Multinational Experiment 7

Outcome 3 – Cyber Domain

Objective 3.2

Information Sharing Framework

22 January 2013

Point of Contact:

sact.mcdc@act.nato.int

Executive Summary

This Information Sharing Framework (ISF) provides the guidance to establish the capability to increase an organisation's cyber Situational Awareness (SA) enabled by sharing information across a trusted community of interest. It describes the context and the business case for participation, and includes the collaborative governance, federated access control and management of information quality. All of which are required for effective decision making.

Cyberspace has rapidly evolved into a key domain, similar to the other domains of the Global Commons (GC): Air, Sea, and Space, and continues to expand. Increasingly, daily life for citizens, companies and governments depends on the availability of the cyberspace domain. Most of our activities and decisions in our physical world depend on information and access to cyberspace.

Unfortunately, the misuse of cyberspace and the growing number of attacks on cyber networks have become major problems for nations and organisations, which they have to address together if they are to succeed. Sharing information quickly about the status of cyber security controls, potential threats and vulnerabilities, alerts, incidents and more, provides a quality cyber SA. This forms a basis for good decision-making to ensure the normal availability of cyberspace.

Cyber incident information is shared today between working-level organisations, such as CERTs (Computer Emergency Response Teams), but not using any standards-based approach or methodology. For success to be achieved, a top-down, standards-based *Information Sharing Model* is proposed, focusing on security controls based on the policies, procedures and mechanisms for federated Trust, and also the Taxonomies (specifications for data elements and rules for their use) for information interoperability.

Trust is the most important factor in any information sharing community. Trust depends on an AAA Model: *Authentication* ("Are you who you claim to be?"), *Authorisation* ("Do you have permission to undertake the activities?"), and *Accountability* ("Can you evidence what you have done in any court of law?"). The ISF describes federation – the shared use of common policies, procedures and mechanisms that are based on international standards and AAA.

The ISF also leverages taxonomies from ENISA (European Network and Information Security Agency) and IETF (Internet Engineering Task Force).

The *Information Sharing Model* describes the means required for sharing information, proactive (push) and reactive (pull) , alerts and warnings, lessons learned, experiences, and best practices, information on security quality management, proactive artifact handling based on anomalies and predictions.

The Information Management Model is focused on ensuring the quality of the shared information, which is vital to good decisions. Information needs to be timely, accurate with the right degree of richness.

Using federation, AAA and the taxonomies, Multinational Experiment 7 (MNE7) proposes a mesh of Hubs and Nodes to coordinate information sharing and maximise cyber SA. The model is based on existing federated secure collaboration capabilities in defence, intelligence and industry, comprising independent entities bound together by Information Sharing Agreements, and further united by collaborative governance authorities.

Table of Contents

Introduction

1. Historically, the Global Commons has referred to the common domains of air, sea and space across the Earth, not owned by any single nation. Cyberspace is now considered a Global Commons of great significance, as all other domains depend increasingly upon it for their management and future. The need to ensure access to cyberspace is profound and pervasive. Every nation and industry sector on the planet depends daily, and directly or indirectly, on having unhindered access to cyberspace. But cyberspace is boundaryless and vulnerable, facing increasing threats of disruption and data theft – over $2 trillion of global cybercrime is forecast for 2012 – which already have consequences for society, nations, industries and governments. Hence nations must collaborate to ensure universal and safe access to cyberspace.

2. Collaboration depends on the ability to share sensitive information between trusted partners to enable more effective decision making in organisations across industries and governments. The organisations maintaining cyberspace have to collaborate in the same way. This Multinational National Experiment 7 (MNE7) Information Sharing Framework (ISF) describes how sensitive information should be shared across organisations, enhancing the organisational and collective Cyber Situational Awareness (Cyber SA) and improving individual and collective decision making process.

3. The ISF gives strategic guidance on the policies, procedures and mechanisms that any trusted partner will require in order to collaborate. It is a blueprint for collaborative policy development across communities of nations, and military and industry organisations.

Aim and scope

4. The aim of the ISF is to provide guidance for implementing and operating policies, procedures and mechanisms for sharing sensitive Cyber SA information between trusted partners. It is a blueprint for collaborative policy development across communities of nations, and military and industry organisations.

5. The ISF is ultimately for decision makers, particularly in cyber, politics, military, government, industry and academia. It should guide political and legal advisers, policy makers, risk managers, cyber defence organisations, service providers and others.

6. The scope of the ISF includes:

- The *Information Sharing Model*, focusing on federated access control.
- The *Information Management Model*, focusing on the information to be shared.

Context

Understanding Cyber

7. Cyber has roots in the Greek word "*κυβερνητικός*", meaning skilled in steering or governing. The term "cybernetics" is widely recognized in the context of the control of complex systems in the animal world and in mechanical networks. However, since cyber has been introduced it has taken on several meanings. The term is used effectively in business, law and policy, and it has highly useful application in that it provides a reference to the virtual (i.e., other-than-physical) world created by the Internet and other electronic communications. Cyberspace is a domain but it does not exist without the physical ingredients from which it is composed.

