International Standard

ISO/IEC 27035-4

First edition
2024-12

Information technology — Information security incident management —

Part 4: Coordination

Technologies de l'information — Gestion des incidents de sécurité de l'information —

Partie 4: Coordination

Reference number
ISO/IEC 27035-4:2024(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 27035 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Coordination is an important aspect in information security incident management. Incidents crossing organizational boundaries can occur and cannot be easily resolved by a single organization. Emerging threats are becoming increasingly sophisticated and can have a much larger impact than previously. The characteristics of emerging threats and attacks make it more urgent than ever to coordinate incidents across organizations.

Coordination can include relevant parties both within and outside the organization. For example, relevant parties within the organization include business managers and representatives from IT; external interested parties include incident response teams of external organizations and law enforcement organizations. See ISO/IEC 27035-2:2023, Clause 8 for a complete list. This document, however, only considers coordination between multiple organizations. This document provides guidelines for multiple organizations to work together to handle information security incidents. The coordination activities occur throughout the information security incident management process as defined in ISO/IEC 27035-1.

This document addresses the coordination of information security incident management between multiple organizations. Incidents sometimes involve technical vulnerabilities. Guidance on the coordination, disclosure, and handling of technical vulnerabilities is provided by ISO/IEC 29147 and ISO/IEC 30111. Additional information on the coordination of technical vulnerabilities between multiple organizations is provided by ISO/IEC TR 5895.

Information technology — Information security incident management —

Part 4: Coordination

1 Scope

This document provides guidelines for multiple organizations handling information security incidents in a coordinated manner. It also addresses the impacts of external cooperation on the internal incident management of an individual organization and provides guidelines for an individual organization to adapt to the coordination process. Furthermore, it provides guidelines for the coordination team, if it exists, to perform coordination activities supporting the cross-organization incident response.

The principles given in this document are generic and are intended to be applicable to multiple organizations to work together to handle information security incidents, regardless of their types, sizes or nature. Organizations can adjust the guidance given in this document according to their type, sizes and nature of business in relation to the information security risk situation. This document is also applicable to an individual organization that participates in partner relationships.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27035-1, *Information technology — Information security incident management — Part 1: Principles and process*

ISO/IEC 27035-2, *Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*

ISO/IEC 27035-3, *Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27035-1, ISO/IEC 27035-2, ISO/IEC 27035-3 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
incident response team
IRT
team of appropriately skilled and trusted members of an organization that responds to and resolves incidents in a coordinated way

Note 1 to entry: There can be several IRTs, one for each aspect of the incident.

Note 2 to entry: Computer Emergency Response Team (CERT[1)]) and Computer Security Incident Response Team (CSIRT) are specific examples of IRTs in organizations and sectorial, regional, and national entities wanting to coordinate their response to large scale ICT and cybersecurity incidents.

[SOURCE: ISO/IEC 27035-1:2023, 3.1.2]

3.2
coordinated incident management
CIM
process for IRTs from multiple organizations to work together to handle information security incidents

3.3
community
group of associated organizations, individuals and groups sharing common interests

Note 1 to entry: Impacted communities are the groups of people and associated organizations affected by the provision of security services, projects or operations.

[SOURCE: ISO 22300:2021, 3.1.39]

4 Overview

4.1 General

Coordination is an important aspect in information security incident management. As stated in ISO/IEC 27035-1, coordination can occur throughout the information security incident management process, and the responsible roles for coordination should be taken by the incident management team (IMT) and the incident coordinator. Coordination can include both internal and external parties (see a full list of these parties in ISO/IEC 27035-2:2023, Clause 8). Among different parties, there are different degrees of coordination relationships. Some coordination relationships are loose, only involving information disclosure, such as the contacts with internal representatives from the legal department, public relations, or external parties like law enforcement and media. Other coordination relationships are dense, targeting incident response, which involves working with multiple internal incident response teams, or the incident response teams from external organizations and internet service providers (ISPs). See Annex A for examples of information security incident management coordination. ISO/IEC 27035-1, ISO/IEC 27035-2 and ISO/IEC 27035-3 focus on guidelines for information security incident management within a single organization, and internal and external coordination activities are only briefly covered. This document gives further detail on coordination between multiple organizations, and can benefit different organizations to achieve a structured and effective cross-organization incident response. Figure 1 illustrates the scope of this document.

1) CERT is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of this product.

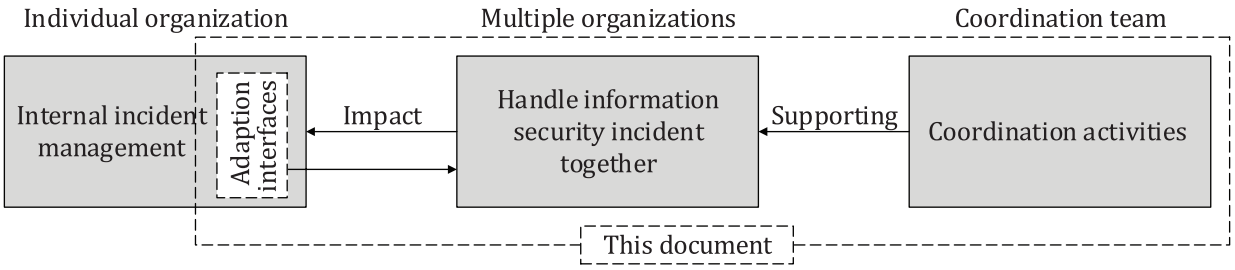

Figure 1 — Illustration of the scope of this document

It is more possible to achieve good coordination between multiple organizations, when organizations use incident management process (see ISO 22320). Based on the incident management process defined in ISO/IEC 27035-1, the coordinated incident management process can be illustrated as in Figure 2. The guidelines on the coordinated incident management process and its key activities are generic, which allows flexibility so that coordination can be applied to incident management partially or entirely as needed (e.g. the loose coordination case which only involves information disclosure is also applicable).

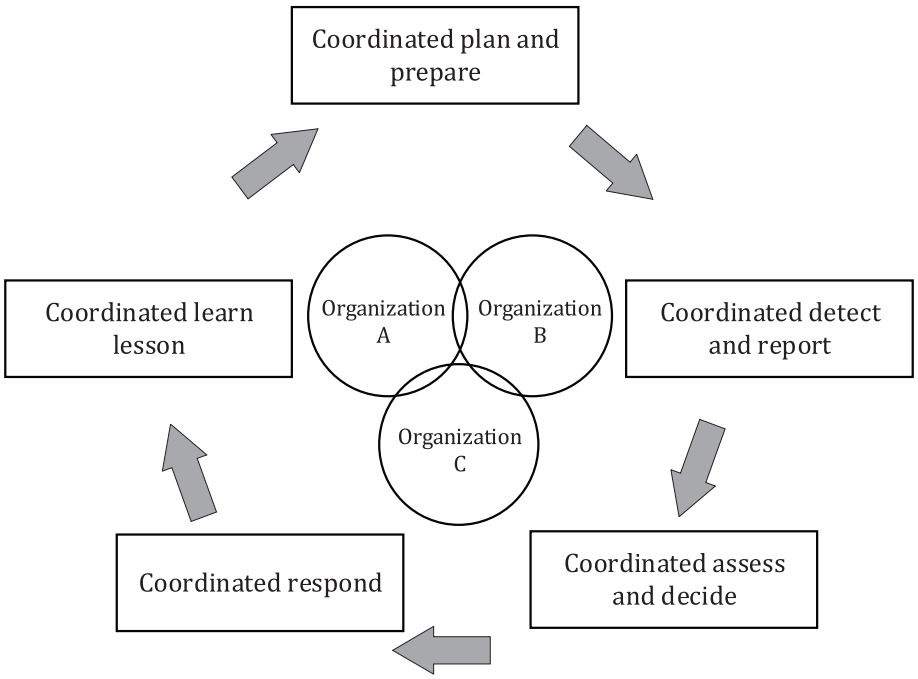

Figure 2 — Illustration of coordinated incident management process for multiple organizations

