials)—and (2) an improved awareness of the cybersecurity profiles, strengths and weaknesses of the partners across the company's extended value chain.

After the forum, several participating companies, including the organizing company, significantly enhanced their cybersecurity practices. For example, Company A revised its cybersecurity playbook to include new risk metrics discussed during the sessions. Additionally, insights from the forum led to a comprehensive review of training materials, integrating best practices shared by participants. These improvements were driven by collective experiences in managing breaches, identifying vulnerabilities and increasing transparency in third-party risk management.

The forum successfully enhanced the organizing company's understanding of the cybersecurity maturity of its extended value chain partners, too. As highlighted in the follow-up interviews, the discussions helped participants recognize both the strengths and potential gaps in their partners' defenses. For example, Company A gained a better understanding of how its partners handle third-party risk, which influenced its approach to assessing vendor security.

This improved awareness also led to ongoing collaboration between some companies, extending the benefits of the forum beyond the sessions themselves. These post-forum actions demonstrate the tangible impact of the discussions and indicate that the forum was not only valuable for sharing knowledge but also for prompting real-world changes in cybersecurity strategies.

Key Cybersecurity Takeaways from the Forum

Change the value-chain cybersecurity culture: Among the most important takeaways from the forum was the need to build a new attitude of transparency and trust across extended value-chain partners.[19] Before the forum, the prevailing attitude of some participants was distrust, as recalled by a participant from the organizing company: "We had been seeing a high level of sensitivity to providing information to us. The information that we needed to provide valuable insights required a willingness of our partners to provide a lot of information." An executive from Company A described this transformation in attitude and culture:

> *"It was invaluable. We witnessed more willingness to have dialog. To stand together instead of standing on our own. I was very impressed that some members were very open about sharing; it helped us, in some cases, confirm and, in some cases, discover new threats we should be thinking about."*

The forum also provided a window into extended value chain partners' culture, as one participant described: "Do they approach cyberthreats from the risk management perspective? Or do they have a "whack-a-mole" approach? Do they just stop everything and patch whatever vendors and the press are screaming about at the moment?"

Harness the benefits: One significant outcome for the organizing company was gaining valuable insights into the effectiveness of its own security measures. Through the sharing of experiences, new potential risk areas for enhancing security were identified. Participants discussed various policies, tools and threats, some of which the organizing company subsequently adopted or acted upon.

19 Pearlson, K. and Prakash, M. "Cybersecurity Culture Maturity Model," Cybersecurity at MIT Sloan: Interdisciplinary Consortium for Improving Critical Infrastructure, August 17, 2023, available at https://cams.mit.edu/wp-content/uploads/Handout_Cybersecurity-Culture-Maturity-Model_Final_SlideDeck_CultureClub.pdf.

Companies also shared detailed practices, disclosed vendor names, and identified products they had tested and validated. Commitments were made to share information with extended value-chain partners in the future, and policies regarding data breaches were established. For example, the organizing company shared its policy for handling breaches involving partners: "If we have a direct network connection with you, we will cut off the connection until we receive assurance the problem has been resolved."

Build an analytic engine: While data sharing and transparency are essential, so too is the development of an analytic capability to put that data to use. One of the organizers described this opportunity/necessity.

> *"There is no 'ERP' [enterprise resource planning] of cyber. But what is improving is the analytical consolidation. The providers/ solutions are still fragmented, but you can bring together the analytics from all those solutions. AI is definitely a growing factor in this analytics. It helps you to find anomalies, and data that don't match. But AI can also be used against you."*

Anticipate and plan for future forums: Interviews with attendees two years later showed an interest in, and a need for, a follow-up forum. New topics they mentioned—as well as the rapid evolution of tools, policies, regulations, and, most importantly, threats and breaches—suggest that planning for regular follow-ups should be the final topic discussed in each forum.

Given the online format, the time and expense commitments for a follow-up would be modest. However, the impetus for organizing a future forum (and many of the likely benefits from it) would likely be perceived by other participants as coming from the organization that originally arranged the forum around its own extended value chain. That inequity, real or perceived, suggests that the follow-up might best be arranged by the original organizer. Yet that organizer may, as in this case, be reluctant to play the leadership role again.

Concluding Comments

Sharing an organization's or industry's preparedness for and response to cyberthreats can yield significant insights that benefit and safeguard the organization, its extended value-chain network and the entire industry. This collaborative effort enhances an industry's ability to mature and effectively address evolving cyberthreats.

