DEFENSE & SECURITY

Strengthening Cyber Civil Defense: How Can ISACs Stay Vigilant to Prevent Cyberattacks?

JULY 31, 2024

A single breached password was used on the dark web to log in to a legacy VPN. Hackers reached servers, encrypted around 100 gigabytes of data, and asked for millions of dollars' ransom. After five days of negotiations, the hackers were paid $4.4 million, but meanwhile, due to oil shortages and panic, millions lined up at gas stations, airlines started seeing disruptions, and several other industries were affected on the East Coast. The Colonial Pipeline attack was just an example of how vulnerable we are. The threat actor was DarkSide, a group whose objective was only ransom. Once the hackers received what they were looking for, Americans returned to their routine lives.

In contrast, let's think about the same scenario with a different threat actor, a state-sponsored group that, instead of aiming at extorting a couple of million dollars of ransom, has as its agenda to target and cripple critical infrastructures, damage the economy, affect mobilization efforts, or just create chaos. The result would be drastically different. In a scenario similar to this latter type, Saudi Aramco, one of the largest oil companies, was hit by an Iran-backed threat actor group, and 30 000 workstations were wiped out. This time, recovery took not five days but five months.

While the above is an example of successful attacks on critical infrastructures, the overall situation is not that bad. Millions of other attack attempts were thwarted by related organizations, including industry-specific Information Sharing and Analysis Centers (ISACs), which started their operations a quarter of a century ago, providing threat intelligence services, increasing collaboration, and building capacity for specific industries. But since the

cyberthreat landscape is evolving and challenges are changing, how can these facilities update themselves and stay vigilant to keep preventing cyberattacks? The answer is that their use of emerging threat intelligence capabilities may help them to break more cyberattack kill chains.

Why Are ISACs Needed in the First Place?

Two bombings changed the priorities of the Clinton administration. After the World Trade Center and Oklahoma City bombings (1993 and 1995, respectively), the president appointed the Commission on Critical Infrastructure Protection in 1997 to prevent further attacks. However, since the Commission considered that they themselves were also open to cyberattacks, the scope was expanded to include cyberthreats.

After Presidential Decision Directive-63 (PDD-63), the first ISACs were created as nonprofit organizations in 1999. The goal was to prevent cyber- and physical attacks via industry-based information sharing and analysis centers that, by increasing public–private partnership, would provide actionable threat intelligence.

What Do We Have Now?

Over the years, companies in most critical infrastructure industries took the initiative to create their own ISACs, with Financial Services, Information Technology, and National Defense as some of initial ones. In some cases, organizations took the lead to expedite the establishment of ISACs such as the North American Electric Reliability Corporation (NERC) for Electricity ISAC, the CISA National Coordinating Center (NCC) for Communications ISAC, and the US Fire Administration for Emergency Management and Response ISAC.

After 25 years, the number of sector-specific ISACs has reached 27 in the US as of 2024. Some of the ISACs started providing services globally and, to increase collaboration and coordination among them, the National Council of ISACs (NCI) was created in 2003. Moreover, the success of the ISAC concept in the US has inspired similar international initiatives. Several other ISACs have been created in countries such as the Netherlands, Japan, and Singapore. The European Union Agency for Network and Information Security (ENISA) reported that “ISACs are effective and can scientifically enhance the level of cybersecurity. They create an ecosystem in which trust is being built among critical operators, and experience can be shared.”

