Enhancing Collaboration to Improve Cybersecurity Practices

The cyberthreat landscape is continually expanding as more enterprises and critical infrastructures increase their attack surfaces owing to their connectivity to the Internet. These attack surfaces can be exploited through a variety of methods with different goals, including distributed denial of service (DDoS) attacks, espionage, data destruction, sabotage and financial theft. Cyberattacks involving ransomware have financial motives and have cost many industries millions of dollars and days or even weeks of downtime.[1] Other cyberattacks have more malicious goals.

A growing number of attacks directly and negatively impact the well-being of civilians, such as attacks on hospitals, water treatment plants, power companies and the airline industry. This has generated a need for immediate international collaboration and agreement among nation-states to eliminate these attacks or, more realistically, be better prepared and more efficient in identifying and responding to these attacks.

Many nations rely on the Group of Government Experts (GGE) and Open-Ended Working Group (OEWG) rules for responsible state behavior in cyberspace, which were established by the United Nations (UN) to maintain peace and security. However, long-standing disagreements about the need for a global, interoperable and open Internet resulted in a consensus report that largely failed to deliver on the OEWG's key objectives, including addressing the root causes of global instability in cyberspace.[2]

YASMIN NAKHLEH JUBRAN

Is a graduate student pursuing a Master of Science degree in marketing at Johns Hopkins Carey Business School (Baltimore, Maryland, USA). She has worked as a scholar research assistant on research funded by the Commonwealth Cyber Initiative, conducted research on marketing sustainability through mobile gaming, and is a former student participant in the Experiential Learning Program at George Mason University's School of Business (Fairfax County, Virginia, USA).

PARSA SADEGHI

Is pursuing a career in data analytics and is interested in cybersecurity. He is a former student participant in the Experiential Learning Program at George Mason University's School of Business (Fairfax County, Virginia, USA).

KEVIN MELECIO

Has contributed to cybersecurity research with the Commonwealth Cyber Initiative, collaborated on a communication plan for the US Cyber Command and is pursuing a software engineering internship with CRCC Asia in Seoul, South Korea. He is a former student participant in the Experiential Learning Program at George Mason University's School of Business (Fairfax County, Virginia, USA).

FELIPE CASABIANCA

Is a director for a cybersecurity enterprise. He is a former student participant in the Experiential Learning Program at George Mason University's School of Business (Fairfax County, Virginia, USA).

BRIAN K. NGAC | CISA, CISM, CRISC, CGEIT, C|CISO, CCSP, CISSP-ISSAP, CSSLP, ISSEP, ISSMP, PMP

Is an instructional faculty member and Dean's Teaching Fellow at George Mason University's School of Business (Fairfax County, Virginia, USA). He developed the Experiential Learning Program where undergraduate students focused on the management of information systems, business analytics and operations management work with real industry participants on real projects. Ngac also works closely with Parsons Corporation and the Information Systems Security Association. If your organization is interested in participating as a client in the Experiential Learning Program, please contact bngac@gmu.edu.

One of the key points of contention is the concept of information sovereignty, which suggests that each state has the right to regulate information communications technology (ICT) within its own territory as it deems necessary. This concept contrasts with the 2018 US-led resolution for the GGE, which stressed the need for an "open, interoperable, reliable and secure information communications technology environment," a core principle of the United States and its allies. In contrast, other nation-states are primarily concerned that this openness could be used to interfere in their internal matters.[3]

Unfortunately, the use of outdated sharing portals can negatively affect both enterprises and government organizations because they tend to be challenging to use and expensive to maintain.

In times of war, governments may explore new options for cyberattacks including DDoS attacks, the deployment of destructive malware and retaliation against other nation-states. For example, the cyberthreat posed by Russia increased after its invasion of Ukraine, leading Australia, Canada, New Zealand, the United Kingdom and the United States to release a joint cybersecurity advisory, warning that enterprises inside and outside the region could be exposed to greater malicious cyberactivity.[4]

The UN's attempt to create an international framework is not progressing fast enough to keep up with international cyberthreats. Therefore, nation-state governments and other key entities must collaborate and use one another's resources to improve threat prevention, recognition and response.