4.2 Coordination team

The coordination team is a special type of incident response team. They usually work as independent entities which focus on the incident management coordination. The coordination team has the following features.

a) The coordination teams focus on activities including information exchanging, information sharing and response coordination. It is possible that the coordination team does not implement incident response activities directly. They facilitate efficient incident management coordination and cooperation among multiple members. By fully dispatching the resources of each member, they help to realize information sharing between members and throughout the entire community.

b) The coordination team should have a defined service constituency. The constituency is usually based on a geographic location or a business domain. Typical examples of coordination teams based on geographical regions are national incident response teams and regional incident response teams in international regions or within a country. The main reason for setting up a coordination team based on

industry sectors is that organizations in the same industry face similar cybersecurity risks. Thus, the appeal and value of information sharing and response coordination is greater.

c) The coordination team acts as a central point in the incident management coordination. Multiple coordination teams can be arranged in a peer mode or a hierarchical mode. The coordination team and the members can be regarded as forming a community, whereby the coordination team acts as a central point when coordination is needed between multiple members. If the impact of the incident exceeds the coordination team's constituency or capability, the coordination team should contact another relevant coordination team or relevant community member for assistance.

4.3 Principles of coordination

4.3.1 Timeliness principle

Information security incidents are highly time-sensitive. Any threat information and incident status has a certain validity period. Therefore, all parties should agree on the time requirements of each item before performing incident management coordination and observe the agreed time in the coordinated incident management process.

4.3.2 Roles and responsibilities principle

Clear roles and responsibilities should be defined for incident management coordination activities. When working under a coordination model with multiple organizations involved, it is important for all parties to know the role that they play and what their respective responsibilities are under the model. In this manner, all parties know what is expected of them to enable cohesion and minimise confusion. In addition, where the lead coordinator role changes (e.g. depending on the content and context of the specific incident), criteria should also be established to determine who leads coordination for that incident.

4.3.3 Common understanding principle

Communicating and coordinating incident response information can be difficult unless the organizations involved utilize shared vocabulary. Organizations should use a common language and terminology to support the exchange of information and facilitate understanding. Also, by adopting a common taxonomy to classify information and standardizing data exchange format, organizations can have common understanding of the security information shared by others. A common understanding can help organizations to reach consensus and ensure their goals are consistent in the incident management coordination.

4.3.4 Confidentiality principle

During the incident management coordination, it is possible for organizations involved to carry out information communication or exchange. Organizations should be careful to protect secret business information and personal sensitive information when transmitting information to external parties. They should consult their legal department to formulate confidentiality rules for information exchange.

5 Coordinated incident management process

5.1 Overview

As illustrated in Figure 2, the coordinated incident management process has the same phases as the incident management process as defined in ISO/IEC 27035-1, namely:

— coordinated plan and prepare (see 5.2);

— coordinated detect and report (see 5.3);

— coordinated assess and decide (see 5.4);

— coordinated respond (see 5.5);

— coordinated learn lessons (see 5.6).

Figure 3 shows an overview of the activities in the coordinated incident management process, covering:

— coordinated activities for multiple organizations to complete together;

— the impacts on the internal activities of an individual organization and the adaption to make;

— if a coordination team exists, the coordination activities it performs.

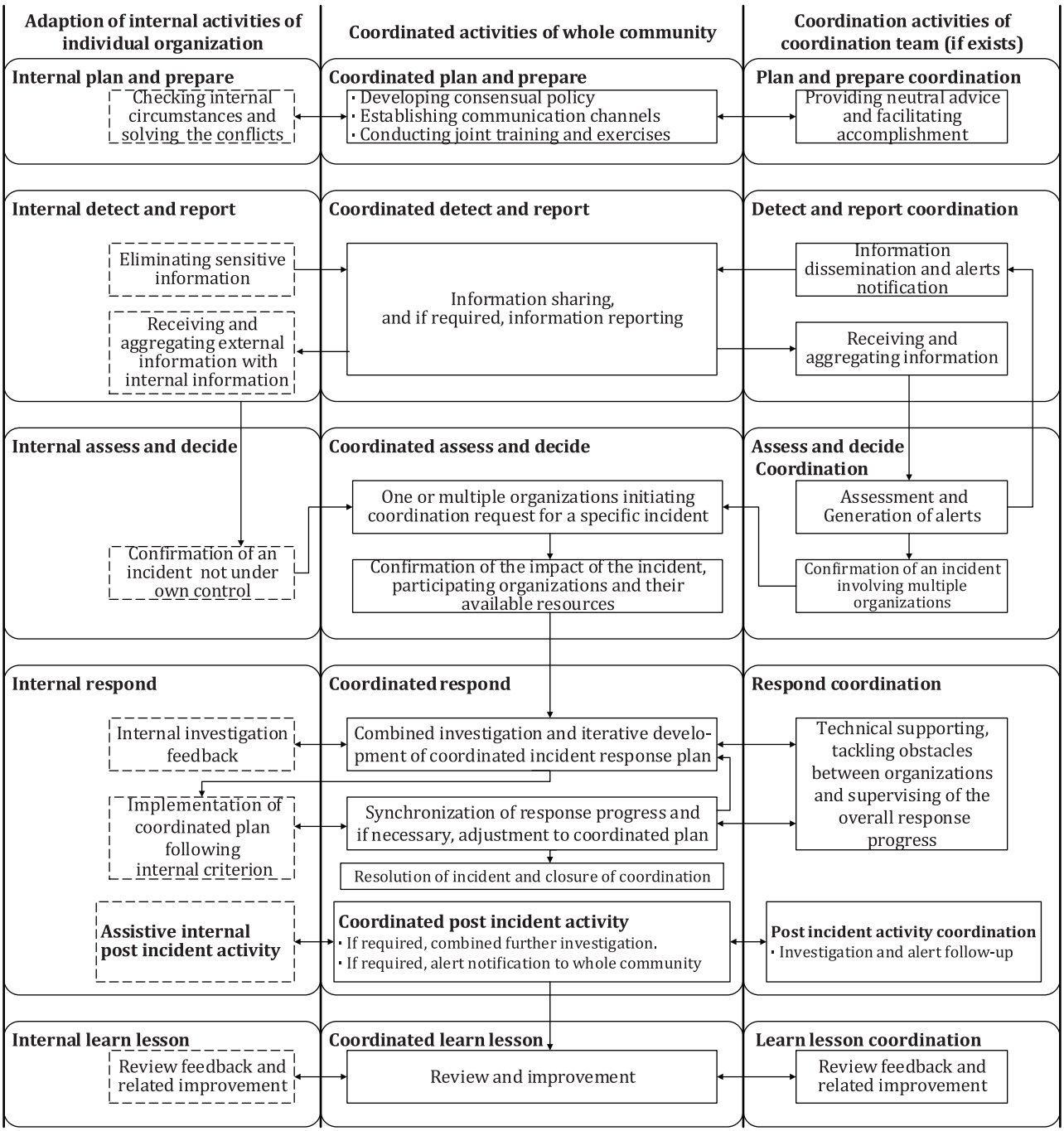

Figure 3 — Overview of coordinated incident management process

5.2 Coordinated plan and prepare

In the coordinated plan and prepare phase, organizations in the community reach an agreement on coordination policies and public framework, establish communication channels, and conduct training and

