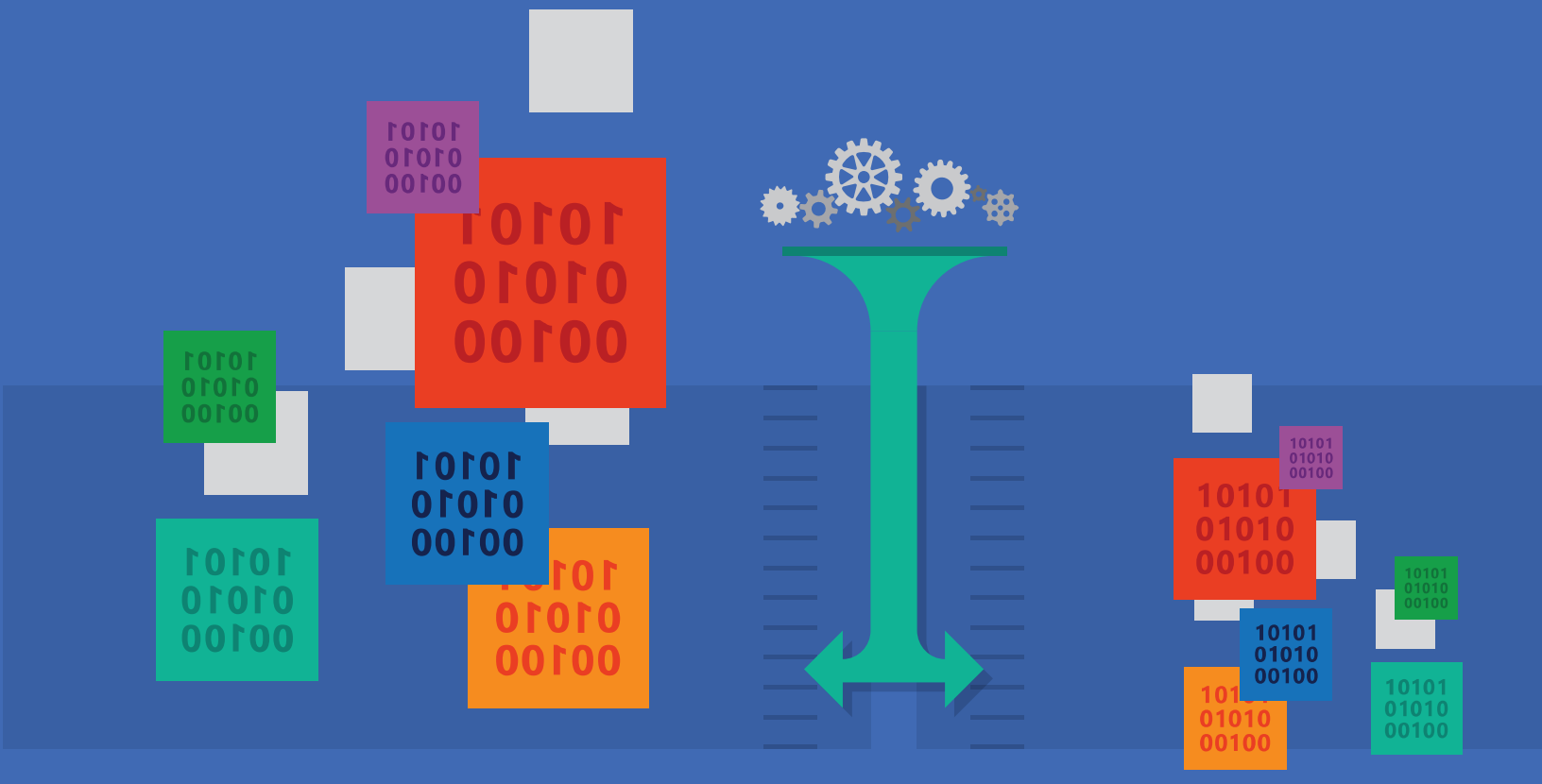
Microsoft

A framework for cybersecurity information sharing and risk reduction

Cristin Goodwin
J. Paul Nicholas



Contributors

Jerry Bryant

Kaja Ciglic

Aaron Kleiner

Cornelia Kutterer

Alison Massagli

Angela McKay

Paul McKitrick

Jan Neutze

Tyson Storch

Kevin Sullivan

Contents

Foreword

Today's cybersecurity threat environment poses a greater challenge than ever before. The recent surge of sophisticated, targeted cyber-attacks against governments and businesses highlights the need for improved defenses. Organizations must protect against attackers who assiduously research their targets, analyze their weaknesses, and use this information to tailor their assaults.

Facing such threats, the benefits of collective action stand apparent. A crucial component of a collective response to cyber-threats is the sharing of information and how quickly it can be acted upon. When information about attackers and methods of attack is shared, organizations are better prepared to thwart them. In this case, forewarned really is forearmed.

Leveraging the years of experience Microsoft has in managing security infrastructure, this paper provides historical background on information sharing, followed by a taxonomy of information exchange that includes models, methods, and mechanisms. It concludes with recommendations that can help lay the groundwork for a more formalized, collaborative approach to sharing information and implementing exchanges.

A framework for cybersecurity information sharing and risk reduction is intended to be a relevant and timely guide for anyone responsible for developing new ideas and solutions for information exchanges. I hope you will find this paper useful in helping to bring about a safer and more secure online ecosystem.