The Sharing of Cyberinformation

Governments frequently use both official and informal procedures to facilitate the exchange of sensitive information, such as issuing memoranda of understanding, adopting laws or creating unique and restricted agreements. Other than exchanging information in person, the most secure way to deliver files is to encrypt them, share the encrypted version and let the receiver decode the contents.[5]

Unfortunately, the use of outdated sharing portals can negatively affect both enterprises and government organizations because they tend to be challenging to use and expensive to maintain. Thus, these enterprises and government organizations frequently revert to email, which can be an unsafe method of sharing files, does not encourage productive teamwork and can result in larger issues, such as the leakage of information through phishing. To reduce the occurrence of cybersecurity risk, collaborative workspace tools such as Confluence and SharePoint, which usually are implemented in a more controlled space, should be used to provide a private and secure method for professionals from multiple countries to collaborate and share information.[6]

Process of Information Transfer Framework

The process of information transfer (PIT) framework was developed by students from George Mason University's School of Business (Fairfax County, Virginia, USA) from a project with the US Cyber Command (USCYBERCOM). The student team was tasked to address USCYBERCOM's challenges of information sharing and communication with allies and partners regarding cybersecurity threats that occur. The student team created the PIT framework with the US government in mind, so it may not be applicable to other countries if they do not have the same governmental structure. However, the overall framework is applicable to any nation-state.

The goal of the PIT framework is to efficiently inform enterprises of cyberthreats and breaches through the sharing of information with others in the network. PIT addresses the communication challenges faced in cyberattacks. The PIT framework provides a continuous and secure intelligence-sharing process for all entities involved, giving each entity the most accurate and up-to-date knowledge about any potential or realized threat. With this shared pool of cyberresources, entities are better able to prevent attacks, detect breaches when they occur and respond to such incidents more efficiently. **Figure 1** summarizes the PIT framework, showing the entities involved in the threat characterization process. **Figure 2** is a bottom-up chart that outlines the steps to take once a threat has been identified.

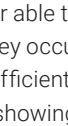
It should be noted that PIT was created and theoretically applied to an attack that had already occurred (SolarWinds); PIT has not been tested in a laboratory setting.

Once a threat has been identified, the next step of the framework is categorizing the threat type by priority—whether it is a top priority or a low priority—and by maturity stage—whether it is a realized threat or a potential threat. After the threat has been categorized, the next step involves comprehensive communication among the board of representatives, which includes four entities:

1. **US government**—This entity represents the federal government and various entities within it, such as US Cyber Command, the National Security Agency (NSA), the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA).
2. **US foreign allies and partners**—This entity represents the different countries that are US allies. Each country has its own representative.
3. **NGOs**—This entity represents the different NGOs that are important in cyberspace.
4. **Corporate allies**—This entity represents the corporate allies of the US government, especially those that conduct business with or within the United States.

Once all the entities are aware of the threat, the next step is to assess the damage. This entails determining which entities have been compromised and how much damage has been caused. By understanding the overall damage, both breached entities and safe entities can share their resources to help eliminate the breach and mitigate the cost. Subsequently, it is vital to create a report that analyzes the costs incurred, the damage caused, why the breach happened and areas of vulnerability.

Finally, all entities should meet to discuss and write a report on preventive measures, containing



LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 1

PIT Framework Summary

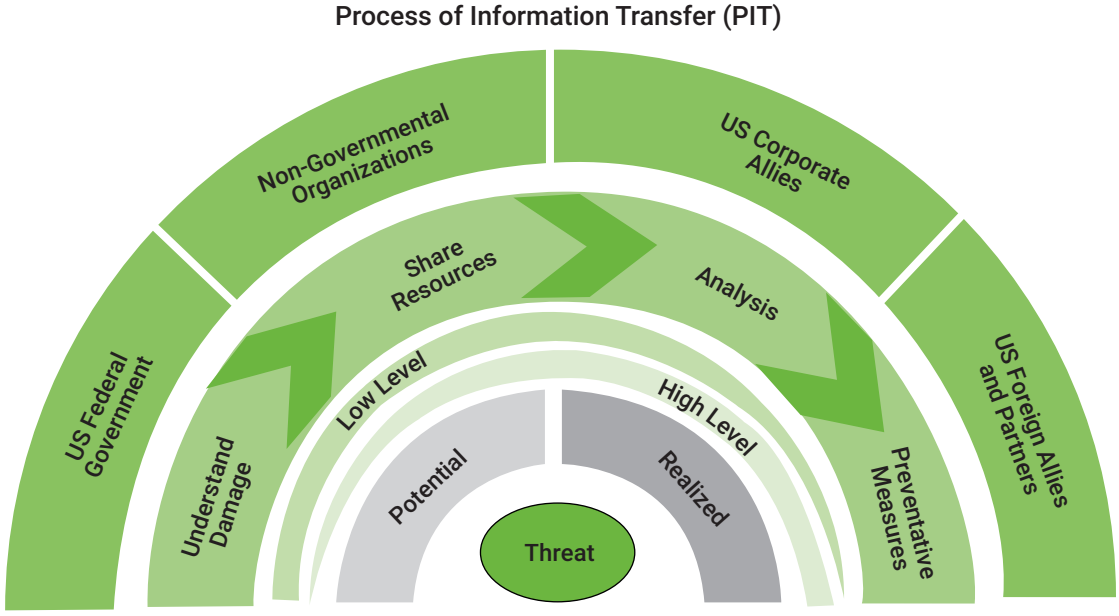
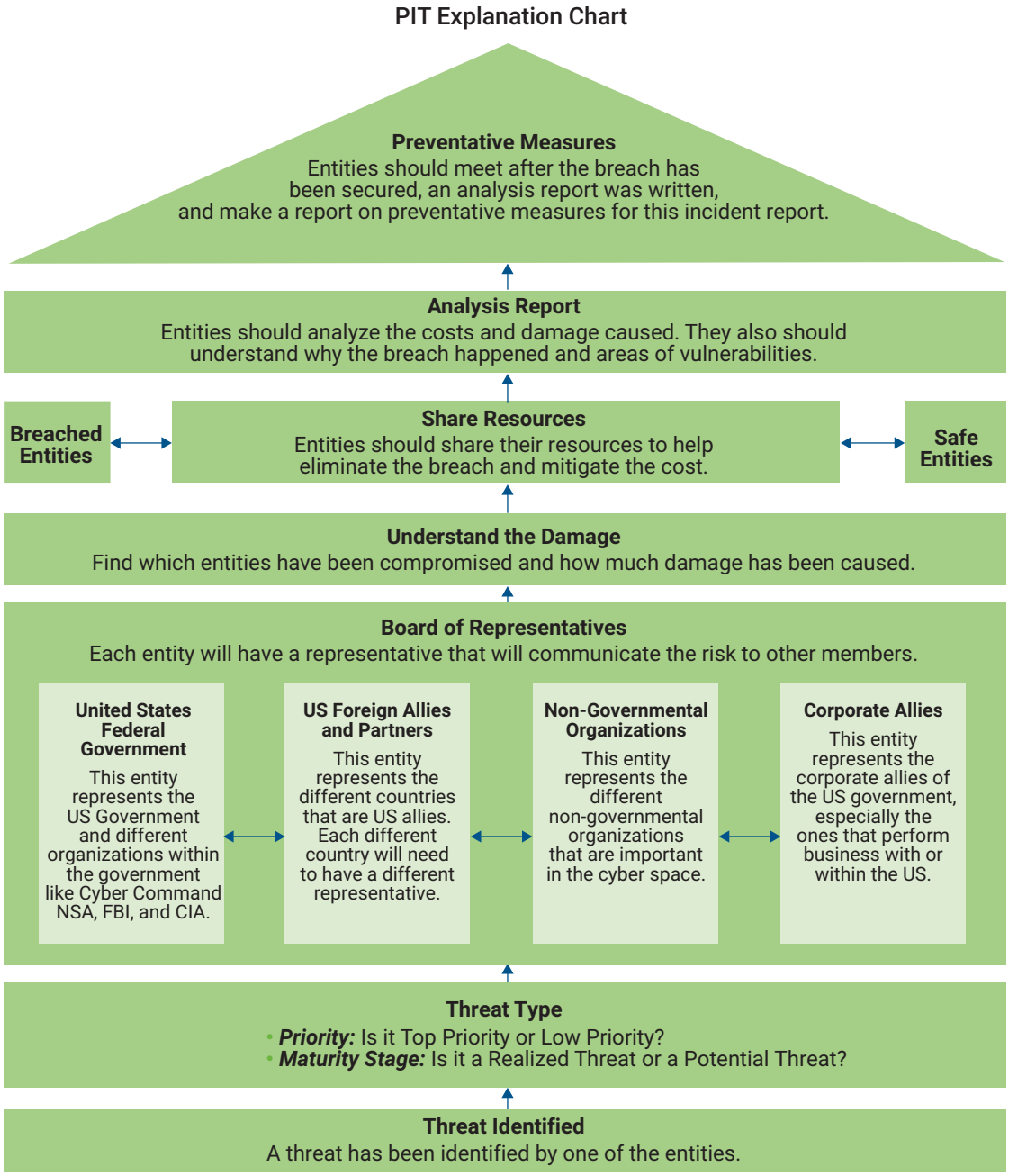


FIGURE 2

PIT Framework Steps



all the information relevant to the specific incident. The board of representatives can use this report to improve their responses to similar threats in the future.