collaborative exercises to enhance incident response capability and mutual trust. Every organization should appoint an incident coordinator responsible for the incident management coordination of the community, and make sure that the organization's incident management team (IMT) consents authority to the incident coordinator and all planning and preparation activities.

The coordinated plan and prepare activities include, but are not limited to:

a) reach an agreement on coordination policies (see ISO 22397), including but not limited:

   — memoranda of understandings (MOUs), or non-disclosure agreements (NDAs);

   — the purpose, scope and resources of coordination;

   — information sharing rules, and requirements of removing sensitive information;

   — event tracking and coordination processes.

b) establish communication channels, including temporary channels, such as telephone, email, meeting, as well as regular channels. Periodical meeting of incident coordinators from organizations in the community, either offline or online, is a good way to improve understanding and build mutual trust. Data exchange format and transmission mechanisms for information sharing should be determined to make the information exchange process as secure and automated as possible;

c) conduct training and exercises on coordination in the community.

The adaption of an individual organization's internal activity includes:

d) appointing an incident coordinator responsible for the incident management coordination of the community, and making sure that the organization's incident management team (IMT) consents authority to the incident coordinator and all planning and preparation activities;

e) establishing organizational information sharing, disclosure, and incident management coordination policies;

f) establishing and preserving appropriate relationships and connections with the community;

g) checking internal circumstances and solving conflicts.

The coordination team performs the following activities to achieve coordination:

h) providing neutral advice and facilitating accomplishment.

5.3 Coordinated detect and report

During the coordinated detect and report phase, the community encourages all members to actively share threat intelligence. It establishes a threat information exchange mechanism and takes technical measures to ensure the security of information transfer channels. Organizations of the community analyse the collected information to make further assessment and decision-making.

Threat information exchange is based on trust. The following elements can be considered:

a) exchanging threat information should have the ability to support members' anonymity;

b) taking effective measures to protect the security of information related to reported vulnerabilities and incidents and to prevent information leakage;

c) attempting to automate as much of the information sharing process as possible;

d) ensuring that threat information sharing mechanisms have the ability to support broad participation. In addition to structured threat information expression and automatic exchange, these mechanisms should also allow information in any format, such as email and verbal.

The adaption of an individual organization's internal activity includes:

e) according to the pre-established shared information approval process, sharing threat intelligence as quickly as possible; it is most valuable when the threat intelligence is shared quickly;

f) performing data sanitization or scrubbing to remove sensitive pieces of data from the incident information without disturbing the information on precursors, indicators, and other technical information;

g) analysing the captured internal incident threats and external threat intelligence shared by the community to identify suspicious incidents. Automated measures should be applied in threat information collection, processing, and use;

h) ensuring that the necessary measures are taken to protect information shared with the team by other organizations;

i) ensuring all the shared information is managed by the responsible incident coordinator for the community, and that the incident coordinator coordinates with other internal incident coordinators to enhance overall information security situation awareness.

The coordination team performs the following activities to achieve coordination:

j) receiving and aggregate information. Automated measures should be applied in threat information collection, processing, and use;

k) performing information dissemination and alerts notification.

5.4 Coordinated assessment and decision

For the coordinated assess and decide phase, organizations in the community should work together to assess the impact of a specific incident and decide on the initiation of coordination.

The coordinated assessment and decision activities include, but are not limited to:

a) initiate the coordination request for a specific incident. In the community, there are three possible cases of initiating coordination requests:

   — One organization becomes aware of a possible incident and finds that the incident cannot be under its own control, so the coordination request is initiated by the organization's responsible incident coordinator for the community;

   — The coordination team becomes aware of a possible incident from reporting or information sharing within the community. The coordination team discovers that the incident involves multiple organizations and initiates the coordination request;

   — Multiple organizations initiate the coordination requests almost at the same time and after assessing the similarity and correlation, multiple requests merge into a single one.

b) assess whether an incident occurred or not, and decide to start the coordination for the incident in the community;

c) assess the impact of the incident and the involved organizations who should participate;

d) assess the available resources that can be provided by the participating organizations;

e) ensure that the incident coordinators of all participating organizations are involved in the assessment and decision process. The incident coordinators should gather internal related data and obtain necessary authority from their organizations.

The adaption of an individual organization's internal activity includes:

f) when aware of an incident not under its own control, the organization should identify the relevant community and distribute incident information to the responsible incident coordinator of the community;

g) the responsible incident coordinator identifies whether a coordination request is needed to initiate the coordination process, or whether a coordination process for the incident already exists in the community, and accordingly notifies the relevant incident response teams to prepare.

The coordination team performs the following activities to achieve coordination:

h) conducts an overall assessment of reporting or information sharing of the community, and analysis and relevance of the information from multiple sources;

i) discovers any abnormalities and assesses the impact;

j) generates timely alerts to the whole community, and when necessary, makes a decision to start response coordination.

5.5 Coordinated respond

For the coordinated respond phase, only the organizations involved by the incident should participate. All participating organizations work together to determine the coordinated incident response plan, then implement their parts accordingly back in their organizations. The incident coordinators of participating organizations are key roles to coordinate both the internal and external response activities.

The coordinated response activities include, but are not limited to:

a) identify which organization will lead the response activities, it is recommended to let the coordination team lead, if it exists. Also identify the associated roles and responsibilities of all parties involved in the incident response.

b) conduct a combined investigation of the incident. The incident coordinators of participating organizations coordinate internal IRTs to conduct an internal investigation, sharing necessary information and participating in a combined investigation of the incident;

c) develop the coordinated incident response plan together. The internal incident response teams of participating organizations develop the coordinated incident response plan, under the coordination of their organizations' incident coordinators. The developing progress is iterative, every organization should provide timely feedback on applicability and validity. The coordinated incident response plan should determine the activities for every participating organization to perform, and the arrangement can be described by a matrix (see Table 1 for an example). The steps to create a matrix are:

   — identifying response activities required to respond to the incident and assigning the response activities to the top row;

   — assigning the participating organizations to the left column;

   — linking each response activity with the participating organizations.