Matt Thomlinson

Vice President, Microsoft Security

Microsoft Corporation

Introduction

It is often said that information is power. This is particularly true in a world that moves at Internet speed. In cybersecurity, receiving the right information at the right time can empower decision-makers to reduce risks, deter attackers, and enhance resilience. Sharing the right information is more than people exchanging data, it is also about the automation of machine-to-machine sharing to counter fast-moving threats.

There is a growing awareness of cybersecurity risk and its implications for national and international security. The sharing or exchange of information is, therefore, being encouraged by legislators and other stakeholders who recognize that the ability to reduce cybersecurity risks to government systems, critical infrastructures, and enterprises increasingly depends on this form of collaboration.

Although *information sharing* has become a common term among policymakers, the concepts related to its practice and purpose are not always clearly understood. Information sharing describes a means of conveying information or experience from one trusted party to another. There is general agreement that information sharing and collaboration reduce cybersecurity risk. But confusion and controversy remain around the particulars:

- Who should share information?
- What should be shared?
- When should it be shared?
- What is the quality and utility of what is shared?
- How should it be shared?
- Why is it being shared?
- What can be done with the information?

Information sharing often begins as an ad hoc collaboration, particularly during a crisis that aligns disparate sectors and even competitors toward a unified, collective response. For example, in 2008, the Conficker Working Group came together to share information and develop a response to the Conficker worm, which had infected millions of computers around the world. Information Sharing and Analysis Centers (ISACs) were mobilized, company incident response teams were activated, government responders were engaged, and the media reported the milestones reached, services restored, and further steps needed. Participants in the response were willing to share information because there was a mutual benefit to be gained from the collective response. Trust developed between the responders, notably between government responders and private sector participants.

The ability to repeat ad hoc exchanges over time builds trust and an expectation that parties will act in a consistent and repeatable way that minimizes harm and maximizes protection. Sustaining these ad hoc efforts in a more structured way requires careful consideration of the what, when, how, and why of information sharing. Understanding these building blocks can help develop structures that not only build trust but also actively support collaboration in reducing cybersecurity risks.

Trust plays a critical role. Trusted relationships foster confidence that information provided will be acted upon and that it will be protected and/or shared appropriately. Although trust is powerful, it is also fragile and, if broken, can have devastating consequences for all parties. Furthermore, trust is impossible to effectively legislate. So, given the complexity of the cybersecurity threats, a private and public collaborative approach to information sharing is called for. Laws can compel incident reporting, but they do not increase trust or collaboration nor do they reduce risks.

The pressure to build effective information sharing programs increases as security incidents in government agencies, critical infrastructure, and private enterprise networks grow in number, scale, persistence, and sophistication. Governments are beginning to recognize the importance of information sharing as a means of reducing cybersecurity risk. Governments, including European Union (EU) member states, the United States, Japan, and Korea, have made efforts to enhance and expand information sharing and many have recognized the importance of balancing privacy and civil liberties.

The security benefits of sharing information must be achieved in a way that does not erode privacy or adversely impact freedoms. Sharing cybersecurity data can create a number of privacy and civil liberties concerns, including:

- What type of information is shared?
- To what extent can it be linked to individuals or organizations?
- Who is the information shared with (particularly when transmitted from the private sector to government)?
- How is the information stored and used?

Strong privacy and civil liberties protections are paramount if an information sharing program is to be widely accepted and to succeed.

The breadth of information sharing needed to address current and future threats requires a clear purpose, a strategy, automation, and operational excellence to succeed. This paper provides a framework for discussing information sharing and offers recommendations for improving its application in reducing cybersecurity risk.

Building blocks for sustainable sharing and collaboration

Building an effective and sustainable information sharing program requires a detailed understanding of the following elements:

- **Actors involved.** Who needs to share information, and who can resolve the issues that emerge?
- **Types of information exchanged.** What information is being shared, and what is the purpose of sharing it?
- **Models of exchange.** What is the impetus behind information sharing? Is it shared voluntarily or a regulated requirement?
- **Methods of exchange.** What is the organizational structure and governance for sharing information?
- **Mechanisms of exchange.** How is the information actually shared?
- **Scope and operational purpose.** How is an information exchange structured to ensure that it delivers the greatest value?

Actors involved

The individuals or types of organizations, each with their own perspectives, interests, and needs, greatly influence the formation of any information exchange. These actors may also have varying degrees of technical capability, face significantly different threats, and have separate motivations for acting upon cybersecurity information. Given the variation in backgrounds of those involved, discerning and articulating the unique needs and requirements is a prerequisite for building trust. Understanding the value each member contributes to the exchange is key. Identifying the membership criteria for any information sharing effort helps build transparency and trust from day one.