Case Study: Applying PIT to the SolarWinds Attacks

It took 14 months to detect the SolarWinds cyberbreach.[7] SolarWinds had about 33,000 customers, which meant that the cyber compromise was far reaching and affected various entities, including the US National Nuclear Security Administration, the US Treasury, the US Department of Homeland Security, the US Department of Energy, portions of the US Pentagon, the US state of California Department of State Hospitals, Kent State University (Kent, Ohio, USA), Microsoft, Cisco, Intel and Deloitte. It was not until FireEye announced its data breach that other enterprises realized they

too had been breached through their SolarWinds products. Consider how PIT could have been implemented in the SolarWinds attack.

Step 1: Identify the Threat

With the SolarWinds attack, the first step was FireEye's detection of the threat. On the plus side, the entities reacted quickly once the threat was identified and communicated with one another about the attack. This was especially evident in the private sector, where FireEye and Microsoft worked together, and both reported the threat to federal agencies.[8] However, it took US Homeland Security a month to respond to the incident. In addition, not all entities were made aware of the attack, so their resources were not utilized. The use of the PIT framework could have mitigated these shortcomings by ensuring that all members of the board of representatives were aware of the attack so that all their resources could be used effectively, leading to a quicker response time. In the case of the SolarWinds attack, most of the communication took place between US public entities and some private-sector enterprises.

Step 2: Categorize the Threat

The SolarWinds attack would be categorized as a high priority and realized threat because critical systems were breached, vital operations were halted, sensitive data was lost or stolen and critical infrastructure lost function (**figure 3**).

It is essential that all entities are contacted as quickly and efficiently as possible in an effort to reduce the damage. However, threat categorization can affect the flow of communication, specifically with which entities are contacted immediately and made aware of the threat.

Step 3: Alert the Board of Representatives

It is important to note that in the case of the SolarWinds attack, the private and public sectors communicated the breach quickly and efficiently. However, one shortcoming was that, for the most part, the United States communicated with and took actions to mitigate this breach for only US entities and agencies. Because the SolarWinds attack was a high priority and realized threat, representatives needed to work fast, and the slow response was noted in a US Government Accountability Office report: "We continue to emphasize that the federal government needs to move with greater urgency to improve the nation's cybersecurity."[9] In this situation, once the corporate allies recognized the threat, the other representatives should have been alerted in the following order: US government, US foreign allies, US partners and NGOs. All entities should be made aware of the threat to ensure that they are not compromised so that they can assist in mitigating the threat.

FIGURE 3
Threat Categories Matrix

	Realized	Potential
High Priority	• Critical systems were breached. • Vital operations were halted. • Sensitive data were lost or stolen. • A critical infrastructure has lost function. ***The SolarWinds attack falls in this categorization.***	Sharing intelligence of a new APT group attacking critical infrastructure by exploiting a specific vulnerability or an attack vector can be helpful.
Low Priority	An event was realized; however, no key systems or operations were disrupted, and no sensitive data were lost or stolen.	These threats can normally be mitigated through regular system patching, proper training and utilizing industry best practices.

When communicating the details of an attack, the entities should create a checklist to follow based on a consensus of their individual observations about the characteristics of the attack. For example, in the case of SolarWinds, the checklist could have included:

1. Check any systems or information related to Orion—the platform that was compromised.
2. Check whether any entity installed a recent Orion update that might have compromised code.
3. Check for possible backdoors in any systems and platforms. SolarWinds hackers used a backdoor that gave them access to areas they should not have had access to.
4. Check for phishing attacks or tactics. The initial malware code was injected into the SolarWinds system through phishing.

In this part of the framework, sharing intelligence is important. It tells the entities what they are being attacked with and how many entities have been attacked. Sharing this information in real time is critical so that the entities can implement the necessary controls to defend themselves.

Step 4: Assess the Damage

The damage in the SolarWinds attack was extensive. Many entities were breached because of an update that SolarWinds shared with everyone, ruining the security and integrity of all the programs and interfaces that interacted with that update and platform.