Table 1 — Example of matrix

	Activity 1	Activity 2	Activity 3	……	Activity N
Organization A	X				
Organization B	X	X	X		X
Organization C	X		X		X
……					
Organization M	X		X		X

d) implement the coordinated incident response plan to achieve the containment, eradication and recovery of the incident. The IRTs of participating organizations take response actions within their organization. Each participating organization should follow its internal criteria and meet the requirements of its part according to the coordinated incident response plan. The incident coordinators of participating organizations supervise internal response progress of their organization to together evaluate overall expectations, and make adjustments to the coordinated incident response plan when necessary;

e) review and confirm the resolution of the incident. The incident coordinators of participating organizations lead the internal review of the response activities and together complete the joint incident report. The incident coordinators should submit the joint incident report to the incident management teams (IMTs).

f) after resolution of the incident, participating organizations should follow a closure process of the coordination relationships and consider whether a coordinated post incident activity is required, including:

   — combined further investigation;

   — alert notification to the whole community.

The adaption of an individual organization's internal activity includes:

g) participate actively in the development of the coordinated incident response plan. The internal IRTs should conduct an internal investigation, verify the applicability and validity of the plan under development, and share necessary information for the development of the coordinated incident response plan;

h) take response actions required by the coordinated incident response plan. The internal IRTs should follow the internal criteria of their organization and report the internal response progress to the incident coordinator to coordinate with overall expectations;

i) perform the internal review of the response activities to draft a joint incident report and provide the required assistance to the coordinated post-incident activity, after the incident has been resolved.

The coordination team performs the following activities to achieve coordination:

j) provide technical support and tackle the obstacles between multiple organizations during the development and implementation of the coordinated incident response plan;

k) supervise the overall response progress and coordinate for unexpected problems;

l) after resolution of the incident, play a key role in the required post incident activity, e.g. lead the combined further investigation, release the alert notification to the whole community and follow up.

5.6 Coordinated learn lessons

In the coordinated learn lesson phase, a single organization or multiple organizations in the community jointly evaluate the incident response process, especially the coordination process. Organizations review the process, identify and document lessons learned from the coordination, and improve the information security incident response and coordination process in a continuous iteration. The activities in this phase are mainly carried out and coordinated by the incident coordinators of the relevant organizations, including:

a) reviewing, identifying, and improving the implementation of information security controls (new or updated controls), and incident management coordination process;

b) reviewing the effectiveness of existing policies, rules, processes and tools throughout the information security incident response and coordination process, and making appropriate adjustments;

c) performing comprehensive evaluation of the performance and effectiveness of the participating organizations;

d) communicating and sharing the results of review within a trusted community (if so desired);

e) deciding whether and to what extent the incident information, related attack vectors and vulnerabilities can be shared with partner organizations or communities, to assist in preventing the same event from recurring in their environment.

6 Guidelines for key activities of coordinated incident management

6.1 Developing coordination policies

Coordination policies are the foundation for organizations in the community to perform incident management coordination. The coordination policies should provide the common vision, principles, procedures, as well as financial support for organizations to handle information security incidents together. The coordination policies can generally include contractual aspects, operational aspects, financial aspects and ethical aspects.

a) Policies in contractual aspects can include:

   1) rules for joining and leaving the community, also multiple grades of membership can be adopted;

   2) non-disclosure agreements (NDAs) outlining confidential material, knowledge, or information that can be shared within a certain range but require restricted access. The community can choose different levels of NDAs according to the actual needs, e.g. NDAs with strict policies can help to build trust, while NDAs with moderate policies can increase participation.

b) Policies in operational aspects can include:

   1) the benefits and responsibilities of members. Generally, if the responsibilities are clearly described to members in the community, they are more likely to be more active, and therefore get better benefits. While basic responsibilities can result in loose connections and less benefits;

   2) the requirements and responsibilities of the members' personnel. Each organization should appoint an incident coordinator responsible for the incident management coordination of the community;

   3) the coordination process, specifying a set of conditions that require coordination, timing requirements in coordination activities and operational mechanisms to organize multi-party response activities;

   4) training and exercises programmes;

   5) media policies complying with information disclosure policies.

c) Policies in financial aspects can include:

   1) whether a fee is needed for membership, and whether multiple grades of membership can involve fee differences;

   2) funding policies for member organizations to hold events such as meetings and trainings, or for an individual to attend events.

d) Policies in ethical aspects can include:

   1) a code of conduct describing expected behaviour for anyone involved. This code of conduct covers various kinds of activities, both online and offline, organized by the community, including coordination communication, meetings, trainings, and special events. A code of conduct can help to create inclusive, open, collaborative and enjoyable environments.

When applying these policies, the community should follow some principles including: considering compliance with applicable legislation, being fair to all members and ensuring transparency by providing timely information. The coordination team, if it exists, can be a central point in sustaining the operation of the community and the implementation of policies. Otherwise, members can hold a secretariat to undertake the function, for example, a secretariat consisting of the incident coordinators of partial organizations.

6.2 Establishing communications

It is important for the community to establish and maintain communication between members. Members are encouraged to begin using communication as early as the initial assessment when trying to understand what is happening or what has happened. The community should ensure the communication is timely, open and accurate. Multiple (separate and different) communication mechanisms should be established in case of the failure of one mechanism. The communication mechanisms can generally be divided into two categories: ad hoc mechanisms and partially automated mechanisms.

a) Ad hoc mechanisms include email, instant messaging clients and the phone. Traditionally, the communication has occurred through ad hoc mechanisms. The ad hoc communication mechanisms may rely more on an employees' connections with peers of partner organizations. The employees use ad hoc channels to manually communicate with peers for sharing information and coordinating incident response activities. These ad hoc mechanisms can be the most cost-effective way of sharing information with partner organizations. However, due to the non-robust nature of ad hoc mechanisms, it is possible to fail easily, for example, due to an experienced employee's resignation. Thus, it is recommended for the organizations to have two or more employees as backup. For the incident coordinators or other important roles, it is better to have multiple communication mechanisms. Periodical meeting of incident coordinators, either offline or online, is a good way to improve understanding and build mutual trust. In addition, ad hoc mechanisms tend to require more manual intervention and are more resource-intensive to process than the partially automated mechanisms, since the information exchanged in ad hoc communication channels can lack standardization.

b) Partially automated mechanisms are desired to make the inter-organizational communication efficient. Organizations should attempt to automate as much of the communication process as possible. In reality, it is not possible to fully automate the communication process, nor is it desirable due to security and trust considerations. Organizations should aim to achieve a balance of automated process overlaid with human-centric processes. According to the community's needs, the partially automated communication solutions can support several aspects:

    1) Information sharing: The inter-organizational communication is mainly used to share information. To automate information sharing, the community should choose the data exchange model and enabling technical transport mechanisms. The members in the community should agree on the data exchange models to ensure that the models are compatible with their incident response systems. It is recommended to select existing standards for data exchange models when the members need to represent the information. Then, members in the community should agree on the technical transport mechanisms for enabling the information exchange to occur in an automated fashion. The transport mechanisms include the transport protocol for exchanging the information, the architectural model for communicating with an information resource, and the applicable ports and domain names for accessing an information resource.

