For the purposes of this response, we categorise the cyber security maturity of organisations into these three categories with these attributes:

	Number of organisations in Group[1]	attributes
A	~1%	• very good security tools, capabilities, data • resources managed well • might use their expertise to market services to other organisations, such as C's
B	~9%	• moderate use of security tools, collection of data and staff capabilities • still implementing and building • struggle with proper allocation of resources
C	~90%	• cannot afford sufficient resources to manage security with internal staff • need to use outsourced services (such as MSSP) to effectively • primarily reactive

I. General Incident Coordination Considerations

1. What does your organization see as the greatest challenge in information sharing throughout the incident response lifecycle?

To consider this question, you have to consider the reason to share. There are generally three reasons to share:

1) You have information relevant to a specific organisation. In this case, the information is most relevant to that organisation and not as relevant to other organisations. For example, you receive attacks from another organisation. The receipt of those attacks indicates that organisation has a problem, and they might not be aware of it. Informing them allows them to take action to resolve the problem. Or an incident involves the exploitation in a vendor's product and there is a need to share with that specific vendor.
2) You have information relevant to a specific sector. In this case, you have information related to attacks against the infrastructure or services unique to a specific sector. The primary beneficiaries of this information are other members of that sector. For example, if your industry operates control systems and you discover a compromise of one of those systems, the other members of your sector who use that equipment would be the primary beneficiaries.

[1] The actual number in each group will vary from sector to sector. For example, in the Banking and Finance sector, which has greater technological maturity than other sectors, the percentage of organisations that are "A's" will be greater than in other sectors.

3) You have general information. In this case the information could be relevant to any organisation with the capability to use that information. For example, you discover a new vulnerability being exploited in a specific browser. Any organisation competent to take defensive steps to protect against that vulnerability could be a beneficiary.

The primary challenge is getting a piece of information securely to the relevant parties without exposing information about your own problems, without informing your adversaries and minimising the resources you have to devote to sharing.

In each of the three general reasons listed above, the sharing variables have different values and the variables can differ depending on whether you are contributing or receiving.

On the sharing (contributing) side, the challenge is distilling information others would find valuable and contributing that to a set of people you are comfortable will not intentionally or unintentionally cause the information to be disseminated to someone undesirable (which could include the public or adversaries). There is also the secondary desire that you are receiving sufficient value in return for your contributions.

The less cyber security maturity an organisation has, the less likelihood it will have information that can be shared and used effectively by other organisations. Additionally, the results from sharing are less predictable the more widely you share. If you share “too widely” you might be exposing information beyond your comfort level to people whom are not [known to be] “trustworthy” and you might be [inadvertently] informing your adversary. Even if these problems do not actually occur, they are feared and that impedes sharing. This is the reason why many sharing groups become less effective as they grow.

On the receiving end of sharing, the challenge is getting information relevant to you that you can rely upon (or have confidence in) and that you have the capability to use. The first two variables are dependent on the quality of the source and the last variable is on your own capabilities (technology and people).

In most cases, the act of contributing and act of receiving are decoupled. So while in general it is understood that for sharing relationships to be successful (bilateral or multilateral), all participants receiving must contribute, for a variety of reasons, some organisations will not contribute a sufficient volume of information to be considered reasonable by their peers. This has led some information sharing groups to impose mandatory minimums on contributions with organisations failing to meet those minimums expelled from the sharing group.

The most mature organisations are less likely to have problems with the volume of contributions as they clearly understand the value and have information with significant value.

In addition, there is a technical capability aspect to this challenge. Current technologies for secure communications require significant knowledge, overhead for key management, or require unacceptable amounts of human interaction to facilitate the timely sharing of information.

2. Describe your organization's policies and procedures governing information sharing throughout the incident lifecycle. Also describe to what degree senior management is involved in defining these policies and procedures.

In our experience, usually only "A" companies have thought this through in a thorough way, and they make organisational decisions on how to share information. A primary method of making this decision is to join a group (formal or informal) that exchanges information.

Unfortunately, these conversations have often led to policies that require legal counsel review of information to be shared, which also decreases the timeliness and utility of the information.

3. What role does senior management have in the execution of your policies and procedures?

Today, this varies widely. In organisations with less mature cyber security capabilities sharing is occurring without the knowledge of senior management as technical staff forge their own relationships with their peers outside of the organisation.

Senior management should be involved in crafting the organisation's cyber security strategy and policies. Because some of the most valuable sharing must occur in a very timely fashion to obtain maximum value, senior management should not be involved in the decision to share each piece of information, but rather more broadly in establishing the strategy and parameters, and broad relationships, and should encourage lower-level relationships to be developed with appropriate peer organizations.

4. To what extent is information sharing incorporated into your organization's overarching policies and processes?

The more mature the organisation's cyber capabilities, the more likely it is to be incorporated in policies and processes. We believe that the vast majority of organisations do not address this type of sharing in written policies in a comprehensive way. Often, the policies and processes are dictated by the framework of the sharing relationship rather than internal discussions and decisions.