To mitigate a threat as quickly as possible, entities should implement a process used by the US military to respond quickly in critical situations called the observe, orient, decide, act (OODA) loop.[10] After observing the criteria and finding the threats in the entities' systems, the next step is to orient, which in this case means sharing the extent of the damage and the costs of the cyberattack among all entities. Based on the damage, they then decide how to react and act.

Step 5: Share Resources

Microsoft and FireEye worked together to recognize the severity of the SolarWinds issue and which parts of their organizations were compromised. The two enterprises shared information to mitigate the damage. This collaboration prevented the attack from spreading to other parts of their organizations. However, collaboration was not limited to these enterprises; US agencies such as the FBI, Office of the Director of National Intelligence (ODNI) and Cybersecurity and Infrastructure Security Agency (CISA) also worked together to handle the incident.

This step is linked to the decide part of the OODA loop, where resource sharing is imperative and timing is key. Enterprises focus on their competitive advantage, which means that they focus on the capabilities they excel in and outsource other activities. This concept can also be applied to cybersecurity practices and information systems. When the United States and its allies share their best resources and capabilities, they excel at mitigating threats.

Step 6: Compile an Analysis Report

Microsoft and FireEye quantified the specific assets that were compromised by the SolarWinds attack and communicated with their customers and partners. In particular, many of FireEye's security tools were stolen and were being used in other countries. It is imperative for enterprises to analyze the incident and report the effects to the necessary parties.

Step 7: Implement Preventive Measures

Preventive measures should be created and shared with all members of the board of representatives. Once these measures are put in place, new monitoring methods should be implemented. This step uses the act element of the OODA loop. After Microsoft and FireEye released the information and notified the relevant government agencies, the affected parties and government agencies instituted new policies to avoid similar situations and created guidelines for how agencies should address such issues in the future. It is also important to note that a crisis response team is a critical factor in addressing and responding to incidents.

Conclusion

Cyberattacks are growing in number and complexity, and they are targeting critical infrastructure. The fight against cyberattacks requires collaboration and pooling of resources, coupled with a fast response. The proposed PIT framework facilitates an easy-to-understand and logical communication structure between the private and public sectors as well as between the United States and its allies. Through the PIT framework, the involved entities participate in a continuous and secure intelligence-sharing process that arms them with the knowledge they need to address both realized and potential threats. Having access to a shared pool of cyber intelligence allows for better prevention, detection and response.

Endnotes

1 Vijayan, J.; "Five Reasons Why the Cost of Ransomware Attacks Is Rising," CSO Online, 10 March 2021, *https://www.csoonline.com/article/565518/what-does-a-ransomware-attack-cost-beware-the-hidden-expenses.html*

2 Tolppa, M.; "First UN OEWG Concludes With a Consensus Report—What Does it Mean for Future Cybersecurity Discussions Under the Auspices of the First Committee?" The NATO Cooperative Cyber Defence Centre of Excellence, *https://ccdcoe.org/library/publications/first-un-oewg-concludes-with-a-consensus-report-what-does-it-mean-for-future-cybersecurity-discussions-under-the-auspices-of-the-first-committee/*

3 Basu, A.; I. Poetranto; J. Lau; "The UN Struggles to Make Progress on Securing Cyberspace," Carnegie Endowment for International Peace,

19 May 2021, *https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491*

4 US Cybersecurity and Infrastructure Security Agency (CISA), "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," 9 May 2022, *https://www.cisa.gov/uscert/ncas/alerts/aa22-110a*

5 UK Department of Education, "Information Sharing—How to Share Information Securely," January 2011, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/417700/Archived-information_sharing_how_to_share_information_securely.pdf*

6 Donovan, S.; "Management and Oversight of Federal Information Technology," US Executive Office of the President Office of Management and Budget, 10 June 2015, *https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf*

7 Jibilian, I.; K. Canales; "The US Is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal," Business Insider, 15 April 2021, *https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12*; Miller, C.; "Throwback Attack: FireEye, the Cyberattack That Started SolarWinds," Industrial Cybersecurity Pulse, 13 January 2022, *https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-fireeye-the-cyberattack-that-started-solarwinds/*

8 *Ibid*.

9 US Government Accountability Office, "Solarwinds Cyberattack Demands Significant Federal and Private-Sector Response (Infographic)," 22 April 2021, *https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic*

10 Feloni, R.; A. Pelisson; "A Retired Marine and Elite Fighter Pilot Breaks Down the OODA Loop, the Military Decision-Making Process That Guides 'Every Single Thing' in Life," Business Insider, 13 August 2017, *https://www.businessinsider.com/ooda-loop-decision-making-2017-8*