    2) Managing contact relationships: An organization should maintain various contact channels with peers in the community. It is an efficient way to use technical methods to automate the management of the contact relationships.

    3) Utilizing integrated communication: It is possible to integrate multimedia communication facilities and personal communication devices as partially automated communication channels. Examples include video conference systems for convenient communication during incident management coordination, enabling short or instant messages which can be automatically pushed to the responsible employee when important alerts are received.

Organizations should protect sensitive information when communicating with external parties. For security consideration in inter-organisational communication, see ISO/IEC 27010 for details.

6.3 Threat and event Information sharing

6.3.1 Overview

Information sharing is the activity in which security information is exchanged and shared among different organizations, industries or sectors based on the standardization and normalization of security information,

and the technology and transmission technique of the information system. The security information in this document includes threat information and defence measures including risk information and event information used to describe the intentions, methods, tools, procedures and results of the behaviours that may threaten the normal operation of the network; information which may expose network vulnerabilities; behaviours, equipment, programs, signatures, techniques or other measures to detect, prevent or mitigate known or possible threats or security vulnerabilities.

Information sharing is an important aspect in the incident management coordination. Organizations should perform information sharing throughout the coordinated incident management process. In the coordinated plan and prepare phase, organizations should first establish information sharing relationships. In the coordinated detect and report phase, the coordinated assess and decide phase and the coordinated respond phase, organizations are encouraged to actively participate in sharing relationships. In the coordinated learn lessons phase, organizations should evaluate all the information sharing activities and make necessary improvements. 6.3.2, 6.3.3 and 6.3.4 give guidelines for information sharing, including information types, establishing and participating in information sharing relationships.

6.3.2 Information types

The security information shared throughout the coordinated incident management process can be divided to several types. Some of the main types are listed in Table 2.

Table 2 — Example of information types

Information type	Description
Indicators (also referred to as indicators of compromise(IOC))	Technical artefacts or observations that suggest an attack is imminent or is currently underway or that a compromise has already occurred. Indicators can be used to detect and defend against potential threats. Examples of indicators include the IP address of a suspected command and control server, a suspicious domain name, a URL that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message.
Tactics, techniques, and procedures (TTPs)	Description of the behaviour of an actor. Tactics are high-level descriptions of behaviour, techniques are detailed descriptions of behaviour in the context of a tactic, and procedures are even lower-level, highly detailed descriptions in the context of a technique. TTPs can describe an actor's tendency to use a specific malware variant, order of operation, attack tool, delivery mechanism (e.g. phishing or watering hole attack), or exploit.
Security alerts	Brief, usually human-readable technical notifications regarding current vulnerabilities, exploits, and other security issues. These alerts are also known as advisories, bulletins, and vulnerability notes.
Threat intelligence reports	Prose documents that describe TTPs, actors, types of systems and information being targeted, and other threat-related information that provides greater situational awareness to an organization. Threat intelligence is threat information that has been aggregated, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.
Tool configurations	Recommendations for setting up and using tools (mechanisms) that support the automated collections, exchange, processing, analysis, and use of threat information. For example, tool configuration information can consist of instructions on how to install and use a rootkit detection and removal utility, or how to create and customize intrusion detection signatures, router access control lists (ACLs), firewall rules, or web filter configuration files.

6.3.3 Establishing information sharing relationships

To establish information sharing relationships, organizations should accomplish the following activities.

a) Define the scope and mode of information sharing activities: the organizations can choose one of the following modes of information sharing:

   — Joining an existing sharing community. There are many sharing communities that have been organized on the basis of geographic region, political boundary, industrial sector, business interest, or threat space. Many of these sharing communities have multinational constituencies and global reach.

   — Establishing a new sharing community. If the organizations have adequate capabilities and resources, it is also beneficial for them to establish their own new sharing community, which enables them to establish information sharing rules more focused on their objectives and benefits.

   — adopting a mix mode of the above two modes. The organizations can also adopt a mix mode. On the one hand, the mix mode can take advantage of the knowledge of existing sharing communities by defining clear interfaces and selecting interested information. On the other hand, the mix mode can take advantage of more suitable information sharing rules as an independent sharing community.

   For the scope of the information sharing activities, the sharing community can be divided into multiple membership levels. For example, for higher membership levels, the qualified member should be more reliable, capable, and constrained by stronger confidential rules, and in some commercial communities, members can be required to pay higher membership fees.

b) Define the objectives of information sharing: the organizations should identify the objectives that describe the desired outcomes of information sharing, taking into account the following aspects:

   — the common vision and benefit shared by the organizations;

   — technological and resource constraints;

   — the priority if there are multiple items in objectives;

   — existing external policies that can have impacts.

c) Establish information sharing rules: whether joining an existing sharing community, or establishing a new sharing community, information sharing rules should be established to facilitate the publication and distribution of the security information. These rules help to control the dissemination of the security information, and prevent adverse consequences that can be caused by improper disclosure of the security information. The information sharing rules should include:

   — listing the types of security information that can be shared;

   — describing the conditions and circumstances when sharing is permitted;

   — identifying approved recipients of the security information.

   — describing any requirements for redacting or sanitizing information to be shared;

   — specifying if source attribution is permitted;

   — applying information handling designations that describe recipient obligations for protecting information.

   Sharing rules can be specified in a variety of ways including: Memoranda of Understanding (MOUs), Non-Disclosure Agreements (NDAs), Framework Agreements, or other agreements.

d) Plan to provide ongoing support for information-sharing activities: to guarantee the information-sharing activities can be continuously performed, the sharing community can require the members to

have support plans for information sharing activities. The plan should identify the personnel, funding infrastructure, and processes for:

— collecting and analysing the information from both internal and external sources;

— acquiring and deploying protective measures;

— acquiring and deploying monitoring and threat detection infrastructure.

6.3.4 Participating information sharing relationships

To keep participation in information sharing activities, the members in the information sharing community will typically perform some or all of the following activities:

a) Engage in ongoing communication: the information sharing communities can use a variety of communications methods to share threat information with their members:

— receiving security information via email lists, text alerts, and web portals without infrastructure investment specific to information sharing. The content received through these delivery channels can require manual processing in such cases;

— using schemed data feeds to apply automated collection, processing, and use of security information. Examples of data schemas include STIX (XML, JSON), Incident Object Description and Exchange Format (IODEF, RFC 5070 and possibly RFC 6545), VERIS Framework, Facebook Threat Exchange (JSON), CRITs Data Model (JSON);

— other information sharing methods, such as conferences and workshops;

The organizations participating in information sharing need dedicated staff for communications, since the content received through various communication channels can require manual processing, or travel can be required to attend conferences, workshops and training events. Less mature organizations and inexperienced employees can gain knowledge enrichment and practical insights from skilled practitioners through the training events.

b) Publish and respond to security alerts: the information sharing community can publish security alerts notifying members of emerging vulnerabilities (see ISO/IEC 29147), exploits, and other security issues. The security alerts commonly include the following fields:

— brief overview/executive summary and detailed description, which would include indicators;

— platforms affected (e.g. operating system, application, hardware);

— estimated impact (e.g. financial loss, individual's personal safety, dignity, finances, liberty or identity, non-compliance with legislation, commercial confidentiality and legal privilege, reputation, confidence and service delivery);

— severity rating;

— mitigation options, including permanent fixes and/or temporary workarounds;

— references for more information;

— alert metadata (e.g. alert creation and modification dates, acknowledgements).