Actors and their roles in the cybersecurity information sharing ecosystem	
Government	Governments have national economic and security duties that include the need to defend their own classified and unclassified systems, fight cybercrime, and help reduce the cybersecurity risk to its citizens.
Private critical infrastructure	Although the protection of critical infrastructure is often in private hands, its security is central to the government's goals of ensuring such critical national interests as public health and defense.
Business enterprises	Private companies have an interest in preserving the security of sensitive information, such as customer data, trade secrets, contract information, and other intellectual property.
IT companies	Firms creating IT products and services have an interest in preserving the security and integrity of their offerings. They often share information on vulnerabilities in products or services so that security firms can create solutions to remedy them, or they may produce and distribute software updates that remedy vulnerabilities for their customers.
IT security firms	IT security firms, including antivirus vendors, computer forensics experts, and penetration testers, collect and sell cybersecurity information, along with services flowing from that information, to others in the ecosystem.
Security researchers	Security researchers track malicious software and targeted attack campaigns, and they find vulnerabilities in software, hardware, and services through academic work, business, or voluntary collaborative efforts or to satisfy individual curiosity. They may notify relevant responders to help mitigate threats and remedy weaknesses, or they may choose to report their findings publicly.

Table 1. Actors involved in information sharing

Types of information exchanged

Seven major types of information are typically shared through exchanges. The following conceptual framework illustrates how they relate to one another and how they can be leveraged for specific outcomes.

Types of cybersecurity information	
Incidents	Details of attempted and successful attacks that may include a description of information lost, techniques used, intent, and impact. The severity of an incident could range from a successfully blocked attack to a serious national security situation.
Threats	Yet-to-be-understood issues with potentially serious implications; indicators of compromise, such as malicious files, stolen email addresses, impacted IP addresses, or malware samples; or information about threat actors. Threat information can help operators detect or deter incidents, learn from attacks, and create solutions that can better protect their own systems and those of others.
Vulnerabilities	Vulnerabilities in software, hardware, or business processes that can be exploited for malicious purposes.
Mitigations	Methods for remedying vulnerabilities, containing or blocking threats, and responding to and recovering from incidents. Common forms of such information include patches to plug vulnerabilities, antivirus updates to stop exploitation, and directions for purging malicious actors from networks.
Situational awareness	Information that enables decision-makers to respond to an incident and that may require real-time telemetry of exploited vulnerabilities, active threats, and attacks. It could also contain information about the targets of attacks and the state of critical public or private networks.
Best practices	Information related to how software and services are developed and delivered, such as security controls, development and incident response practices, and software patching or effectiveness metrics.
Strategic analysis	Gathering, distilling, and analyzing many types of information to build metrics, trends, and projections. It is often blended with projections of potential scenarios to prepare government or private sector decision-makers for future risks.

Table 2. Types of cybersecurity information

Information sharing

The foundation for cybersecurity risk management

- **Information sharing is the process of sharing information about cybersecurity incidents, threats, vulnerabilities, best practices, mitigations, and other topics.**
- **Information sharing can help entities better manage**

Cybersecurity information types

Incidents

Details of attempted and successful attacks that may include a description of information lost, techniques used, intent, and impact. The severity of an incident could range from a successfully blocked attack to a serious national security situation.

Threats

Yet-to-be-understood issues with potentially serious implications; indicators of compromise, such as malicious files, stolen email addresses, impacted IP addresses, or malware samples; or information about threat actors. Threat information can help operators detect or deter incidents, learn from attacks, and create solutions that can better protect their own systems and those of others.

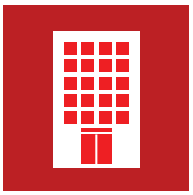
Vulnerabilities

Vulnerabilities in software, hardware, or business processes that can be exploited for malicious purposes.

Key actors

Government

Private critical infrastructure



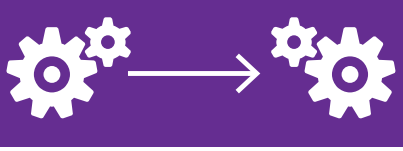
Business enterprises

Exchange

Mechanisms of exchange

Person to person

Machine to machine



cybersecurity risk by improving collaboration.

- **By better understanding information sharing, organizations can create programs that are responsive to the challenge of cybersecurity.**

Microsoft

www.microsoft.com/cybersecurity

Mitigations

Methods for remedying vulnerabilities, containing or blocking threats, and responding to and recovering from incidents. Common forms of such information include patches to plug vulnerabilities, antivirus updates to stop exploitation, and directions for purging malicious actors from networks.

Situational awareness

Information that enables decision-makers to respond to an incident and that may require real-time telemetry of exploited vulnerabilities, active threats, and attacks. It could also contain information about the targets of attacks and the state of critical public or private networks.

Best practices

Information related to how software and services are developed and delivered, such as security controls, development and incident response practices, and software patching or effectiveness metrics.

Strategic analysis

Gathering, distilling, and analyzing many types of information to build metrics, trends, and projections. It is often blended with projections of potential scenarios to prepare government or private sector decision-makers for future risks.

IT companies

IT security firms

Security researchers

Methods of exchange

Formalized	Trust-based	Security clearance-based	Ad hoc
			

Each type of information has a different use. Some information helps government and private sector entities assess the risk to cybersecurity at a national or an organizational level, including the risk to critical infrastructure. Some contributes to analyzing cybersecurity in the long term and to creating incentives for better security. Other types of information can be used to detect attacks, identify incidents, and observe those incidents to determine the objectives of the attackers. Some, such as best practice information, is more directly actionable for improving hardware, software, and services or for making immediate improvements to network defense. Additionally, security information concerning fraud and abuse can be used to protect the identities, defend account compromises, and for general ecosystem hygiene. Finally, information sharing is increasingly viewed as a tool to facilitate attribution and legal responses.