8. Several definitions of cyberspace exist. Here are two:

a. Cyberspace is an electronic medium through which information is created, transmitted, received, stored, processed, and deleted; and

b. Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

9. There is a growing international consensus that cyberspace is both virtual and physical. It is not just limited to networks; it is also includes the information and entities that interact with each other and with information within and across networks. The ISF assesses that any nation whose interpretation of cyberspace is focused only on physical networks, is at an increasing disadvantage with the shift to information exploitation and augmented reality. Augmented reality is a live, direct or indirect, view of a physical, real-world environment whose elements are augmented by computer-generated sensory input such as sound, video, graphics or GPS data; it is in increasing use in law enforcement, military, crisis management, aerospace, health and elsewhere.

Using Cyberspace

10. Cyberspace has enabled extraordinary transformation, benefits and financial growth in recent times. Its use continues to expand in volume of users and functional capabilities. Citizens, consumers, government employees, industry employees, devices and systems expect cyberspace to deliver more and enable faster change. Governments encourage these developments but are only just starting to address the implications – see European Digital Agenda and the U.S. Cyberspace Policy Review.

11. Attitudes are changing. Younger generations in developed countries have no experience of a pre-internet, paper-driven, manual world where concepts of friendship, social responsibility, community and trust, and the nature of business were all very different. They have different views and values that can extend into the workplace where cyber-crime, insider fraud, intellectual properly theft and illegal financial trading are all increasing.

12. Immigration and social mobility create cultural and ethnic diversities that can complicate notions of national citizenship, identity and community. Internet-enabled social networking has magnified both the benefits and risks of these changes, and enabled new social engineering threats that liberal societies find difficult to address.

13. Technology enables changing use and behaviours. The desire for convenience and financial benefit often ignores major security risks, more so in cyberspace where users readily ignore risks that would concern them in the physical world. Users – people, governments and companies – are an increasing part of the problem when it comes to protecting cyberspace. A polarization between trusted and untrusted users exists.

14. Criminals continue to make great use of cyberspace, where they have four key advantages:

a. Cyberspace wasn’t built with security in mind – it is insecure and untrusted. No common trust mechanisms exist in cyberspace. Anonymity is easy in cyberspace and it is easy to hide;

b. Cyberspace enables criminals to expand their business empires internationally and adapt rapidly to changing opportunities, and do so faster than governments;

c. There is a relative lack of awareness, coordination, legislation and law enforcement capability within and across nations. CERT coordination is only just beginning. There is insufficient coordinated proactive and preventative activity; and

d. Less developed nations are particularly vulnerable. Citizens may embrace mobile technologies but their governments are unable to detect and prevent organised crime from establishing flourishing bases for global cyber-crime.

15. If users, service providers and governance organisations know who to trust, the detection of bad people and organisations, and remedial action becomes much easier.

Protecting Cyberspace

16. The boundaryless nature of cyberspace, the speed and scale of effects, and the relative ease with which one can remain anonymous, compounds the complexity of the challenges facing the decision makers and organisations responsible for ensuring secure access to cyberspace. Automation linked to human evaluation and oversight is paramount.

17. The two strategic threats of concern to MNE7 are:

a. Deliberate or inadvertent disruption of:

(1) Cyber services (a range of data exchanges in cyberspace for the direct or indirect benefit of humans); and

(2) Cyber infrastructure (the aggregation of people, processes and systems that constitute cyberspace), i.e. more than just the network.

b. Data exfiltration – the deliberate theft or inadvertent loss of sensitive data that could be used for criminal purposes. This may sometimes be state-sponsored.

18. Deliberate state-sponsored attacks are a major concern of governments, however the advent of offensive capabilities for cyber warfare and cyber-attack are leading to governments preferring to use cyber proxies, often organised crime.

19. The growing number of internal and external attacks on cyber infrastructure has become one of the most serious economic and national security threats worldwide. EUROPOL reported to the European Commission (EC) DG HOME Expert Group in 2010 that ID fraud is now the top enabler for all aspects of crime across Europe and almost all crime is internet-enabled at some point.

20. The EUROPOL iOCTA report indicates that global cybercrime exceeded $1 trillion in 2008. Subsequent expert discussions, including U.S. Government agencies project global cyber-crime to be around $2 trillion in 2012. UK Government's Fraud Indicators for 2012 report £73 billion fraud, up 20%, reinforcing an EC expert committee's assessment of some €500 billion fraud across Europe in 2011, making it a dominant contributor to the Euro crisis. The European Parliament is developing new legislation to force greater accountability into information systems containing sensitive information, which will strengthen the legal basis for protecting cyberspace. Some nations are taking similar measures.