Upon receipt of a security alert, the organizations should first double-check if the alert is credible and from a trusted, reliable source. Then if the alert applies to systems, applications, or hardware that the organizations own or operate, organizations should properly respond. The actions include:

— characterizing the overall impacts of the alert by assessing factors such as the severity of the alert, the number of affected systems within the organization, the effects an attack can have on the organization's mission-critical functions, and any operational impacts related to the deployment of mitigating security controls;

— identifying and extracting indicators from an alert;

— using indicators to develop and deploy detection signatures;

— making configuration changes;

— applying patches;

— notifying personnel of threats;

— implementing or enhancing security controls.

c) Consume and use indicators: organizations should carefully consider the characteristics of indicators that it receives and should take a risk-based approach to determining how indicators can be most effectively used. The consumption and use of indicators from external feeds commonly include some or all the following activities:

— validation: validate the integrity of indicator content and provenance through digital signatures, cryptographic hashes, or other means;

— decryption: transforming encrypted indicator files or data streams back to their original format;

— decompression: unpacking compressed indicator files, archive (e.g. zip, tar), or data streams;

— prioritization: processing indicators based on relative importance, the perceived value of a data source, the overall confidence in the data, any operational requirements that specify that data sources be processed in a particular order, the amount of effort required to transform the data into actionable information, or other factors;

— categorization: reviewing indicator metadata to determine its security designation and handling requirements. Sensitive information can require encrypted storage, more stringent access control, or limitations on distribution.

Organizations may use externally and internally-generated indicators to achieve the following improvements:

— adding or modifying rules or signatures used by firewalls, intrusion detection system, data loss prevention systems, and/or other security controls to block or alert on activity matching the indicators;

— configuring security information and event management solutions or other log management-related systems to help with analysis of security log data;

— scanning security logs, systems, or other sources of information, using indicators as search keys, to identify systems that have possibly already been compromised;

— finding matching records when investigating an incident or potential incident to learn more about a threat, and to help speed up incident response and recovery actions;

— providing additional information to security operations centre analysts;

— educating staff on threat characteristics; and

— identifying threat trends that can suggest changes to security controls are needed.

d) Organize and store cyber threat information: depending on how indicators are being used, organizations should organize indicators in a knowledgebase. Free-form methods such as wikis can be quite flexible and suitable for developing working notes and indicator metadata. Structured databases are also useful for storing, organizing, tracking, querying, and analysing collections of indicators. Information commonly recorded in a knowledgebase includes the following, when known:

— source of an indicator;

— rules governing the use or sharing of an indicator;

— date or time an indicator was collected;

— length of time that an indicator is still considered valid;

— whether or not attacks associated with an indicator have targeted specific organizations or sectors;

— groups or actors associated with an indicator;

— aliases of any associated actors;

— TTPs commonly used by an actor;

— motives or intent of an associated actor;

— individuals or types of individuals targeted in associated attacks; and

— systems targeted in attacks.

e) Produce and publish indicators: many organizations in the information sharing community only consume indicators, however, some organizations with more advanced security capabilities can produce and publish their own indicators. A producer of shared security information should handle the following issues:

— deciding what information should be shared. Indicators that are produced and published should include metadata that provides context for each indicator, describes how the indicator should be used and interpreted, and how the indicator relates to other indicators.

— deciding what data formats should be used. The use of standard data formats for exchange of indicators enhances interoperability and allows information to be exchanged with greater speed. Unstructured formats (e.g. text documents, email) are suitable for high-level threat reports and ad hoc exchanges of indicator information and other materials intended to be read by security personnel rather than machines. For time-critical exchanges of indicators however, such as automatically configuring a firewall to block specified communications, the use of standard data formats is encouraged because such formats reduce the need for human assistance.

— deciding how sensitive data should be handled. The indicators that an organization publishes can be sensitive, so proper safeguards should be used to prevent unauthorized disclosure or modification. Indicator data can be protected using a variety of methods, including encrypted network communications, authentication and authorization mechanisms, and storage in hardened repository. If a repository is used, an organization should have a written SLA for the repository that specifies expected availability, security posture requirements, and acceptable use policies.

6.4 Conducting coordinated exercises

To enhance the readiness of the community for incident management coordination, it is important to conduct coordinated exercises. However, there are additional difficulties involved in conducting coordinated exercises, compared to the single organization exercises. These potential difficulties include:

a) the threats confronted by the community can require complex exercise scenarios and emerging threats can bring new challenges;

b) member organizations can be located far from each other, which brings difficulty to face to face exercises;

c) culture differences can bring obstacles to communication and understanding between member organizations.

To address the above challenges of the coordinated coordination exercises, the community should consider the following:

d) besides ordinary exercises, the community can conduct experimental exercises for emerging threats or complex scenarios that have not been addressed;

e) the community can attempt to enable as many online activities for exercises as possible, in all types of exercises including discussion-based, table-top and live exercises, while also be aware that face-to-face activities are still important to improve understanding and build trust;

f) the community can set up the cyber range to support exercises. It is a more effective way for the member organizations to construct the cyber range together by sharing affordable resources, because it is not easy for most organizations to have their own cyber range.

Overall, the coordinated exercise can follow three steps:

g) Prepare for the coordinated exercise, including:

   1) Define the goal of the coordinated exercise. An exercise can have more than one goal, including:

      — testing the existing coordination process;

      — training the personnel of the member organizations;

      — strengthening understanding of multiple members;

      — examining the capabilities and competencies of members;

      — studying and exercising for emerging threats or complex scenarios that have not been addressed.

   2) Prepare the documentation for the coordinated exercise. According to the goal and scenarios of the coordinated exercises, the incident coordinators coordinate relevant IMTs and IRTs to participate. Many essential documents are needed, for example: briefing documents for exercise scenarios, event driven scripts and exercise report templates.

h) Conduct the coordinated exercise. It is just as important to have online coordinated exercises as face-to-face coordinated exercises. To conduct online coordinated exercises, it is particularly important for the community to apply enabling techniques to keep pace of every participant's action, and scatter exercise data collecting.

i) Evaluate the coordinated exercise. The evaluation criteria should be developed before the exercise. According to the evaluation criteria, the observations made during the exercise are the basis of the evaluation. The coordinated exercise report should include background information about the exercise, the observations made during the exercise, and recommendations for enhancing the coordination process. Each incident coordinator submits the coordinated exercise report to the IMT of its own organization, and the organizations in the community can work together to improve the coordination and the exercise process.