Increasingly, vulnerability and mitigation information is seen as useful in helping actors across the different sectors decide how best to best assess and manage risk. This trend reflects a growing understanding of the need to develop better analytical capabilities to understand strategic threats and to better anticipate new risks to Information and Communications Technology (ICT) and the whole spectrum of the economy it enables.

High-quality strategic information can help to project where the next classes of cyber-threats may come from and to identify the incentives that could motivate future attackers, along with the technologies they may target. Additionally, strategic analysis can help put incidents into a broader context and can drive internal changes, enhancing the ability of any public or private organization to update risk-management practices that reduce its exposure to risk.

Often, information is shared by one party with another without any expectation of immediate or near-term reciprocity. However, a company may supply information about an impacted customer or a technical vulnerability in the hope that, over time, trust will grow between partners and information will flow in both directions.

During the past 15 years, governments have focused on increasing the flow of information shared internally or with close allies. Most often, this sharing has occurred around specific cybersecurity incidents, with the goal of acquiring data to gain insight into the nature and scope of a security incident. This after-action analysis is critical to understanding attack trends. It is the challenge of government to ensure the right balance of collecting, analyzing, and disseminating information to defeat the immediate attack and to prepare for long-term security.

In addition to incident response, there is a robust and growing effort to share best practices related to the secure development of software and services. These include security controls, coding and development practices, and practices for patching software and responding to incidents, along with metrics of the effectiveness of these procedures.

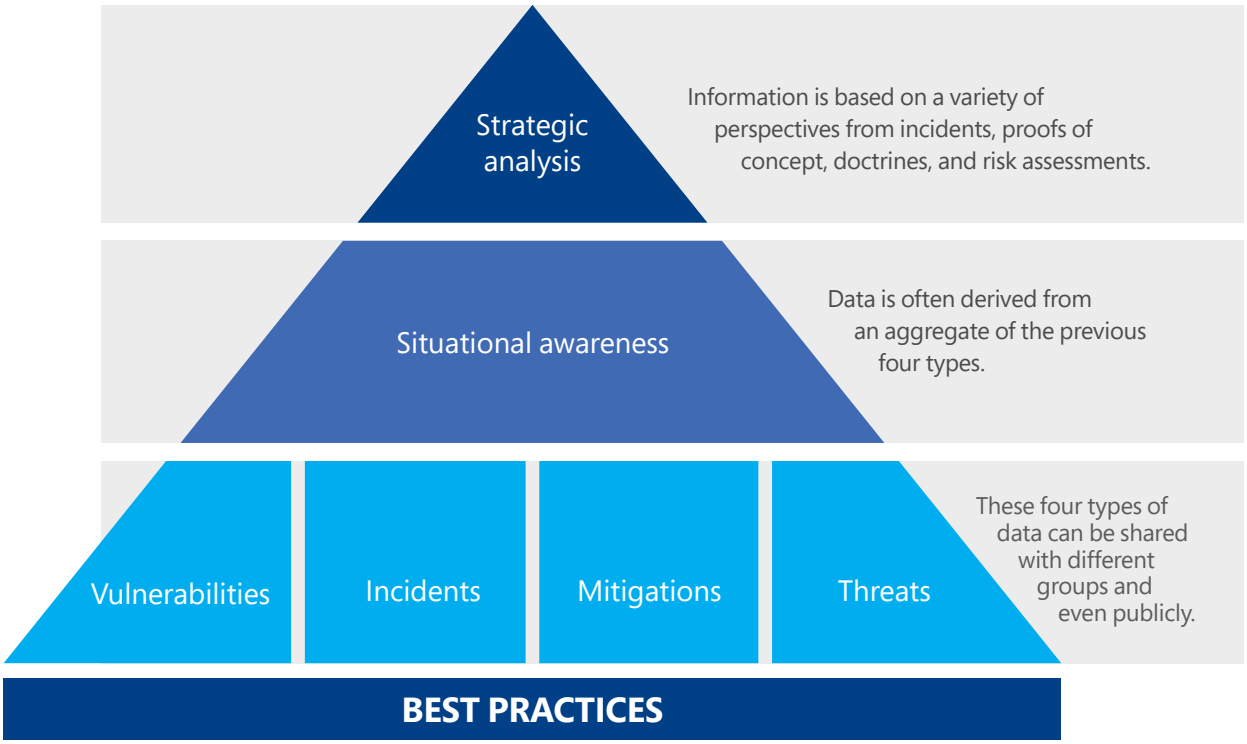


Figure 1. Types of cybersecurity information

Models of exchange

Information sharing can range from sporadic ad hoc exchanges to exchanges established through long-term formal organizations. The different approaches most often reflect variables such as the level of trust between the parties, the legal authority of various actors, and the relationships between the stakeholders. Each model has its advantages, but selecting the right model for the right purpose is vital to success. The following highlights two exchange models: voluntary sharing and mandatory disclosure.

Voluntary exchange models

The voluntary exchange of data is perhaps the richest and most valuable exchange that exists in the cybersecurity ecosystem. With voluntary information sharing, actors identify a need or a reason to exchange data and to begin to share and use what is valuable and actionable. Governments and companies often decide with whom to share information based on the type involved and the objectives of the parties.

For example, governments may voluntarily share with other governments on a bilateral basis or they may choose to share with a group of governments. In other instances, a government's need for national security gives it a clear mandate to share important information with industry, specifically about threats and vulnerabilities.