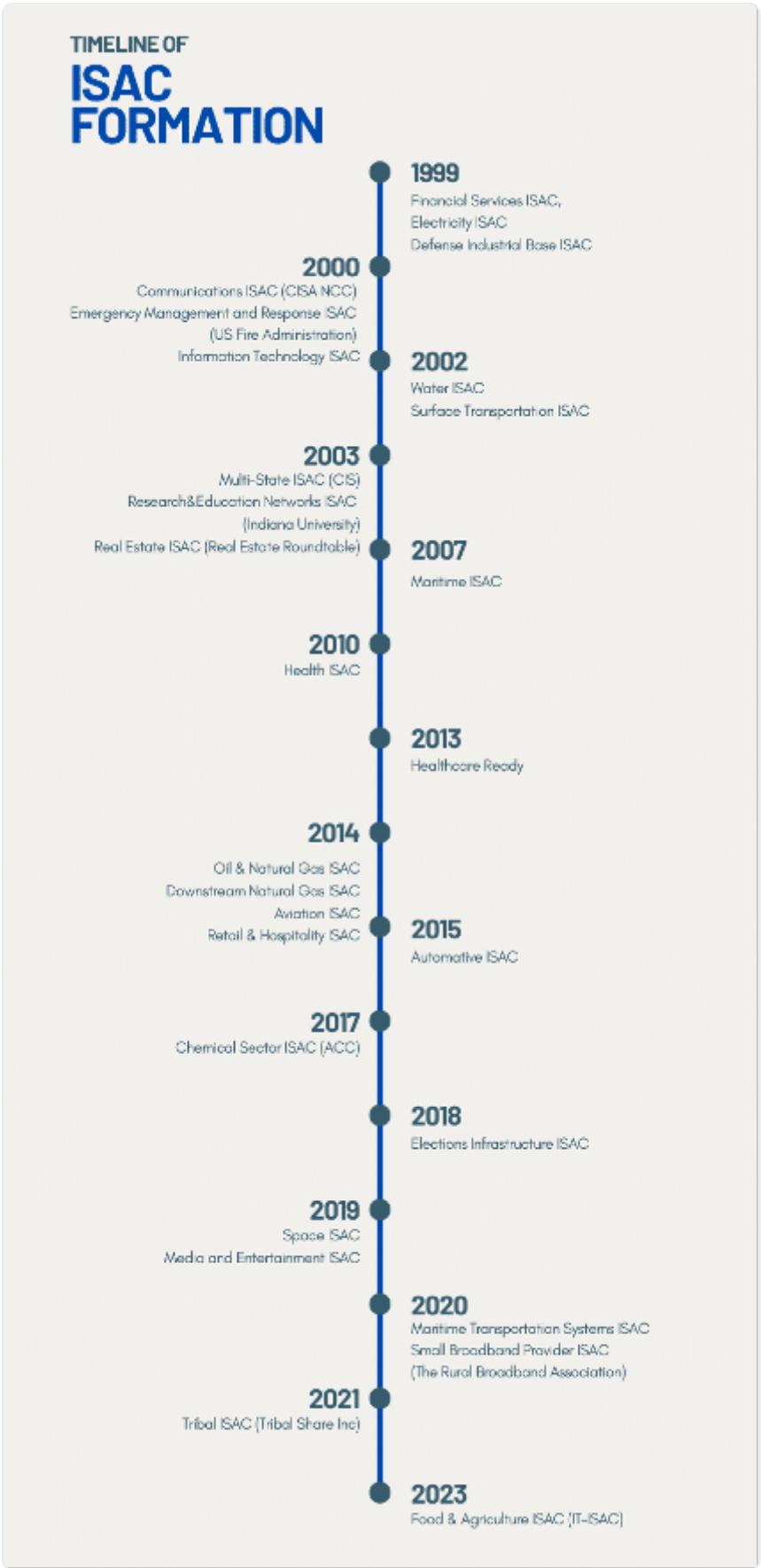
TIMELINE OF
ISAC FORMATION
1999
Financial Services ISAC,
Electricity ISAC
Defense Industrial Base ISAC
2000
Communications ISAC (CISA NCC)
Emergency Management and Response ISAC
(US Fire Administration)
Information Technology ISAC
2002
Water ISAC
Surface Transportation ISAC
2003
Multi-State ISAC (CIS)
Research&Education Networks ISAC
(Indiana University)
Real Estate ISAC (Real Estate Roundtable)
2007
Maritime ISAC
2010
Health ISAC
2013
Healthcare Ready
2014
Oil & Natural Gas ISAC
Downstream Natural Gas ISAC
Aviation ISAC
Retail & Hospitality ISAC
2015
Automotive ISAC
2017
Chemical Sector ISAC (ACC)
2018
Elections Infrastructure ISAC
2019
Space ISAC
Media and Entertainment ISAC
2020
Maritime Transportation Systems ISAC
Small Broadband Provider ISAC
(The Rural Broadband Association)
2021
Tribal ISAC (Tribal Share Inc)
2023
Food & Agriculture ISAC (IT-ISAC)

Fig.1: Timeline of ISAC Formations

What Services Do ISACs Provide?

Over the years, the number of services that ISACs provide has increased. Depending on the number of ISACs providing them, we can categorize these services into four groups.