21. Within MNE7, cyber defence and cyber security are synonymous. The traditional view of cyber security has focused on technical factors. This is changing as requirements advance for information protection, cyber services and cyber infrastructure protection. Within the ISF, cyber security is defined as - a property of cyberspace that is an ability to resist intentional and unintentional threats, and to respond and recover.

22. Cyber security experts are used to considering enterprise risks and requiring mitigations based on Confidentiality, Availability and Integrity (CAI). This is inadequate for information sharing where shared risks dominate. They require a federation model based on agreed security controls and a trust regime based on federated access controls.

Cyber Situational Awareness

23. Attacks will happen and nations, governments, organisations and industry have to be prepared, together.

24. The rapidly changing nature and complexity of cyber threats have highlighted the weakness of isolated (lone or individual) organisational and national responses. Individual cyber security organisations can even increase damage to the business or nation in some cases. It is only by working together that cyber defence organisations can succeed. Such collaboration requires the sharing of sensitive information on the basis of a 'need-to-share' and a community 'need-to-know', allowing those threatened or under attack in the cyber domain to pool knowledge and get advice on the actions they can take to protect themselves.

25. There is currently a gap in our ability to gain and share sufficient cyber SA at the national and international levels to enable effective decision making. The gap inhibits our ability and willingness to work with allies and partners to provide collective cyber security and to take collective actions to ensure resilience and the normal operation of daily life for governments, services, businesses, consumers and citizens.

26. Current cyber security focuses on enabling detection and post action reporting. Much more could be done on collaborative prevention, to ensure stronger cyber defences across cyber infrastructure and cyber services. Cyber SA enables this.

27. Cyber SA in MNE-7 is defined as - the human perception of the elements of cyberspace within an operational and business context, the comprehension of their meaning, and a projection of their status in the near future.

28. Cyber SA exists to enable effective organisational and collaborative decision making to support the protection of cyber infrastructures and cyber services in cyberspace.

29. Cyber SA comprises five major activities that together enable protection:

a. *Physical world status.* Information on any events or developments that could impact access to cyberspace or be impacted by an incident in cyberspace.

b. *Prevention status.* This is healthy Normality or "What Good Looks Like". This includes the health of specific cyber defensive measures of internal systems, government organisations, industry partners and international allies. These health measures comprise a defined set of security controls based on agreed, standards-based, policies, procedures and mechanisms. They include compliance with the latest counter-measures e.g., patch updates. Examples of "What good looks like" within a given Level of Assurance are described in Annex A.

c. *Cyber Threats and Vulnerabilities (T&V) status.* Based on a defined methodology, the T&V status is a major contributor to Cyber SA.

d. *Planned Changes.* A forecast of planned changes and the status of any changes or modifications being implemented helps avoid them being confused as incidents.

e. *Incident Management.* This is dealing with unplanned and unforeseen events that could cause disruption, material loss or damage.

30. The primary functions that use, manage and generate cyber SA include:

a. Decision making, including legal and policy advisers;

b. Intelligence;

c. Incident management;

d. Coordination and communication;

e. Information management.

Benefits and Challenges

31. Information sharing networks exists today leading to cyber SA. Their benefits are cumulative and decision-makers and cyber experts are only just beginning to realise their significance and scale. However, there are many challenges, particularly amongst traditional and isolated governments and industries that have yet to appreciate the need to work together in cyberspace to protect it as a Global Commons, see Annex B.

Information Sharing Model

Architecture View

32. Figure 1 shows Organisation A sharing information with Organisation B, conducting business within and across all of government, military and industry. The stack has 5 layers:

a. Process, where decisions are made;

b. Information, which supports decision making;

c. Applications, which presents data as information;

d. Data, which is interoperable and has quality;

e. Infrastructure, which provides secure hosting and communication.

33. The red line between Collaboration and Competition moves up and down depending on the degree of collaboration. However, the minimum requirement for collaboration is for Data and Infrastructure. Without these, an organisation is isolated.