Similarly, voluntary efforts in the private sector can be bilateral or may involve a group of entities. Private sector entities often share information on incidents, threats, vulnerabilities, and mitigations to, among other things:

- Contribute to a collective national defense or response.
- Protect their customers, brand, and products.
- Inform authorities of serious situations.
- Report criminal activity.

In some instances, a private sector company will voluntarily share information with both industry and government.

The most effective scenarios for sharing information seem to be private company–to-company exchanges, in addition to the collective responses to large incidents or threats. Thus, as governments look to develop the most effective information sharing regimes or incident reporting obligations, they must consider how to deepen trust, provide a collective benefit while minimizing reputational risk, and respond to a clearly articulated national incident.

Lastly, it is also worth noting that some cybersecurity information is exchanged through commercial sales by security companies and researchers. Because of an increase of information about threats, incidents, and vulnerabilities, a significant market has emerged to meet the demand for better security. Private incident response and forensics firms have recently become important both as responders to breaches and as network monitors, operating from the proprietary information they collect and from information shared by third parties. However, certain purchased information may be used outside its intended purpose (for example, to exploit systems), so it is important that any such information is protected.

Mandatory disclosure models

Governments increasingly require the disclosure of security event information to regulators and other government authorities, investors, or impacted individuals, including customers. Although these regulatory disclosure provisions are currently limited in most countries, there is a consistent push toward requiring greater incident reporting, particularly when the incident impacts critical infrastructure.

In the United States and the European Union, laws require that companies report breaches of personally identifiable information to persons impacted by the breach. For example, the European Commission's draft NIS Directive would create additional requirements on "market operators" to report serious incidents to national authorities.

There is a concern that a mandatory approach to incident reporting will distract from the more important focus on information sharing or incident response. It is critical that governments do not conflate incident reporting or their own need for situational awareness with information sharing between trusted parties.

Moreover, suggestions around moving from voluntary information sharing to required information sharing have generally been received with reluctance by the private sector. Mandatory incident reporting is inherently one-directional and does not, on its own, improve operational security or response. Often, the focus is on the reporting itself and not on how the gathered information will be used, calling into question the fundamental goals of mandatory reporting. It is critical that mandatory incident reporting be clearly focused and narrowly scoped to ensure reported data is used to improve security and that privacy is protected. Microsoft offers the following principles to help guide the development of mandatory incident reporting policies.

PRINCIPLES FOR INCIDENT REPORTING POLICIES

Policies that require sharing security incident information should be:

- aligned to clearly defined outcomes, such as protecting privacy, public safety, response coordination, or improving security defenses.
- flexible and commercially reasonable and should leverage commonly accepted approaches and international standards, where possible, avoiding incompatibility.
- attentive to balancing the risks and benefits associated with publishing incident details.
- mapped to specific outcomes and not arbitrarily chosen with timelines for reporting incidents.
- supported with research and development in both the public and private sectors.

Methods of exchange

Organizations can exchange information any number of ways. The four most commonly used are formalized, security clearance-based, trust-based, and ad hoc. In almost all situations, the method of exchange determines which actors can be included and it defines the scope of the program. Therefore, when designing an exchange, it is important to determine the method that best corresponds to the group membership and its goals.

Formalized exchanges

A formalized exchange is one based on an agreement, such as a non-disclosure agreement, legal contract, or a membership agreement. Its conditions identify the parties and often state what information is to be exchanged, how it can be used, and how its confidentiality will be protected.

One example of a formalized exchange is the Microsoft Active Protections Program (MAPP),[1] a program for security software providers that currently brings together more than 80 partners. Members of MAPP receive security vulnerability information from the Microsoft Security Response Center (MSRC) in advance of the monthly security updates from Microsoft. This information enables them to give their customers updated protections, such as antivirus software, network-based intrusion detection systems, or host-based intrusion prevention systems. Another example is the Asia Pacific Computer Emergency Response Team (APCERT),[2] a membership-based organization established to enhance cooperation among more than 30 CERTs in the Asia Pacific region.

Security clearance-based exchanges

Certain information-exchange programs, especially those involving intelligence services, need to exchange classified and other sensitive information through protected channels, sometimes directly with a single party. A security clearance-based exchange represents a subset of a formalized exchange, one that is narrower in scope and participation.

In the long term, the security clearance process builds trust between participants. However, it can also severely constrain the actors involved, such as limiting participants to those of a particular country—a challenging requirement in a global market. Getting private sector participants cleared can be difficult and slow and is made even more complex by the international workforces found in large technology companies. Such classified exchange is more likely to be successful when involving defense contractors or other entities which are accustomed to working with classified material.

Trust-based exchanges

Trust-based groups are often closed groups of like-minded cybersecurity actors who inform one another on an ad hoc basis when they see security issues of common concern. They work on the principle that trust is extended to unknown members through chains of trusted relationships with other known members. They generally do not have formal agreements or contracts covering the exchange of information between members, but they may implement systems like the Traffic Light Protocol (TLP).[3] The TLP uses a color-coded system to identify those with whom information may

1 Microsoft Active Protections Program. Security TechCenter. 2014. www.microsoft.com/security/msrc/collaboration/mapp.aspx

2 Asia Pacific Computer Emergency Response Team. www.apcert.org

3 "Traffic Light Protocol." US CERT. https://www.us-cert.gov/tlp

be shared, thus signaling originator's intent and easing fears about the extent of disclosure. The TLP also speeds information exchange, since recipients intrinsically know with whom they can share that information—without having to refer to the originator for permission to share it.