The novel, extended value-chain forum described here exemplifies what can be achieved through strategic communication across a company's business partners. By exchanging information about common threats, mitigation strategies, risk acceptance approaches, and best practices, the entire network is strengthened and important relationships are established.

Appendix A: Global Cybersecurity Sharing Regulations and Facilitating Agencies

Cybersecurity information-sharing regulations differ significantly across regions, with varying degrees of government involvement and obligations for private-sector firms. Below, we summarize key frameworks from different countries and regions, highlighting their approaches to firm-to-firm information sharing, mandatory reporting and cross-border considerations.

United States: Cybersecurity Information Sharing Act

The Cybersecurity Information Sharing Act (CISA) of 2015 encourages the voluntary sharing of cybersecurity threat information between private companies and the federal government. CISA offers liability protections to incentivize participation, but there are no penalties for not engaging in information sharing.

European Union: NIS2 and GDPR

The NIS2 Directive from 2023 (with the enforcement date of Oct 17, 2024) mandates information sharing in critical sectors, including energy and healthcare, with penalties for noncompliance. The directive encourages collaboration across sectors and borders, with strict requirements under the General Data Protection Regulation (GDPR) to protect personal data during such exchanges.

Regulation	Country/ Region	Firm-to-Firm Information Sharing	Mandatory Reporting	Government Involvement	Cross-Border Considerations
CISA	U.S.	Voluntary	No	High (DHS, CISA)	Limited restrictions
NIS2	E.U.	Mandatory in critical sectors	Yes (for critical sectors)	High (E.U., CSIRTs)	Strict (GDPR compliance needed)
SOCI Act	Australia	Encouraged for critical sectors	Yes	High (CISC)	Less restrictive than GDPR
Cybersecurity Act	Singapore	Encouraged, but no direct mandate	Yes	High (CSA)	Controlled by national law
Basic Act on Cybersecurity	Japan	Voluntary (encouraged in critical sectors)	No	High (NISC)	Less restrictive than GDPR
CCCS/CTX	Canada	Voluntary, public-private partnerships	No	High (CCCS)	Follows local regulations
China's Cybersecurity Law	China	Limited (focus on government sharing)	Yes	Extremely high (state control)	Very strict (data localization)

Canada: Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security (CCCS), established in 2018, promotes voluntary information sharing through public-private partnerships. While CCCS provides a framework for incident response and collaboration, there are no mandatory reporting requirements for firms.

Other Regions

Countries like Australia, Singapore and Japan have implemented varying degrees of encouragement for cybersecurity information sharing, but with different levels of government involvement and cross-border considerations, as shown in the table above.

Appendix B: Challenges of ISAC Membership and Alternative Information-Sharing Approaches

Despite the potential benefits of sector-based information sharing and analysis centers (ISACs), several challenges may limit their effectiveness, particularly for industries like forest products. One significant limitation is the sector-based model itself. For example, the MFG-ISAC primarily connects companies involved in manufacturing. While this focus allows for the sharing of similar threats within the sector, it does not facilitate information exchange across the entire extended value chain.

This matters because companies operating in different industries often face unique cybersecurity challenges that may require either a broader or more focused perspective. In this forum, for instance, logistics providers were included (broader), while the forum also focused on elements of the OT/IT interface that are somewhat unique to forest products (narrower).

Another concern raised by participants in our interviews is the involvement of government representatives in ISACs. Many expressed reluctance about engaging in information sharing when government officials are present, fearing that discussions may become asymmetrical. In such settings, it was noted that government representatives often play a more passive role, primarily listening rather than contributing, which can hinder open dialogue among private-sector participants.

Additionally, member companies in ISACs have no voting or veto power regarding the admission of new members. This lack of control can

Exhibit A.1: Invitation Letter to Participate in the Forum Sent by the Organizing Company A

Forest Products Industry Forum on Cyber Security

You are invited to participate in a virtual cyber security forum jointly hosted by [redacted] and the University of North Florida, Coggin School of Business. The forum objective is for the [redacted] forest products industry to become stronger regarding cyber security threats. We believe by fostering an open dialog and information sharing we can all learn from one another and help protect industry value.

Forum sponsors:

[redacted]

The ideal participant for this forum would be the person that informs the security strategy for his/her organization and not the security practitioner. This does not need to be the CIO. If you have received this invitation but believe another person from your organization is a better fit, you are welcome to substitute. The forum will work best if we have the right representative from each organization.