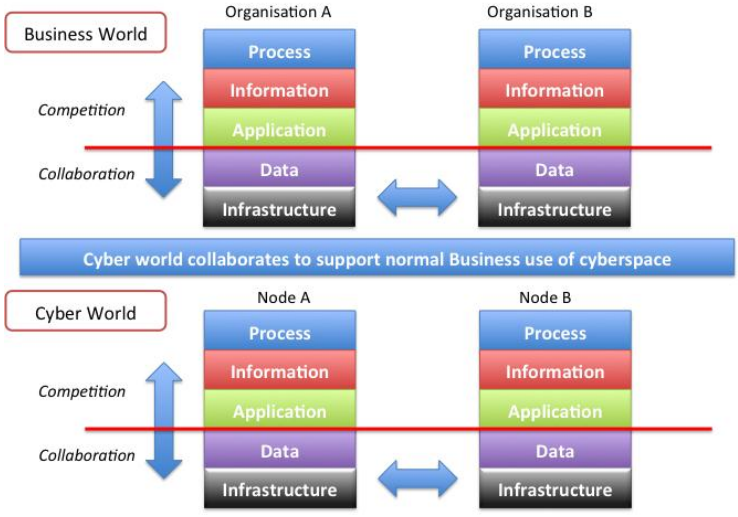


Figure 1 - Collaborating to Support Business

34. Similar cyber defence organisations, i.e. CERTS, have to collaborate to ensure business organisations can access cyberspace. By sharing cyber security information and coordinating their actions cyber defence organisations are more aware and better prepared to handle threats and disruptions within cyberspace. This requires both business and cyber defence organisations, leading to :

a. To trust each other and each to be trustworthy, which requires AAA – Authentication, Authorisation and Accountability – see paragraph 44.

b. To understand each other, which requires a taxonomy of definitions for data and rules for their use. Such definitions and rules enable automation, compliance and enforcement – see paragraph 51.

35. The more organisations are trustworthy, the less vulnerable they are to threats and the less of a burden they are for cyber defence organisations.

36. Expanding these bilateral relationships across a mesh of business organisations doesn't scale. A federated approach is required based on Common Policy, standards and collaborative governance. The structure of cyber defence organisations will need to leverage federation if they are to collaborate and use cyber SA information effectively.

Structural View

37. Today's structure of cyber defence organisations has arisen from a bottom-up, reactive evolution, sharing threat and vulnerability information before incidents and post-incident reports afterwards. Organisations have arisen on the basis of local need to do different things. In the main, they don't monitor the same threats, don't coordinate their defences and they don't share much information – they just don't collaborate. That's now changing as a result of multinational cyber security strategies and international collaborative initiatives, such as the ENISA Good Practice Guide for Incident Management.

38. MNE7's approach is top-down, to interconnect and align existing organisations (e.g. CERTs and WARPs (Warning, Advice and Reporting Points)), and establish the core structure of cyber organisations to enable collaborative protection, detection, prioritisation, response and improvement, made possible by sharing cyber security information, leading to cyber SA, under control. Its approach also recognises the primacy of legislation to underpin cyber security, and that this presents the challenge of multi-jurisdictionally. All of this is made possible by federation – the shared use of common policies, procedures and mechanisms, which are based on current and emerging international standards.

Hub and Node Structure

39. MNE7 has a functional approach to information sharing, using the Hub and Node concept. A Node is the focus for a trusted 'community of interest' (e.g., a national financial, health or transport community) of cyber organisations (e.g., WARPs, CERTs, CIRCs (Computer Information and Resource Centres)). Nodes use standards-based sharing processes tailored to meet additional needs, implemented in common policies, procedures and mechanisms.

40. A Node's functional scope includes support for cyber defence intelligence (threats, vulnerabilities and analysis), cyber defence operations (development, internal and external monitoring, and access control management) and cyber incident management. The degree varies with the maturity level shown in Figure 2.

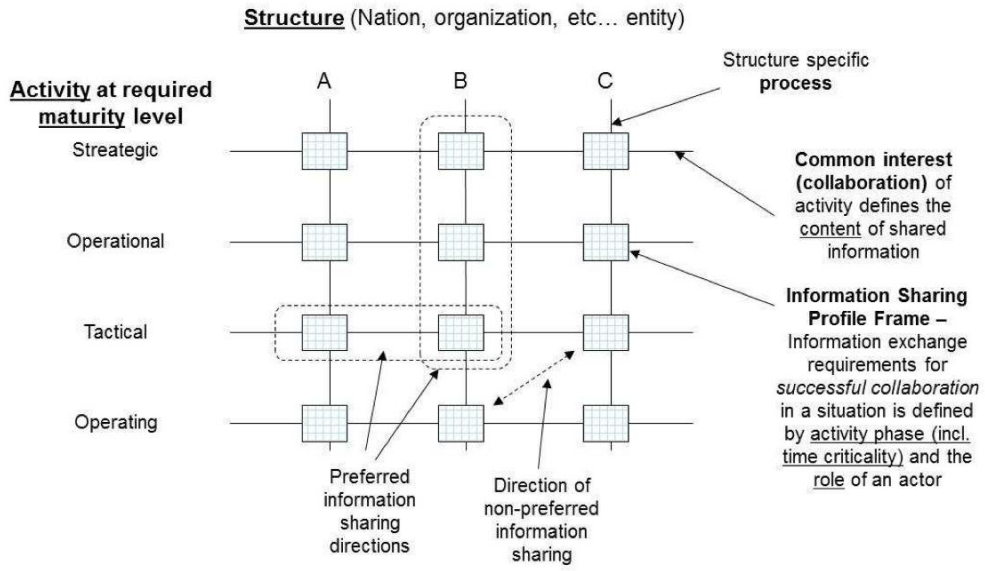


Figure 2 - Mesh of Hubs and Nodes

41. Nodes vary considerably. They can range from being small, geographically local and focused on a small specialist community with limited functionality to being large, multifunctional, national or international. However, they are all involved in the coordination of cyber incident management across individual organisations in their community.