Systems to establish and maintain trust among members can range from simple nominations by existing members to rigorous vouching and vetting systems. Trust is often afforded to individuals and not directly to the organizations for which they work. This means that, if an individual leaves an organization, the organization may not have the right to nominate another representative. Trust is built among participants based on their contributions, collective actions, and shared experiences.

Ad hoc exchanges

Episodic or ad hoc information sharing often occurs in response to particular events, such as a new challenge or crisis, and is often of limited duration. This type of sharing is highly relevant and very focused on solving a particular set of problems. When successful, it can lay the foundation for more organized exchanges.

Mechanisms of exchange

An information exchange may use multiple mechanisms, depending on the nature of the information, actors involved, and the issues being addressed. To identify the most appropriate mechanism, the levels of automation required and the format of the information being exchanged need to be considered.

Person-to-person exchanges

Many information exchanges are person-to-person exchanges of unstructured information. The most common mechanisms are email and phone calls, although encrypted email and web portals may also be used. For example, the Financial Services Information Sharing and Analysis Center (FS-ISAC)[4] and the US CERT allow participants to submit threat data that they collect through a web portal. Another example is the UK self-help portal for small communities, "Warning, advice and reporting point" (WARP),[5] which is based on ISO 27010[6] and which encourages information sharing. Such an exchange mechanism is potentially valuable because it can handle large amounts of data and can allow participants to anonymously submit information. However, the challenge with person-to-person exchanges is that they are difficult to scale, requiring significant personal relationships with history and trust to facilitate the exchange of information.

Machine-to-machine exchanges

Among security professionals, there is currently a lot of focus on developing systems that automate the exchange of information. It is believed that such systems enable actors not only to identify information important to them more quickly, but also to automate mitigations to threats as they occur. In the United States, recent examples of machine-to-machine information exchanges include: the Security Event System and its Collective Intelligence Framework component, from the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC);[7] Public Regional Information Security

4 FS-ISAC. https://www.fsisac.com/

5 Warning, advice and reporting point. www.warp.gov.uk

6 "ISO/IEC 27010:2012 Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications." IsecT Ltd. 2014. www.iso27001security.com/html/27010.html

7 Research and Education Networking Information Sharing and Analysis Center. http://www.ren-isac.net/

Event Management (PRISEM),[8] from the state of Washington; and the Enhanced Cybersecurity Services (ECS)[9] offered by the US Department of Homeland Security (DHS).

Microsoft Interflow[10] is a security and threat information exchange platform for professionals working in cybersecurity that works with a similar set of principles. It uses industry specifications, such as Structured Threat Information eXpression (STIX)[11] and Trusted Automated eXchange of Indicator Information (TAXII),[12] to create an automated, machine-readable feed of threat and security information that can be shared across industries and groups in near real time. This can help reduce cost and increase the speed of defense by automating processes that are currently often performed manually.

Information formats

Many (if not most) information exchange initiatives rely on people to actively communicate with their counterparts, which means that sharing is informal and situation-dependent. As information exchange is automated, standards need to develop to ensure machine-readability and interoperability.

Open response

When responding to an incident, organizations such as ISACs or the Industry Consortium for Advancement of Security on the Internet (ICASI)[13] share general information over a conference call and provide specific information by email. A request for support or resources may come in any format an organization uses, such as spreadsheets or simple text files.

Unique information sharing

New and novel incidents almost always result in the need to share information in unique ways. The party under attack may only be willing to share enough information to facilitate a more rapid restoration of their systems. Although what is shared may seem routine (proof of concept or exploit code, hashes, or machine configuration information), the incident may be unique and the information shared only once.

Structured information sharing

In an effort to improve the consistency, efficiency, and interoperability of information, initiatives to use standardized formats for information exchange are underway. The Incident Object Description Exchange Format[14] is an Internet Engineering Task Force standard that defines a structured representation of incident information. Similarly, the Structure Threat Information eXpression (STIX) seeks to standardize the format of incident, threat, vulnerability, mitigation, situational awareness, and strategic analysis information.

8 "The Public Regional Information Security Event Management (PRISEM) System." Office of the Chief Information Officer of Washington State. February 26, 2014. https://ocio.wa.gov/news/prisem

9 "Enhanced Cybersecurity Services." US Department of Homeland Security. September 8, 2014. www.dhs.gov/enhanced-cybersecurity-services

10 "Microsoft Interflow | Private Preview." Microsoft Security TechCenter. 2014. http://technet.microsoft.com/en-us/security/dn750892

11 Structure Threat Information eXpression. http://stix.mitre.org/

12 Trusted Automated eXchange of Indicator Information. https://taxii.mitre.org/

13 "Driving Excellence & Innovation in Security Response." Industry Consortium for Advancement of Security on the Internet. 2012. www.icasi.org

14 Incident Object Description Exchange Format. http://www.ietf.org/rfc/rfc5070.txt

Basis for information sharing

The scope of exchange can greatly influence the mechanisms of trust used, whether that scope includes small, regional groups of researchers holding regular meetings and calls to discuss threats and vulnerabilities or that scope involves high-level intelligence sharing between national governments.