We anticipate the forum size to be approximately 10-15 companies spanning across the diverse forest products industry. The forum would take place in the last calendar quarter of 2021, prior to Thanksgiving, with the date(s) to be finalized following the confirmation from the participants.

It is intended that the outcomes from the forum discussion will be published in an industry research paper/article by the University of North Florida, and that future forum meetings could be scheduled if the initial meeting proves beneficial.

The planned forum agenda:

1. Welcome
2. Antitrust statement and expectations
3. Introductions
4. Forum discussion
   - Technical
   - Trends
   - Emergency Response / Preparedness
   - Awareness / Training
   - Governance / Support
   - Value Chain Collaboration
   - Cyber Maturity
5. Closing / next steps

Anti-trust counsel will be present. Small breakout groups may be used to facilitate robust discussion.
Please RSVP via email to [redacted] with your acceptance or declination by <DATE>. We do hope you will choose to participate in this forum and help our industry become stronger in the face of ever-increasing cyber threats.

undermine trust among existing members and create reluctance to share sensitive cybersecurity information—companies may worry about the types of organizations that join the ISAC and the potential risks to their data and strategies.

Appendix C: Research Methodology

In the first stage of this retrospective research, we had access to extensive meeting notes, the facilitator's observations and participant feedback. As a result, we could draw useful lessons based on the discussion of cybersecurity challenges faced and best practices deployed.

Participants' immediate feedback was assessed using the results of the questionnaires sent to the participants shortly after each meeting. It included the following statements and potential responses (strongly disagree, somewhat disagree, neither agree nor disagree somewhat agree strongly agree):

- The forum met my expectations
- The forum's depth was appropriate
- The forum provided practical information
- The pacing was appropriate
- I would recommend this forum to a colleague

Since the forum—initially planned as one meeting—ultimately turned into four meetings, several questionnaires included a question asking participants to select topic(s) "for a deeper dive in the next forum." The participants also had an opportunity to share additional comments in an open-ended format.

We also had access to the forum invitation sent to all prospective participants. It allowed us to supplement our analysis of the forum's expectations and organizational efforts on the part of the organizing company. We share the invitation screenshot, with identifying information retracted, in above Exhibit A.1.

The two co-authors who served as forum facilitators also summarized the interaction patterns between forum participants, including the level of openness, willingness to share information and any hesitations observed.[20]

In the second stage, we conducted follow-up, semi-structured interviews with three participants two years after the first meeting. The interviewees were asked to assess the forum's long-term effectiveness and to share their thoughts on the potential value of similar future forums. The conversations were either recorded and transcribed or carefully documented by the co-authors. The list of starting questions included:

- After each cybersecurity forum meeting, you were asked to rate the usefulness of the session. Now, two years later, how would you assess it?
- What value do you see in holding cybersecurity talks with companies in the same industry?
- Would you recommend to a CIO in a company in a different industry to participate in/organize a within-industry cross-organizational cybersecurity meeting similar to the Forest Products Industry Forum on Cybersecurity?
- Have you made any cybersecurity-related changes in your organization as an outcome of the forum?
- Have you attended other interorganization cybersecurity information-sharing events since the Forest Products Industry Forum on Cybersecurity? If so, what were they? What value was derived?
- In the 2021 forum, some of the major discussion topics included transparency and trust among partners, identifying breaches and threats, incident preparedness and response, operation technology vulnerabilities, and governance and support from outside and from the senior management. If you participated in a similar cybersecurity forum again, are there new issues that you would want to address or old ones that you would like to revisit?
- Would you participate in a similar cybersecurity information sharing forum again?

20 The authors acknowledge that the research was driven not by pre-implementation design, but by the availability, post-forum, of a considerable body of notes, as well as the observations of the forum facilitators and that of three participants. A more structured approach, such as the "action principles" proposed by Lacity, Wilcocks and Gozman, might be considered for those studying a similar forum. See Lacity, M., Wilcocks, L., and Gozman, D. "Influencing Information Systems Practice: The Action Principles Approach Applied to Robotic Process and Cognitive Automation," *Journal of Information Technology* (36:3), 2021, pp. 216-240.