42. Nodes can aggregate into a larger community or federation of Nodes to support wider needs and establish a Node for that larger community. However, being one step further removed from tactical, front line organisations, this higher-level Node will be less involved in dynamic incident management and more focused on coordination and information sharing. Information sharing tends to flatten hierarchies, so MNE7 sees relatively few higher-level Nodes.

43. Instead, MNE7 considers a Hub to be the information focus for supporting high level decision making. A Hub operates to support Nodes and to enable top-level, usually national or international decision-making. A Hub can be considered as a Node with two extra functions:

a. An information repository for all kinds of cyber related information required by its member Nodes and their communities, much like today's CIRCs, to support the design, development, implementation, operation and change management of any node or cyber defence organisation, including cyber intelligence.

b. A high-level decision-making capability, including legal and policy advisers, with access to executive law enforcement organisations and having the authority and capability to switch off or disconnect rogue organisations affecting critical national infrastructures.

44. The relationships between Hubs, Nodes and tactical cyber organisations are not hierarchical. They are interconnected, subject to there being a business need and compliance with federation policy.

45. There would normally only be one Hub for a nation or a region of smaller nations, or international organisations (e.g., NATO and EU), or there may be two Hubs for a global industry sector (e.g., banking, aerospace) or a technology community (e.g., Microsoft, Linux).

46. Figure 2 shows a simplified interconnection of Hubs and Nodes to illustrate the relationships. The operational level has government and industry organisations doing normal business; the tactical level of CERTs, WARPs, CSIRTs (Computer Security Incident Response Teams) etc., focused on incident management; the operational level of Nodes, coordinating and supporting the tactical level and providing information for the Strategic level of Hubs.

47. In reality, each entity in the structure will have many peer-to-peer relationships with other entities at more than one maturity level. Figure 3 illustrates the community and interconnected nature, where all the same icons are also connected to each other but the links are not shown.

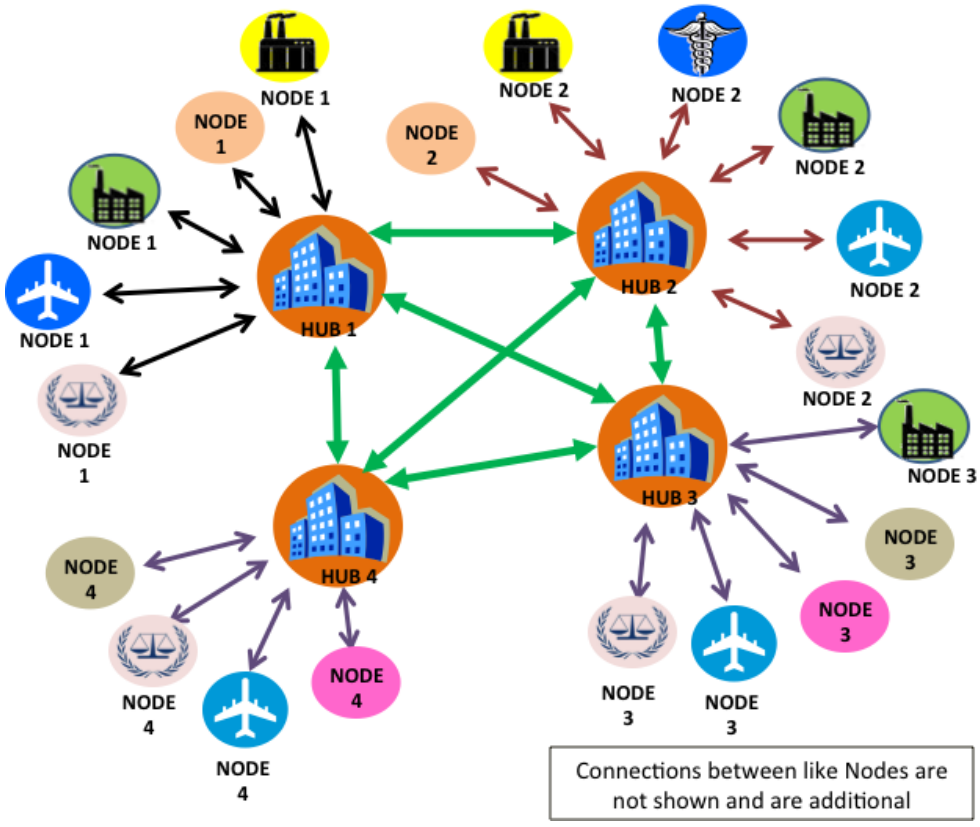


Figure 3 - Interaction between Communities

48. The main functions in Hubs and Nodes are compared further in Annex C.

Information Sharing Agreements

49. An Information Sharing Agreements (ISA) is an agreement made between two or more collaborating organisations which describe verification and compliance methodologies, and define at least:

a. Scope and what types of information are to be shared and in what circumstances.