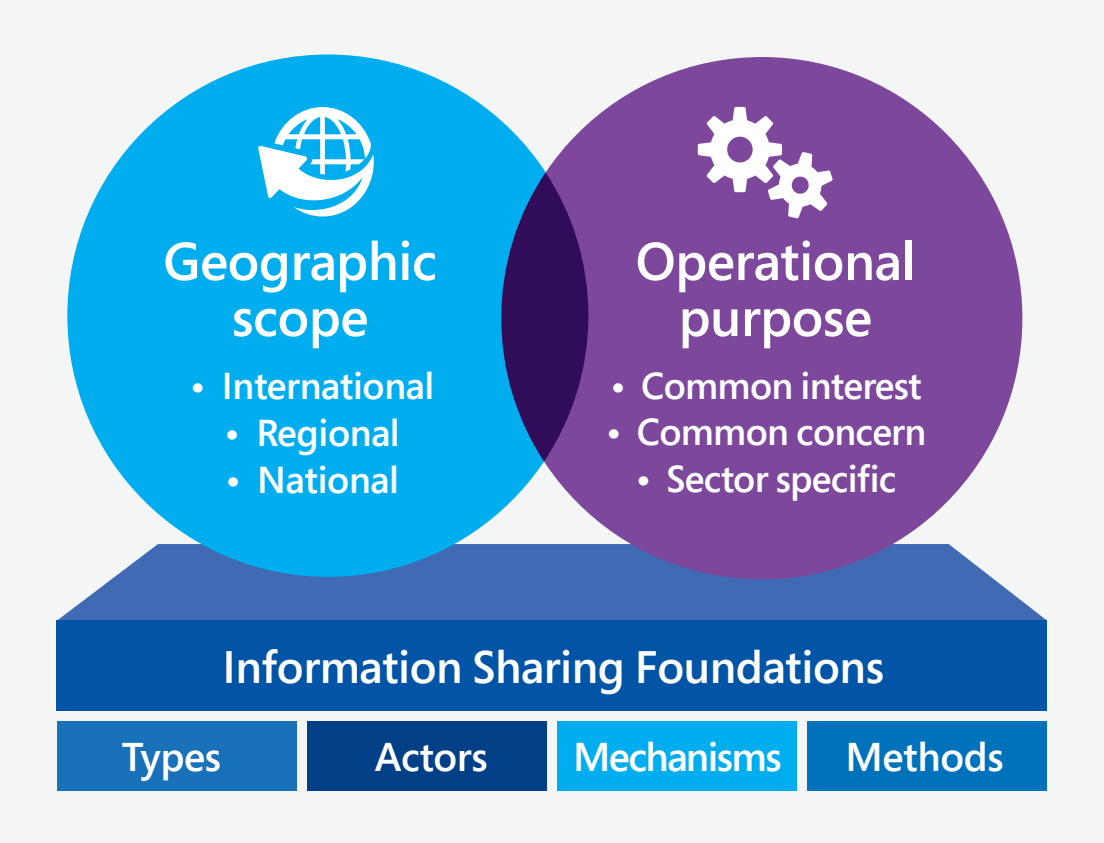


Figure 2. Information sharing foundations: Geographic scope and operational purpose

The right actors are critical to creating information exchange groupings. Information exchange is often composed of a community of individuals and organizations selected for their expertise, ability to effect change, and insight. In some instances, trust is the key gating factor. Two distinct factors limit or expand information exchange relationships: geographic scope and operational purpose.

Geographic scope

Regional. Some information exchange programs, especially in the private sector, operate through local companies, universities, and experts who discuss shared threats and vulnerabilities. In the United States, nonprofit programs, such as the Bay Area Chief Security Office Council[15] and the Massachusetts Advanced Cyber Security Center,[16] offer examples of regional exchange organizations. The US Federal Bureau of Investigation (FBI) has also developed InfraGard,[17] a regional public/private hub for sharing information. The local nature of such programs has the benefit of building trust through face-to-face meetings.

National. Numerous exchange programs at the national level, both voluntary and required, include and impact all of the major exchange actors. The inherent regulatory and security role of national governments indicates the need for national exchange programs. In the United States, most proposals from Congress and the executive branch have focused on national-level participation in new information exchange schemes.

International. Cyber-threats are often international in scope, so information exchange participants may want to share information across borders. For governments, such sharing can be problematic because passing sensitive or even classified information normally only takes place with close allies. As a result, efforts aimed at building international exchange programs that include governments have made little progress. For example, the European Public Private Partnership for Resilience (EP3R)[18] attempted to build a European Union-wide exchange program involving both government and private actors but has been slow in establishing an effective information exchange mechanism.

Operational purpose

Sector-specific. Certain information sharing schemes are sectorial in nature. Given the potential for threats to multiple providers within a single sector, sector-specific sharing has become a popular means of information exchange for critical infrastructure providers and, in particular, for government agencies. The ISACs and the Defense Industrial Base Cyber Pilot[19] are examples of information exchange relationships that are sector specific.

Common interest driven. Actors often group together to exchange information and best practices on a specific cybersecurity issue. Such relationships can be either ad hoc or institutionalized. For example, SAFECode[20] brings together a number of stakeholders to exchange best practices on developing secure software code and on creating better software assurance models. Similarly, ICASI brings together private participants to exchange information on procedures for responding to security incidents.