Core services are provided by all ISACs. Sharing indicators of compromise (IOCs) among organizations helps ISAC members to increase their preparedness. For example, when an organization is attacked by a threat actor using a malicious file, the victim organization shares the hash of the malicious file with other member organizations, making them aware of the threats. In addition to the IOCs that member organizations share, ISACs may bring government, open source, and paid threat feeds into their data lake. To enable intelligence sharing among member organizations, ISACs utilize standardization methods.

Common services are provided by most of the ISACs. Human-readable notification reports for vulnerabilities, incidents, malware, and threat actors help member organizations learn from the latest experiences of victim organizations. In most cases, these reports are provided by ISAC analysts. Additionally, ISACs organize regional threat calls and set up peer communications and workgroups to increase collaboration and cooperation among member organizations. Also, organizing events and creating best practices and playbooks can be included as common services that ISACs provide to increase the readiness and awareness of the member organizations.

Less common services, ones provided by a small number of ISACs, include capacity-building support for their members, such as tabletop and hands-on cyberattack exercises and workshops that increase readiness and building capacity for member organizations.

Specialized support services, offered by only a couple of ISACs, provide free or low-cost security services to their members, including security operation center (SOC) support, post-incident media response support, and dark web and social media monitoring. By adding these services to their portfolios, these ISACs thus provide more value for their member organizations.