b. How information is to be used, shared, released, secured, stored, purged and managed. Policy for further use of information (or not) is to be specified.

c. Who (organisation and role) is involved in sharing and managing information, defining the roles and responsibilities.

d. What access control model and policies are to be used.

e. What taxonomies and data labels are to be used.

f. What legal or policy timeframes exist affecting the use, management and retention of information.

g. What procedures are to be followed to enforce compliance, resolve issues and disputes, and to repair/restore normal information sharing arrangements.

h. What supporting legal, regulatory and policy documents must be observed to ensure compliance. These could include Non-disclosure Agreements, Memorandum of Understanding, contracts, and Terms of Reference.

50. In practice, organisations cannot support multiple ISAs, each with another organisation. Instead, organisations subscribe to one ISA for each community of interest in which they participate. Each community's ISA will have some commonalities and some differences in their Authorization and Accountability models. However they should have a single Authentication model based on federation at an agreed Level of Assurance - multiple authentication models are difficult, costly and risky to manage.

51. A simple example of an ISA is at Annex D.

Information Sharing Processes

52. The primary means of sharing information include push and pull methods. Every Node, Hub, WARP, CERT etc. would be expected to use most of these methods, with federated access control based on AAA:

a. Secure email is a push mechanism, used both to exchange information and to alert. PKI (Public Key Infrastructure) enabled Secure Email meets the requirements for at least EAL4 (Evaluation Assurance Level 4). It is based on a special use of PKI federation (see below).

b. Dashboards provide key performance and status indicators together with alerts.

c. Secure databases with formatted/structured data. These facilitate a high degree of data analysis and data integrity, but are increasingly giving way to more flexible content management tools handling data of all types.

d. Collaboration tools (such as Sharepoint, Team Room…) are a push mechanism, and are ideal for creating large scale repositories of documents with associated information management for unstructured information.

e. Business social network. This is a subscriber-based model where any community organisation or person can offer information, to which anyone can subscribe.

f. Collaboration tools are expected to blur with content management and social networking tools in the near future.

Trustworthiness, Federation and AAA

53. As business becomes more collaborative and international, so there are increasing legal, regulatory, and commercial requirements for accountability and information protection in regulated industries and organizations. Such information protection requires access control, which requires identity, authentication, authorisation and accountability (AAA) – these are the basis of trust. MNE nations have specified Trust as the most important enabler for sharing Cyber SA.

54. Trust across multiple organisations requires federation, where all federation members agree to abide by a set of policies, procedures and mechanisms defined in federation Common Policy. All organisations have to be considered Trustworthy to trust each other in the community. Their internal implementations are audited by certified Trusted Third Parties prior to being allowed to operate. They also need a common language to understand each other. Federation requires collaborative governance and agreed Common Policy.

55. Trustworthiness ratings are being applied to organisations. If organisations are not sufficiently rated on a trustworthy scale, this can affect their ability to do business.

56. For Authentication, governments and industry sectors are implementing High Assurance (Level of Assurance (LoA) 3 or 4) PKI federations and inter-federations, in accordance with international standards, to support the sharing of sensitive information. This includes several MNE7 nations. Internationally, NATO and law enforcement organisations are doing likewise. Looking forward, only LoA 3+ federation-compliant cyber security organisations can expect to share sensitive information internationally. Non-compliant nations need to federate as soon as possible, which means either using an existing PKI Bridge or building a national bridge, which then federates with other PKI Bridges to provide the foundation for information sharing communities.

57. The ability of any nation/organisation to use this ISF, and share cyber SA, depends on them having the ability to federate at LoA 3+. Further information is at Annex E.

58. For Authorisation, all organisations in a community require a common definition of user roles (what a role means, how it should be used and the types of information that a role can access) and a taxonomy, which specifies the meaning and use of a data entity and associated attributes.

59. For Accountability, national authorities approve a trust scheme to certify Trusted Third Party (TTP) auditors. At LoA 3+, approved schemes include *tScheme*, *Kantara Initiative* and *Webtrust*; other nationally approved schemes may be internationally acceptable. Accountability may also require:

a. Accreditation by a national security organisation.

b. Installation of monitoring agents within an infrastructure to notify national authorities of any policy violations or possible incidents.

c. Frequent or regular inspections by TTPs to verify continued compliance.

Taxonomies

60. Taxonomy is a set of agreed definitions for data and rules for their use. The word taxonomy derives from the Greek words *“taxis”* meaning arrangement or division and *"nomos"* meaning law. In the context of cyber SA, taxonomy is the classification according to a pre-determined system with the resulting catalogue used to provide a framework for sharing information. Collaborating organisations need taxonomy so that they can understand and use information consistently and coherently across the community. Taxonomy is used for information preparation.