6.5 Building trust

Trust is essential for the multi-party coordination relationships to handle information security incidents together. However, building trust is a comprehensive problem that involves many aspects of issues in information security incident management coordination. Methods that can build trust include but are not limited to:

a) defining confidential data types and the access restriction rules in coordination policies, such as NDAs;

b) describing clear requirements in information sharing rules for removing sensitive information where possible;

c) holding training events or technical meetings from time to time, either virtual or face-to-face ones are helpful, such as a periodical meeting between incident coordinators of organizations in the community;

d) conducting regular coordinated exercises;

e) encouraging members to actively participate in the community's communication;

f) supporting members to maintain stable and trained personnel to participate in coordination activities;

g) encouraging members to get familiarized with the organizational culture of other members.

Annex A
(informative)

Examples of information security incident management coordination

A.1 Example of large-scale DDoS attack mitigation in cloud service scenario

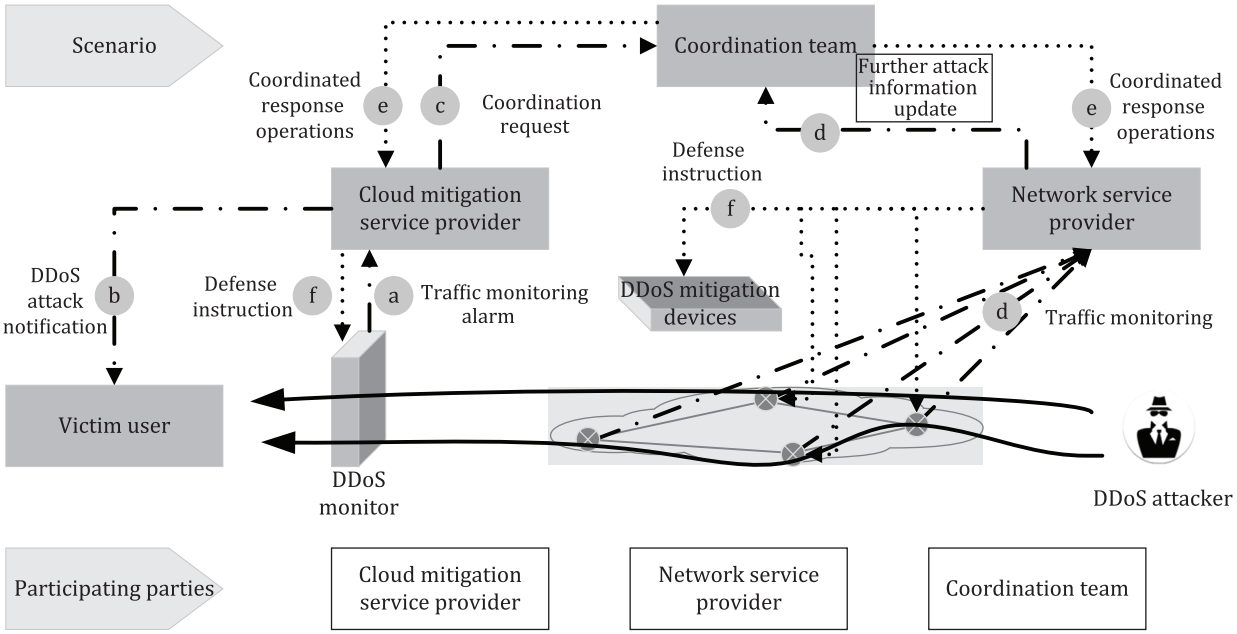

Figure A.1 — Coordination in large scale DDoS attack mitigation in a cloud service scenario

In the example shown in Figure A.1, a distributed denial of service (DDoS) attack is carried out in a cloud service scenario, which is illustrated by the solid lines. To mitigate the affect of the DDoS attack, relevant parties can perform coordination activities using the following steps a) to f), which are referring to a) to f) in the figure.

a) The cloud mitigation service provider detects that the user is under attack. The network service provider detects the attack through network routers and DDoS monitors.

b) The cloud mitigation service provider immediately sends a DDoS attack notification to the victim user.

c) The cloud mitigation service provider implements the configuration strategy according to the user requirements and sends the defined instructions to the DDoS mitigation devices. Under the circumstance that the attack flow exceeds the capacity, the cloud mitigation service sends the coordination request to the coordination team.

d) The cloud mitigation service provider and the network service provider synchronize the attack information with the coordination team.

e) Upon receiving the coordination request for the DDoS attack, the coordination team organizes the cloud mitigation service provider and the network service provider to jointly determine the coordinated response plan.

f) The cloud mitigation service provider and network service provider send disposal instructions to network routers and DDoS mitigation devices according to the coordinated response plan.

A.2 Example of botnet mitigation coordination scenario

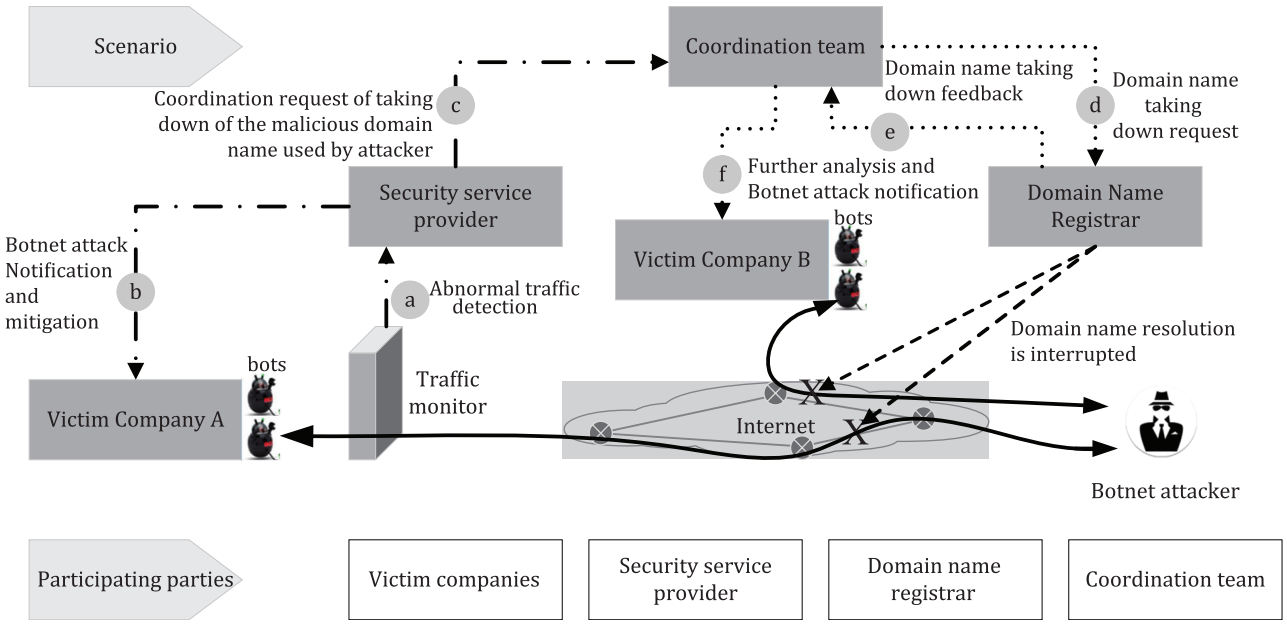

Figure A.2 — Coordination in botnet mitigation scenario

In the example shown in Figure A.2, a botnet attack affects two victim companies, which is illustrated by solid lines. Company A outsources security management to a security service provider, and the security service provider detects the botnet attack. Company B operates its own IRT and also benefits by recovering from the same botnet attack. The coordination activities include the following steps a) to f), which are referring to a) to f) in the figure.