15 Bay Area Chief Security Office Council. http://www.bayareacouncil.org/issues-initiatives/cyber-security-policy-summary

16 Advanced Cyber Security Center. 2013. www.acscenter.org

17 InfraGard. https://www.infragard.org/

18 "European Public Private Partnership for Resilience (EP3R)." European Union Agency for Network and Information Security. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

19 "DOD Announces the Expansion of Defense Industrial Base (DIB) Voluntary Cybersecurity Information Sharing Activities." US Department of Defense. May 11, 2012. http://www.defense.gov/releases/release.aspx?releaseid=15266

20 SAFECode. www.safecode.org

Common concern driven. Sometimes groups form to share information about a common dependency on a type of technology. Good examples are the Centre for the Protection of National Infrastructure (CPNI)[21] in the United Kingdom and the Control Systems Information Exchange in Europe. These forums provide a trusted environment in which members can share information about control systems or critical operations risks.

In other cases, when vulnerabilities threaten a number of diverse actors, organizations may choose to solve the problem together in real time. The Conficker Working Group (referenced earlier) is often cited as an effective cybersecurity partnership. The German Anti-Botnet Advisory Centre similarly brought together government, Internet service providers, and antivirus vendors to tell people how to clean machines which have been enlisted in a botnet.

21 Centre for the Protection of National Infrastructure. www.cpni.gov.uk

Recommendations

Reducing cybersecurity risk increasingly depends on information sharing and collaboration among a wide range of actors, leveraging many different models, methods, and mechanisms. Establishing effective information sharing programs is a difficult undertaking. Successful information efforts require commitment, trust, cooperation, and a clear sense of value. The following recommendations build on the concepts explored in this paper to support and advance information sharing efforts for public and private organizations:

1. Develop an overarching strategy for information sharing and collaboration.

An information sharing strategy can help organizations to identify priorities, establish shared values, and set a course for building effective information sharing processes. A strategy can reduce confusion and increase support for information sharing efforts within an organization and among its partners.

2. Design with privacy protections in mind.

Information sharing efforts must respect privacy and civil liberties and should be designed with the aim of protecting these to the highest degree. Such efforts should include robust protections built into the exchange and must be based upon Fair Information Practice Principles or other internationally accepted privacy and civil liberties policies.

3. Establish a meaningful governance process.

Information sharing succeeds or fails based on trust and the value of the data shared among members. As a result, after the cybersecurity problem has been identified and declared as an incident, entities should establish clear goals for its resolution and should evaluate the actors, types of information, model, methods, and mechanisms of exchange that best support these goals. Ensuring that members follow the rules (and that rules are enforced) is essential to the credibility of the effort. A meaningful governance process should include appropriate management of the data shared, from its creation and release to its use and destruction (where necessary and appropriate).

4. Focus sharing on actionable threat, vulnerability, and mitigation information.

Shared threat, vulnerability, and mitigation information can create immediate improvements in cybersecurity and can help create better outcomes for ICT consumers in general. Sharing actionable information empowers actors to better defend networks and mitigate threats. Exchanging this type of data can help to build trust particularly in early stages of information sharing. Automated sharing mechanisms are increasingly used to rapidly share and act upon this information. Using machine readable formats to exchange threat and mitigation information can help automate defenses and reduce risk.

5. Spur voluntary information sharing by building interpersonal relationships.

Interpersonal relationships and trust between exchange program participants, along with trust in the program itself, are critical. Trusted relationships create an atmosphere with certain mutual expectations about behavior. Reciprocity can be a strong factor in driving cooperation in collective action problem scenarios. If members of an information exchange program expect that their counterparts, even those in direct competitive relationships, are acting in good faith, they are more likely to share information on threats and vulnerabilities.

6. Require mandatory information sharing only in limited circumstances.

Mandatory incident reporting is very different than voluntary information sharing. In some instances, such as in the case of national security and public safety, there may be a need for mandatory incident reporting. But such mandatory approaches should be narrowly defined and implemented through trusted mechanisms. This helps ensure that only the right information is shared with the appropriate stakeholders in the proper timeframe. Moreover, such a narrow approach strengthens privacy and the protection of civil liberties. Policy efforts should encourage information sharing processes, which are transparent about how such data is used and which ensure that information shared back to the submitters is valuable and timely.

7. Make full use of information shared, by conducting analyses on long-term trends.

A greater understanding of the root causes of cybersecurity incidents can help prevent future incidents and can foster improved security analyses. In many cases, a detailed analysis of the incidents can inform the selection and prioritization of cybersecurity risk mitigations for organizations. The exchange of this information could improve critical infrastructure operations and could help ICT vendors make products and services more resistant to abuse, compromise, or failures. Furthermore, such analyses can also help build knowledge of long-term trends, giving network defenders a better understanding of emerging cyber-threats and of shifts in exploitation methods.

8. Encourage the global sharing of best practices.

The exchange of best practices is an arena in which national governments can play a proactive role by engaging with other actors. One aspect of public/private information sharing that has been successful in many other areas of security and technological development is the creation and distribution of information on standards and best practices and of their effectiveness. Strong relationships built between governments and other actors on best practices represent good starting points for growing exchange relationships related to other cybersecurity information. Governments may also look to incentivize the acceptance of best practices, specifically by private critical infrastructures, since such information can build a stronger defensive posture.

Microsoft