61. In working to define taxonomy, it should: be media independent; have a specific use; have a logical hierarchy; be easy to understand by users in different divisions or departments; conform to other published taxonomy standards; not be redundant to other defined metadata; avoid acronyms or abbreviations where possible; and not nest further than 5 levels.

62. A number of taxonomies already exist for incident management nationally, in ENISA, the Afghan Mission Network etc. However, the emerging standard for large scale cyber SA for Incident Management is IODEF (incident Object Description Exchange Format) IETF (Internet Engineering Task Force) RFC 5070 at Annex F.

Information Release - Traffic Light Protocol

63. The Traffic Light Protocol (TLP) is one example of how to classify and release information within a federated information sharing community. Using TLP, the originator can label information with one of four colors to indicate what further dissemination, if any, can be undertaken by the recipient. The recipient must consult the originator if wider dissemination is required. There are four traffic light colors:

a. *RED* - personal for named recipients only: In the context of a meeting, for example, RED information is limited to those present at the meeting. In most circumstances, RED information will be passed verbally, in person or by secure email.

b. *AMBER* - limited distribution. The recipient may share AMBER information with others within their organization, but only on a 'need-to-know' basis. The originator may be expected to specify the intended limits of that sharing. The originator has to be informed of dissemination.

c. *GREEN* - community wide. GREEN information can be circulated widely within a particular community. However, it may not be published or posted publicly on the Internet, nor released outside the community.

d. *WHITE*- unlimited. Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.

64. The TLP can be used in conjunction with information classification models, such as the Priority Information Requirements (see Annex G) to relate kinds of information to releasability to access control.

Information Management Model

65. Decision-making is important for information sharing. A Hub and Node information sharing decision-making process is shown in Annex H. The quality of decision-making depends largely on the quality of available information. Quality is more than the integrity, completeness, timeliness and accuracy of the information, which often degrade over time. Information needs to be in a form that is rapidly consumable internally and externally. This requires both the business processes and information management processes to be as harmonised as possible.

66. Information isn't static – it has a lifecycle of at least four stages. AAA and information quality apply at each stage, both to changing and using the information.

a. *Creation.* It must be reliable.

b. *Update.* This is the period of use. Information must be accurate and have quality. Information is constantly evolving as a result of events and decisions elsewhere. For cyber SA, it is essential to validate relevant information and be confident it reflects the actual situation that the decision is trying to affect.

c. *Archive.* If the information has to be kept for legal, operational or business reasons, it must be securely archived and accessible as appropriate.

d. *Delete and purge.* Deletion is only temporary. Purging may be required for legal or national security reasons.

67. Key actions for information management include:

a. *Type of information*: decide what types of information are important to supporting each major business process.

b. *Taxonomy*: use a suitable taxonomy to categorise and classify all relevant information, so it can be analysed easily and accessed instantly under control at run time.

c. *Source and availability*: if specific information comes from multiple sources (multi-mastering), decide where the master information lies at any time and ensure its availability.

d. *Roles*: different roles have different information requirements in different circumstances. Use the same roles to manage external and internal user access for each type of information. Minimise the number of roles.

e. *Classification*: minimise the security classification of shared information where possible, to enable information sharing.

68. To ensure regulatory compliance, particularly for privacy, information should be anonymised but links should be retained so that identities can be revealed if there are grounds to do so. (See ISO/IEC 29191 – Partially anonymous, partially unlinkable authentication, available from national ISO bodies).

Generation and Maintenance of Cyber Situational Awareness

69. Cyber SA depends on all participating organisations managing their internal and shared cyberspace risks in compliance with agreed Common Policy. This requires two concurrent activities:

a. Risk Assessments internally and across the community of interest, using an agreed methodology, such as ISO/IEC 27000 series. This should cover:

(1) Policies (including legislation and regulations), procedures and mechanisms.

(2) Asset inventory – information, systems, devices, applications, indexes, taxonomies, metadata, users. Every asset should be known and trusted.

(3) Threats and vulnerabilities – internal, shared, external. Deliberate attack, insider threat, user negligence, non-compliant behaviour.

(4) Detection and prevention measures – network, information, users.

(5) Other counter-measures – deception, honey-traps, metadata extraction, cryptographic techniques etc.

b. Risk Mitigation strategies, including:

(1) Mandatory use of federated identity and access management.

(2) Monitoring of users, systems and information flows.

(3) Prevention of any policy violations. Enforcement action against any violations.

(4) Resilience to prevent any threat or vulnerability affecting business continuity or critical information resources.

(5) Constant improvement to address any changes or weaknesses identified by the risk assessments.