Incorporation of sharing in policies and processes is highly variable based on the type of information shared and the type of organisation shared with. It is more likely that the sharing of information with business partners, vendors, and news media will be spelled out in policies than sharing with peers. Some organisations are also required to share (mandatory reporting) for regulatory reasons.

5. How much of your incident handling effort is spent on the different phases of the incident handling lifecycle (from NIST SP 800-61): (1) preparation, (2) detection-and-analysis, (3) containment-eradication-and-recovery, (4) post-incident-activity.

6. What are the relevant international, sector -specific or de facto standards used or referenced by your organization to support incident handling and related information sharing activities?

This remains an area for work. While some standards do exist, they do not have broad adoption, and the use of standards is more likely in organisations with advanced cyber security capabilities. For example, you are more likely to find a standard like OpenIOC, IODEF, STIX, etc. used amongst "A" organisations.

7. How do you determine that an incident is in progress (or has happened)?

"B" and "C" organisations operate based on discrete incidents that follow the traditional incident lifecycle, which initiate with a "discovery" or "report". "A" organisations tend to manage incident response differently. Rather than focusing on specific, discrete incidents, they focus on activity of adversaries and the specific, on-going changes to their defences they can make to impede the objectives of their adversaries tactics, techniques, and procedures (TTPs).

In "B" and "C" organisations, there is usually a "discovery" or "report" of some activity that indicates there is an incident underway. They can be from an internal or external report, which could include an automated alert such as from an intrusion detection service.

"A" organisations tend to be continuously analysing their collected data and intelligence, applying new learning to that data to make discoveries of new "incident activity". This *learning* can come from internal analysis or information from their peers in other organisations.

8. How do you determine that an incident has been handled and requires no further action?

Again, this depends upon the cyber security maturity of the organisation. More mature organisations focus on reconstitution of an impacted service and business process and on how this specific activity should guide changes in broad defences or the defence against specific adversaries. This is accomplished through a series of parallel activities.

One specific shortcoming is lack of forensic analytical rigor. Understanding the tactics and techniques underlying an incident requires additional expertise and expenditure of resources that are not likely to be available in less mature organizations. This likely leads to decreased situational awareness, and missing a significant opportunity to improve defensive posture of the organizations and potentially peers.

Less mature organisations will focus on the conclusion of the investigation including possible legal/law enforcement aspects, and repair of compromised systems or services. This tends to be a more serial process.

9. How do you determine when to coordinate and/or share information with other organizations regarding an incident?

The value of sharing is directly proportional to the organisation's cyber maturity. The more mature the cyber capabilities the more valuable sharing can be.

Less mature organisations are likely to focus more sharing activities on sharing reasons 1 (specific organisation) and 2 (sector) (see question 1). They are likely to have less capability to effectively use general information shared with them and are less likely to be able to generate sufficient timely information other organisations would find value in receiving.

Note that for "C" organisations, they are more likely to have some or all of the incident response processed outsourced. As part of that outsourcing, their security vendor might be sharing unattributable information from their customers' security incidents. In this case, the "C" organisations might be benefiting from that bilateral/multilateral exchange without realising it is happening, and since it is unattributable information, their risk is low. Also note that the "C" organisations might be buying these services from "A" organisations, and one model for plugging "C" organisations into an effective sharing model is through buying service from "A" organisations.

10. Do you have documented case studies or lessons learned to share (good or bad examples)? If so, please provide URLs or attachments with your response.

II. Organizational Capabilities and Considerations for Effective Incident Coordination

Incident handling teams and coordinating centers often collaborate at varying stages of the incident management lifecycle described by NIST SP 800-61. Within this context, individual organizations may offer specific capabilities and may have specific considerations related to effective incident coordination.

1. Do you maintain a list of key contacts for use during an incident? If so, are these contacts identified as individual people, or as positions?

2. What is the size of your organization (e.g. staff, contractor s, members)? How many individuals are involved in incident coordination activities carried out by your organization?

3. Relative to the incident response lifecycle defined by NIST SP 800-61, what aspects of incident coordination occur within your organization?

4. What services and assistance (e.g. monitoring, analysis, information) does your organization provide to others both inside and outside your organization relating to incident coordination?

5. Does your organization have any method for understanding and describing the quality or sensitivity of different types of information shared by a third party? For each type of information, can you describe the method?

This is an area that is not mature and needs additional research. If larger sharing groups are going to be successful, there has to be the capability to allow a recipient of information from a sharing group to understand what level of confidence they can place in that information.

For example, within a sharing group, a contributor could gain a “reputation” based on the ranking of the information used by recipients. This can allow a recipient to take action, in part, based on the reputation of the contributor. Perhaps, for a contributor with a high reputation, a receiver might be more willing to take a contributed indicator and add it to a “block list” where they would only be willing to add it to a “watch list” for contributors with lesser reputations.

6. Approximately how many employees (please indicate full time or part time as appropriate) do you devote to incident response?