Appendix D: List of Forum Discussion Topics

Discussion Topics	Discussion Items
Technical	a) Which IT roles are typically in-house vs. outsourced, including the role of network security? b) What are the best methods to evaluate the linkages between systems and risks? c) How do we evaluate our ability to detect intrusion (also from inside) and protect against it? d) Have we evaluated the best methods of containment to identify and protect against a dormant hacker that could be lurking inside our systems undetected? e) How is security for process-control and manufacturing-automation systems handled—is this the responsibility of the IT organization or another (manufacturing, engineering, etc.) organization? What methods are used to keep up to date on threats in this space? Do we evaluate our technology footprint for cyber risks associated with obsolete hardware/software? f) What certifications do you require of those working in the security area of IT?
Trends	a) Have you seen attack vectors changing? Can you discuss examples? b) How do you learn about new vulnerabilities to watch out for? What are good sources of general information (such as www.cisa.gov and www.mitre.org)? What about industry-specific sources? c) How is the forest products industry uniquely vulnerable? d) What have the trends been regarding industry players being hacked (public examples)? e) Does senior leadership of the company take cybersecurity seriously? f) Are the increased threats related to social engineering recognized?
Emergency Response/ Preparedness	a) How will/did you handle a crisis if it occurs? What preventative measures have you put into place? Have you conducted your own spearfishing and security operations? b) How will/has the incursion or threat of a cyberattack affected your organizational culture, your employees and organizational leaders? c) What is the level of preparedness to react in the event of a cyberattack among various groups? i. IT team ii. Executive leadership team iii. Employees d) Are business-continuity steps in the event of a cyber event known (and tested) at all the right levels (senior leadership, operational, etc.)? e) Is a detailed cyber response plan (“script”) documented? Is the plan kept updated and/or enhanced from time to time? If so, how often? Is the plan known to all key stakeholders? Is the plan informed by regulatory or other requirements? Is the plan detailed enough to be able to be useful for a variety of different cyber events (at different times, different attack areas, etc.)? Is the plan available in other than electronic form (in the event it is not accessible)? Are key outside partners included in the plan?
Awareness/ Training	a) How much of your effort has been centered on system protection? How much has centered on personnel training and or human systems development (i.e., rules, procedures, etc.)? b) Are you able to risk profile your users based on actual security behavior? Are additional steps taken for those with a higher-risk profile? Do you conduct targeted training to increase the cyber defense IQ of your employees? c) How much effort is spent on training for senior leadership (awareness/tabletop exercises, etc.)? Does this include all stakeholders that may be needed in a cyber event (including outside the company)?

Discussion Topics	Discussion Items
Governance/ Support	a) What external sources do you use to inform your IT security policies (in-house/ outsourced)? b) What are the top three categories of costs of cybersecurity defense and mitigation (legal/ technical/insurance/training/others)? c) How much of emergency response is supported through an insurance framework (incident response support, planning support, etc.)?
Value-Chain Collaboration	a) How much IT infrastructure and security information do you share with your business partners? i. What is the level of maturity of our industry with respect to transparency in the cybersecurity area? Expectation of transparency in the marketplace on cyber matters? ii. Do you find your supply-chain stakeholders openly share security incident information (during or after)? b) What type of security-posture information is required of key partners (suppliers, customers, service providers, etc.)? c) Is there an expected third-party security framework and risk assessment performed? d) What is the expectation of notification of partners in the event of a breach (especially for linked systems)?
Cyber Maturity	a) What is the priority for security in the IT organization? Do you utilize the standard three-phase crisis management plan/risk-mitigation plan before the crisis? Do you respond during the crisis? And do you engage in proactive recovery and communications strategy following the crisis? b) How do you evaluate the state of the company's current security technology (level of comfort and assessment metrics) and formal certification, such as ISO? c) "Tone from the top": How is cybersecurity preparedness embedded in your organization beyond IT? d) Is cyber insurance a part of the risk-management process? If so, how can it be used proactively for the most value even before an attack? e) Consideration of periodic third-party audits (reputable firms with references)? Does audit scope evolve as threats evolve? Do audits simulate the new avenues of threats?
Manufacturing Protection/ Network Segmentation	a) What are the best methods of segmenting the Operational Technology (OT) assets (servers, endpoints, networks, appliances, etc.) from the IT assets and from the outside world? b) How do you manage instances where there is a legitimate need for OT connections to IT or the outside world? c) How are portable storage devices (e.g., USB sticks) managed in the OT environment? d) Is virus protection for OT assets part of the security posture? What challenges are encountered for older assets? Is this managed in-house or by hardware providers? e) What are the best methods to allow and manage access by third parties (such as hardware vendors) who legitimately need to monitor or manage OT equipment? f) Is there alignment between IT and OT in the need to secure the OT assets? g) Is OT leadership included in the cyber-response plan? h) What is the best method to assess the current state of OT security in a manufacturing location?