a) The security service provider detects abnormal traffic by monitoring of intrusion detection sensors, firewalls, logs and other security devices. After comprehensive analysis, it is confirmed that Company A is under botnet attack.

b) The security service provider notifies Company A and takes necessary technical counter measures to help Company A recover from the botnet attack, including cleaning all infected systems and removing the bots installed.

c) Through further analysis, the security service provider determines the domain name used by the attacker. The security service provider contacts the coordination team to request taking down the malicious domain name.

d) After verification, the coordination team forwards the request to the responsible domain name registrar to take down the malicious domain name (the dashed lines). The traffic from the bots to the botnet attacker is interrupted since the domain name is no longer resolved.

e) The domain name registrar cooperates to take down the malicious domain name and sends feedback to the coordination team.

f) The coordination team through analysis further finds another victim Company B, and notifies Company B about the attack information. Since the malicious domain name is already taken down, Company B is no longer under attack, however Company B should still perform a self-check, clean all infected systems and remove the bots installed.

A.3 Example of cross-border phishing takedown scenario

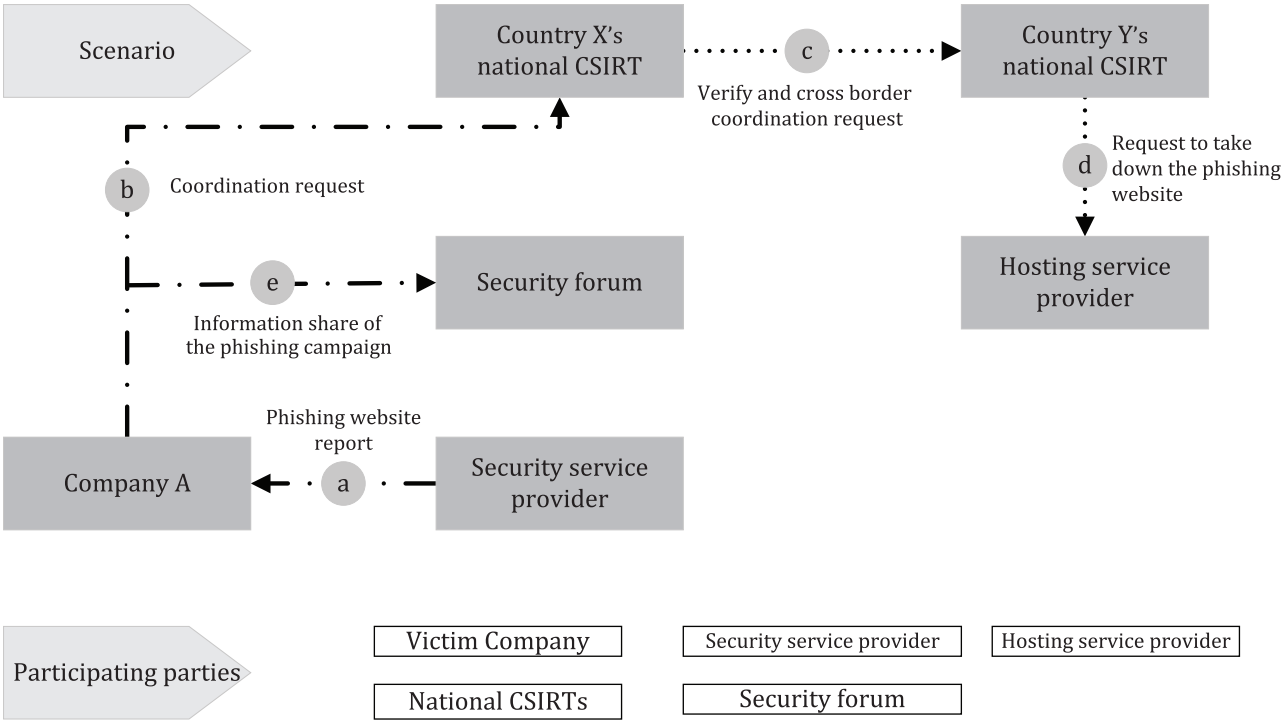

Figure A.3 — Coordination in cross-border phishing takedown scenario

In the example shown in Figure A.3, the activities of the cross-border phishing takedown coordination include the following steps a) to e), which are referring to a) to e) in the figure.

a) A Company A in country X which runs an online store received a report from the security service provider that there is a phishing website that mimics Company A's online store.

b) After the investigation, it was identified that the phishing website is hosted in a server hosted in country Y. Company A wants to have the phishing website taken down. However, Company A does not have a direct contact to the owner of the server.

c) Company A consults country X's national CSIRT for cross-border coordination with the hosting service provider.

d) Country X's national CSIRT contacts country Y's CSIRT to take down the phishing website.

e) Company A can also share the phishing campaign with an industry security forum such as the Anti Phishing Working Group (APWG).

Bibliography

[1] ISO 22300:2021, *Security and resilience — Vocabulary*

[2] ISO 22320:2018, *Security and resilience — Emergency management — Guidelines for incident management*

[3] ISO 22397:2014, *Societal security — Guidelines for establishing partnering arrangements*

[4] ISO/IEC 27010:2015, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

[5] ISO/IEC 29147:2018, *Information technology — Security techniques — Vulnerability disclosure*

[6] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Computer Security Incident Handling Guide[online]. Paul Cichonski, Thomas Millar, Tim Grance, Karen Scarfore. August 2012 [viewed 2024-07-15]. Available at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[7] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide to Cyber Threat Information Sharing[online]. Christopher Johnson, Mark Badger, David Waltermire, Julie Snyder, Clem Skorupka. October 2016 [viewed 2024-07-15]. Available at https://csrc.nist.gov/publications/detail/sp/800-150/final

[8] INTERNET ENGINEERING TASK FORCE. (IETF). RFC 5070: The Incident Object Description Exchange Format [online]. Edited by R. Danyliw, J. Meijer and Y. Demchenko. December 2007 [viewed 2024-07-15]. Available at https://www.rfc-editor.org/rfc/rfc5070.txt

[9] INTERNET ENGINEERING TASK FORCE. (IETF). RFC 6545: Real-time Inter-network Defense (RID) [online]. Edited by K. Moriarty. April 2012 [viewed 2024-07-15]. Available at https://www.rfc-editor.org/rfc/rfc6545.txt

[10] VERSION S.T.I.X. 2.1[online]. Bret Jordan, Rich Piazza, Trey Darley. 10 June 2021 [viewed 2024-07-15]. OASIS Standard. Available at https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html

[11] VERIS. [online]. [viewed 2024-07-15]. Available at https://verisframework.org/index.html

[12] Facebook Threat Exchange. [online]. [viewed 2024-07-15]. Available at https://developers.facebook.com/docs/threat-exchange/

[13] CRITs Data Model. [online]. [viewed 2024-07-15]. Available at https://crits.github.io/

ICS 35.030
Price based on 22 pages

iso.org