7. If possible, list examples of highly effective computer security incident response teams and comment on what made them successful.

Systems and networks where a wide variety of security-relevant data is collected for both real-time analysis and retrospective analysis. Tools to analyse the collected data and capability to build upon the tools and analysis. A wide variety of dynamic defensive capabilities. Good analytical incident staff.

8. Based on your personal or your organization's experience, what are the most and least effective communication mechanisms used (e.g., phone, email, etc.) when coordinating an incident, and why? In what order do you typically use specific communication mechanisms?

The least effective is completing lengthy incident response web forms. These take too much time to complete and divert resources away from response efforts.

The most effective communication methods depend on the nature of the information being shared. If it is indicators, they need to be shared quickly, so they require sharing mechanisms that can facilitate fast sharing of structured actionable information to groups of people.

If the information is best practices learned from incident activity, it is best shared either in technical exchanges or in white papers.

9. Do you have examples of alternate communication mechanisms used because an incident has degraded communications?

An alternative question is do you have alternative communication mechanisms if you can no longer trust your primary communication mechanisms because they are or might be under the control or observation of an adversary. Many mature incident response capabilities establish communication mechanisms totally separate from any of their organisation's infrastructure to help manage this type of problem.

10. Do you hold regular incident review meetings? Between organizations? How frequently? If your team does not hold incident review meetings regularly, why not?

11. What skillsets (e.g., network sniffing, system administration, firewall configuration, reverse engineering, etc.) does your organization need most when an incident is in progress?

12. Are there incident handling and response skillsets that are specific to your industry or sector?

13. How do those skills relate to information sharing and communication before, during and after an incident?

III. Coordinated Handling of an Incident

1. Do you report incidents or indicators to US-CERT?

2. Do you coordinate incident response with organizations other than US-CERT?

3. Do you participate in an incident coordination community such as the Defense Industrial Base (DIB), the Defense Security Information Exchange (DSIE), or an Information Sharing and Analysis Center (ISAC)? What are the benefits? Are there any pain points?

Many responses from section I apply here. In addition, I believe that organizational and personal trust, appropriate direction, and perception of ulterior motives often lead to challenges with these relationships.

4. How is information about threats and/or incidents shared among coordination community members?

Mainly in human-parsable information products, although some

This is primarily defined by the type of data and how critical it is to be shared quickly. Indicators generally need to be shared quickly to have the greatest impact. To best defend against a new threat, organisations need to deploy new defensive measures against them, and reduce the time that their organisations are vulnerable. That is most effectively done when those indicators are shared quickly and defensive measures deployed quickly.

Organisations can also share information that is which has less temporal criticality. For example, discussing new methods or techniques for managing web browsers to minimise the possibility that a compromised web browser can result in an adversary obtaining sensitive data. Sharing these best practices is frequently best done via exchange of written practices or interactive technical exchanges.

5. How do you prioritize incidents?

6. How do regulatory requirements affect your organization's ability or willingness to share information or collaborate during an incident?

7. What regulatory bodies are you required to report information to regarding incidents? For each regulatory body, what kind of information does your organization report and what has been your organization's reporting experience?

IV. Data Handling Considerations

1. What, if any, types of information would create risk or disadvantage if shared by your organization?

The information that is of higher risk also tends to be the information other organisations can least effectively use if shared: commercial impact of the incident, specific victims, regulatory or legal liability/impact, criminal investigative information, some root causes associated with employee mistakes or wrongdoing.

2. What kinds of information would you never share with a peer during incident handling?

For most organisations it includes: the business impact, the nature of specific information (intellectual property) stolen, damaged or impacted, status of criminal investigations, names of other associated parties (such as customers, business partners).

Note, there are some exceptions to these amongst organisations with a very strong bilateral or multilateral sharing agreement or in very unique circumstances unique to a specific incident.

3. What types of protections, redactions, or restrictions would aid your organization in sharing information?

Ability to effectively share without possibility of attribution (can be impeded by regulation, need to value the volume of data contributed), better tools and mechanisms for secure sharing in a timely fashion.

4. Do you use specialized formats to communicate incident information?

5. What do you see as the pros and cons of specialized formats for representing and communicating incident information?

Distilling data and analysis into a standard format that is useable is a challenge. Analysis tools and methods frequently do not create data in a form that can easily be represented in a standard format. Of the standard formats that exist today, a few use used broadly – most are not.

6. What incentives exist for your organization to share information with other organizations during an incident?

The main incentives are

- because you need an immediate response from them to help you resolve the incident,
- to receive information valuable to your defences when someone else experiences activity first and can share that with you.

7. What disincentives exist that might prevent your organization from sharing information with other organizations during an incident?

- having a prior bad experience from sharing.
- insufficient resources to divert from response to sharing (when sharing is not integral to responding, such as sharing with a vendor when you have a vulnerable product)
- having legal, compliance, public relations or other personnel outside of incident response personnel influence against sharing.

8. If available, please provide an example when sharing with other organizations proved to have negative implications for your organization's incident response.