Discussion Topics	Discussion Items
Incident Response Process/Crisis Management	a) Is there a clear expectation of reporting for potential security events that is understood and followed by the user and IT community? b) Does IT have a method of prioritizing the evaluation of all reported security events—and the means to determine if an actual security incident has occurred? c) What are the most important steps in accurately identifying a security incident? Are there expectations for team availability to support this process 24/7? Are there expectations for length of time for the identification step? d) What is the philosophy with regard to disabling outside connections? Do you wait for the completion of the identification step? Do you lock down first and then only re-enable if proven safe to do so? e) Is there a backup/recovery strategy in place to support recovery in the event of a cyber event? What steps can be taken to reduce risks of backups becoming compromised in the event of a cyber event? What should be rehearsed regularly to ensure readiness for an incident? f) Do you test/simulate the cyber event reporting and evaluation process regularly? And only with IT or also including executives and others?
Cloud Security	a) What role does cybersecurity play in your company's strategy for applications—on-premises vs. cloud? b) What are the main cyber considerations/concerns when considering a cloud solution? i. Data encryption ii. Geolocation of data iii. Cloud provider's security framework/disaster-recovery plan iv. Data protection, including for PII c) What is the best way to evaluate the cybersecurity posture of a potential cloud provider? d) What are the main considerations in service agreements with cloud vendors?
Nation-State Attacks	a) How does the rise of sophisticated attacks, some of which are potentially from nation-state actors, change a company's cybersecurity strategy? b) Are there governmental resources that should be brought to bear to understand and assist with such an attack or to assist with prevention? c) For multinational companies, what governmental/political considerations, if any, are considered during infrastructure planning?

About the Authors

Olga Biedova

Olga Biedova is an Assistant Professor of Business Analytics at the department of Supply Chain and Information Management at the College of Charleston. Her research interests are spread across several areas: cybersecurity, emerging information management trends and tools, applied data analytics, and artificial intelligence in business. At the College of Charleston, she teaches core business courses (business statistics and management information systems) and business electives (computer-based decision modeling, business analytics, and artificial intelligence in business).

Lakshmi Goel

Lakshmi Goel is a Professor of Information Systems and Dean of the School of Business Administration at Al Akhawayn University. She was previously a Professor of Information Systems at the Coggin College of Business at University of North Florida where she held the Coggin Strategic Endowed Chair. Her research has been published in top-tier journals such as the *MIS Quarterly*, *Journal of the Association of Information Systems*, *Information Systems Journal*, *Information & Management*, *Information and*

Organization, and *Computers in Human Behavior*. Her area of expertise is learning and knowledge management supported by technologies such as blogs, wikis, and virtual worlds.

Justin Zhang

Justin Zhang is an Associate Professor of Management Information Systems and Business Analytics in the Department of Management at University of North Florida (UNF). He is also the Program Director of the Master of Science in Business Analytics (MSBA) program at UNF. He received his Ph.D. in Business Administration with a concentration on Management Science and Information Systems from Pennsylvania State University, University Park. His research interests include Information and Knowledge Management, Decision Making, Sustainable Development, and Supply Chain Management. He is the editor-in-chief of the *Journal of Global Information Management*, an ABET commissioner, and an IEEE senior member.

Steven Williamson

Steven Williamson is a Professor Emeritus of Management at the Coggin College of Business at the University of North Florida. Before retiring, he was a Professor of Strategic Management at Coggin College and Director of its Endowed Paper Institute for over twenty years. He received a Doctorate in Business Administration with a Management major and a Marketing minor from the University of Memphis. He has won numerous grants and contracts during his tenure as Professor of Strategic Management. As Director of the Paper Institute, he has directed many consulting projects and published numerous articles.

Blake Ives

Blake Ives is a s Distinguished Scholar in Residence at the College of Charleston, and Professor and C.T. Bauer Chair in Business Leadership (Emeritus) in the C.T. Bauer School of Business at the University of Houston.