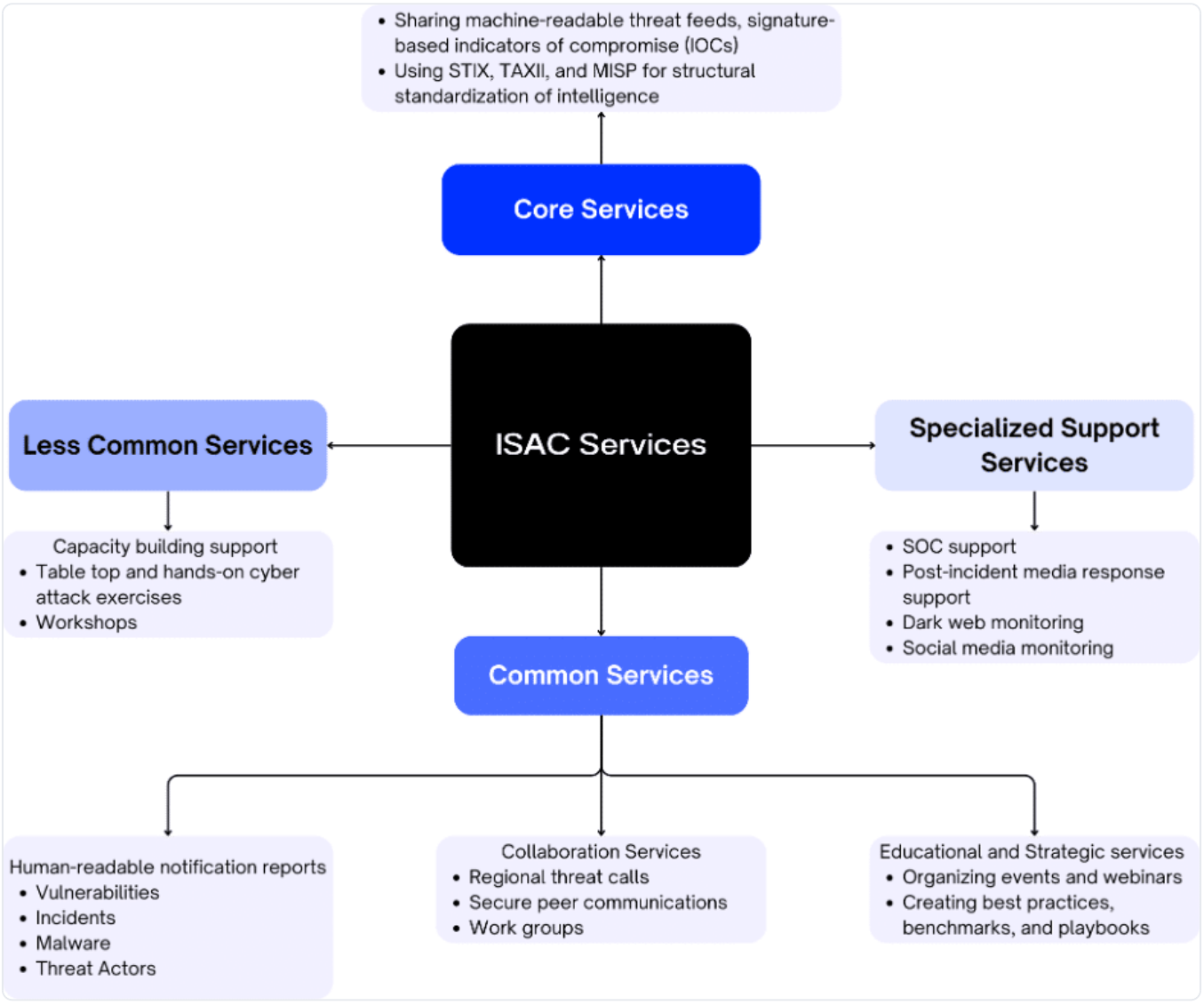

Fig. 2: ISAC Services

What Are the Changes in Cyberspace and the Threat Landscape?

Alongside the increase in the number of ISAC services, it is critical to understand the current cyberspace and threat landscape to ensure that these facilities can provide the required services for their members to prevent attacks on critical infrastructures. Several factors have brought about profound changes.

Covid has made big transformations in our lives and affected cyberspace. Online shopping has increased by 55%, the number of remote workers has tripled, and education has gone

increasingly online in the US. These changes have caused an unprecedented boost in digital infrastructures, making businesses and individuals more **cyber dependent**.

Cloud infrastructure has also been adopted more and more widely because of its cost reduction, scalability, and security. According to Gartner, the cloud services market increased by 42% in the last two years and is expected to grow by around 25% in the next years.

Software-as-a-service (SaaS) application usage has also increased due to its cost efficiency, scalability, and accessibility. According to Statista, SaaS investment has increased by 450% in the last seven years, and it is estimated that by 2025, the SaaS-based business app rate will reach 85%. This is yet another factor that increases organizations' **third-party dependency**.

The emergence of cyber trends, however, comes along with cyberthreats, as Fig. 3 summarizes.

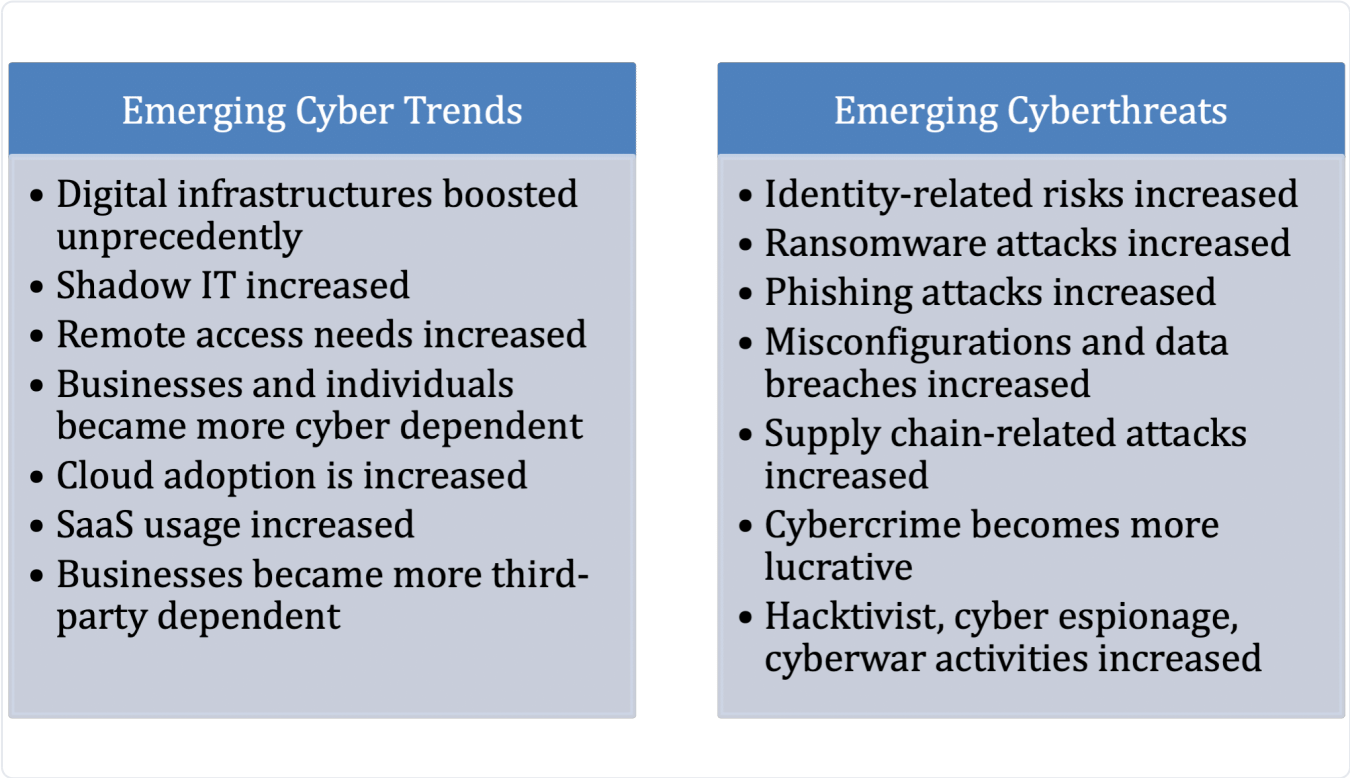

Fig. 3: Cyber trends and threats

Recent digital transformation has also affected threat actors' operations and changed the cyber- threat landscape. The boost in digital infrastructure and increase in SaaS adoption has

reduced the visibility of security teams on their attack surfaces and created Shadow IT, which refers to IT assets unknown or unverified by the security teams. When organizations have unknown assets on their infrastructure, it is obviously impossible to detect their vulnerabilities and configuration weaknesses. On top of that, an increase in remote work is required to provide more remote access to corporate resources. Unknown and unmanaged remote accesses have opened businesses to ransomware attacks, where threat actors remotely access business networks, steal and encrypt corporate data, and ask for a ransom fee to decrypt and not share/sell the stolen corporate data.

The increase in cloud infrastructure usage and SaaS application, combined with increasing remote access needs, has made access management critical to fend off identity-related risks. Compromising a digital identity is, however, more important for threat actors, who deploy information-stealer malware designed to accomplish this goal. To steal files, credentials, and session cookies, threat actors have started using infostealer malware, which even enables them to bypass multi-factor authentication. Subsequently, the stolen data is put on sale on black markets. As a result, IBM and Verizon have put identity theft into the top three initial attack vector lists, and two sayings have emerged from opposite perspectives: “Identity is the new perimeter” and “No need to hack in when you can log in.”

Also, the increase in identity-related risks has increased the number of phishing attacks designed to steal individuals’ credentials and digital identities. Since humans are still the weakest link in the chain, threat actors have used social engineering tactics to convince individuals to click on malicious links and provide their passwords on fake websites. Security organizations have put phishing attacks at the top of the list for initial attack vectors, estimating that between 30% and 45% of cyber-attacks start with a phishing attack.

Furthermore, the rise in cloud infrastructure has also increased data breaches from misconfigured cloud assets. Data breaches from BMW Global and Microsoft made headlines, but these misconfigurations also played a part in the Verizon report since medium and even small businesses have similarly growing problems. The source of the problem is the same: a human misconfiguration error. When a system administrator misconfigures the access rights of a cloud asset, it may mistakenly become public, which is becoming a more common type of

data breach.

Increasing third-party dependency has furthermore allured threat actors to target businesses that enable them to attack other businesses for which they provide services. The recent SnowFlake incident, affecting a leading cloud-based data storage provider, was a good example of this. Threat actors used stolen credentials to log in to SnowFlake accounts, accessing customers' stored data. After exfiltrating the data, they either sold or shared the stolen databases on dark web platforms. Several large enterprises were affected by the attack, including Ticketmaster, Truist Bank, and AT&T.

The digital transformation highlighted above also caught the attention of various actors, including businesses, organized crime groups, hacktivists, and nation states, enabling them to launch cyberattacks to achieve their objectives. Competition-driven industrial cyber espionage activities specifically targeting critical infrastructures increased. Cybercrime, due to its profitability, became one of the top three lucrative illegal businesses alongside drug and human trafficking, and organized crime groups started investing in their cybercrime activities, including business email compromise attacks (BEC) and ransomware. Political tensions in Eastern Europe and the Middle East have increased hacktivist attacks and motivated the aim of nation-states to achieve strategic goals without conventional confrontations.

How Should ISACs Adapt to Evolving Threats?

Changes in cyberspace and the threat landscape not only created new challenges for ISACs in helping their members prevent attacks but also created new opportunities. As detailed above in the ISAC Services section, ISACs have mainly utilized the sharing of signature-based intelligence and threat reports and focused on increasing collaboration between security teams of their member organization to increase preparedness. These efforts have helped US critical infrastructure companies in the last 25 years; however, the changes in the threat landscape has made cyber-attacks more complex, and this, on the other hand, has provided defenders with the opportunity to proactively take action and prevent cyber-attacks. Sharing signature-based intelligence was the best way to break the chain of cyberattacks in their kill chain, but there are new cyber chainbreakers to prevent the new threats. ISACs should utilize these new

services as detailed below to prevent more attacks.

Fig. 4: Cyber attack chainbreakers

Dark web intelligence. Threat actors have started focusing on specific chains of cyberattacks to be more efficient. A threat actor conducts phishing attacks to steal login information, while another focuses on acquiring valid unauthorized remote access using this stolen login information; yet another provides ransomware tools and services; another threat

actor gets unauthorized remote access and the tools and services to conduct ransomware attacks to get paid, and another threat actor focuses on laundering the ransom payment. In such a process, threat actors can stay efficient in their attacks, but all these steps require communication, collaboration, and transactions, which will happen on dark web platforms. When ISACs start utilizing dark web intelligence, they can proactively detect and prevent different types of attacks.

Identity intelligence. Since identity-related risks are increasing, threat actors increasingly focus on stealing, acquiring, and sharing stolen identities. This growing demand matures dark web sources, making the markets more structured and automated. To cope with these transactions and prevent attacks, ISACs should utilize focused identity intelligence to proactively detect and automatically help remediate risks for their member organizations.

Surface web intelligence. In most cases, people misconfigure the access rights of their assets, which results in data leakage on the surface web. Threat actors go after these low-hanging fruits and collect these data to share or sell on dark web platforms; others collect or buy them to conduct new attacks. When ISACs utilize surface web intelligence, they can proactively detect data breaches, especially from code repositories and cloud assets, and prevent data leaks.

Attack surface intelligence. Business needs and new cyber trends are boosting digital infrastructures, which is reducing the visibility of security teams and creating shadow IT. Factors that reduce healthy communications and always increase shadow IT include the following: having a large organization where individual departments can acquire new assets, having several locations, having a group of companies, and executing mergers and acquisitions. It is important to view your organization from an external perspective to see what a threat actor sees, which is critical to eliminate shadow IT. As external parties, ISACs can utilize attack surface intelligence or help their members detect these unknown assets, potentially the weakest link for organizations.

Vulnerability intelligence. An increase in digital infrastructures increases the detected vulnerabilities for security teams. Since resource constraints make it ineffective to patch all

vulnerabilities, prioritization for patch management activities becomes more important. To understand which vulnerabilities are more critical, comparing their CVSS (Common Vulnerability Scoring System) scores will not help because of their limitations. It is important to have data collection points on the dark web, surface web, and known attacks to understand how critical those vulnerabilities are. Threat intelligence on vulnerabilities, called vulnerability intelligence, can be utilized by ISACs to help understand critical vulnerabilities and patch them immediately to prevent attacks.

Phishing intelligence. Signature-based intelligence sharing may help reduce phishing attacks, but threat actors are getting better at creating new assets by utilizing phishing kits, which include tools to easily create phishing infrastructure for people with little or no technical skills. This forces security teams to proactively detect phishing domains before the attacks and take down the domain to prevent the attack even before it begins. Since ISACs provide services for specific industries, they may use threat-hunting activities and data analysis techniques to detect new phishing assets to be taken down for their members.

Supply chain intelligence. Since third-party dependency for businesses is increasing, it is becoming more important to manage and reduce related risks by understanding the cybersecurity posture of third-party and supply chain companies and being aware when they become victims of a cyberattack. These third-party companies include organizations they have contracts with and their infrastructures depend on. Since ISACs provide services for specific industries, it would be more efficient to monitor critical supply chain companies and share supply chain intelligence with their member organizations.

In conclusion, emerging cyber trends and the cyberthreat landscape require new cyberattack chainbreakers to proactively prevent cyberattacks. ISACs play an important role in preventing attacks, and adopting these new chainbreakers may help them maintain vigilance to prevent cyberattacks.

Orion Policy Institute (OPI) is an independent, non-profit, tax-exempt think tank focusing on a broad range of issues at the local, national, and global levels. OPI does not take institutional

policy positions. Accordingly, all views, positions, and conclusions represented herein should be understood to be solely those of the author(s) and do not necessarily reflect the views of OPI.