70. Cyber SA is generated and maintained from pooling and sharing information regarding:

a. Physical world status information;

b. Prevention status information based on the Security Controls;

c. Threat & Vulnerability;

d. Planned changes;

e. Incident management.

71. Establishing Cyber SA requires information from many different sources. The degree of analysis and fusion will vary according to timeliness, urgency and impact. For example, information has context and bias built in. When collecting data from multiple sources on the same subject, the analysis needs to reduce or eliminate this bias in order to increase confidence in the results. The outputs, which vary from small notifications and alerts through to complex analysis documents, inform different decision-makers at different levels (operating, tactical, operational, strategic) in a usable format and within an acceptable timeframe.

Information Preparation

72. Information has to be prepared before decisions can be taken on its release:

a. Data collection and gathering from multiple sources, ranging from general preventative monitoring of users and systems, through to targeted intelligence-led surveillance.

b. Data analysis, synthesis and clarification.

c. Put data into the information sharing context (formatting and anonymisation).

d. Information processing.

e. Information classification and filtering, including censoring data from within the federation to facilitate any caveats on releasability. This requires taxonomy.

f. Information publication or distribution.

73. Shared cyber SA information needs to meet a number of quality criteria:

a. *Timeliness.* Information, especially vital information, needs to be shared as quickly as possible in order to provide decision-makers with the fastest and the most recent information to take necessary and adequate action. A Prioritisation scheme, based on urgency, is being considered e.g.

(1) *Priority 4 – Critical priority*: Risk of national damage, loss of lives.

(2) *Priority 3 – Operational priority*: Risk of damage to critical national and international infrastructure.

(3) *Priority 2 – Planning priority*: Planning to prevent service interruption.

(4) *Priority 1 – Routine priority*: Other normal activities.

b. *Accuracy.* Information needs to be precise, including its origin and be to the point. It should identify and exclude false positives and negatives.

c. *Richness*. There needs to be a balance in the richness of information. Information needs to be as concise as it can be in order to prevent a decision-maker from an 'overload of information' leading to indecisiveness. However, the information needs to be detailed enough for a decision-maker to make well-founded decisions.

74. A scheme to measure the accuracy and richness of information is also required. A way to accomplish this is through subject matter expert (SME) validation at two levels:

a. *Validated*: This information has been reviewed by the appropriate subject matter experts and judged to be credible.

b. *Pre-Validated*: This information has NOT YET been reviewed by the appropriate subject matter experts and judged to be credible.

Types of Shared Information

75. Information is likely to be published in either a formatted report or as structured data. In both cases, taxonomy is required to enable interoperability and consistent use of information.

76. In general, the system operator incident reports should include:

a. Name of the source and target

b. Description of various aspects of the source and target

c. Description of the methodology used by the attacker

d. Identification of the creator of the incident report, and contact details

e. Source of each component of the incident report if it is different from the creator (e.g., the team handling the incident)

f. Description of the impact or potential impact of the incident

g. Description of the actions taken during the course of handling the incident.

77. An example of a report format is at Annex I. Examples of types of cyber SA information are shown at Annex J.

Recommendations

78. An Information Sharing Framework is a 'live' document and it will continue to evolve.

79. Based on the ideas put forward in the ISF of MNE7's Outcome 3 (Cyber) nations are encouraged to:

a. Endorse the implementation, operation and enforcement of the policies, procedures and mechanisms outlined in this ISF, so that organisations can achieve good cyber SA.

b. Support efforts by any future collaborative body to develop and maintain the information sharing, and related cyber SA documents.

80. Areas where future work may be needed include:

a. A federation common policy document, and

b. A standards-based ISF document or set of documents;

c. The development of an ISA template;

d. Establishing links with existing oversight bodies for accreditation, auditing, dispute resolution, etc, and establishing a new body or bodies where none exist;

e. The development of a common dashboard model that shows the status of each of the preventative Security Controls across a community of trust, plus major alerts and notifications for ongoing incident management.

Annex A – Controls for Security Operations Management

1. Detecting threats and vulnerabilities across organisations requires a common baseline view of normality, when everything is working correctly. This normality includes the correct operation of security controls for cyber defence - Controls for Security Operations Management (CSOM).

2. The controls are defined in three documents:

   a. Australian DOD Top 35 Mitigations (http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm). It mentions 35 controls.

   b. SANS CAG3 (http://www.sans.org/critical-security-controls/). It mentions 20 controls.

   c. NIST SP800-53 (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)

3. The differences in the number of controls results from differences in definitions rather than substance. The author organisations' concerns are similar. The strategic intention is to combine these controls in a single international document in due course.

4. Although all three documents overlap, with only minor differences, it is important to note that they derive from an enterprise risk model and do not yet take full account of federation requirements. All three assume the requirement for a full inventory of the approved information assets, network devices, applications and users. The SANS CAG3 includes comparisons of all three sets of controls.

5. The SANS CAG3 is based on a view of attacker activities and associated defences.

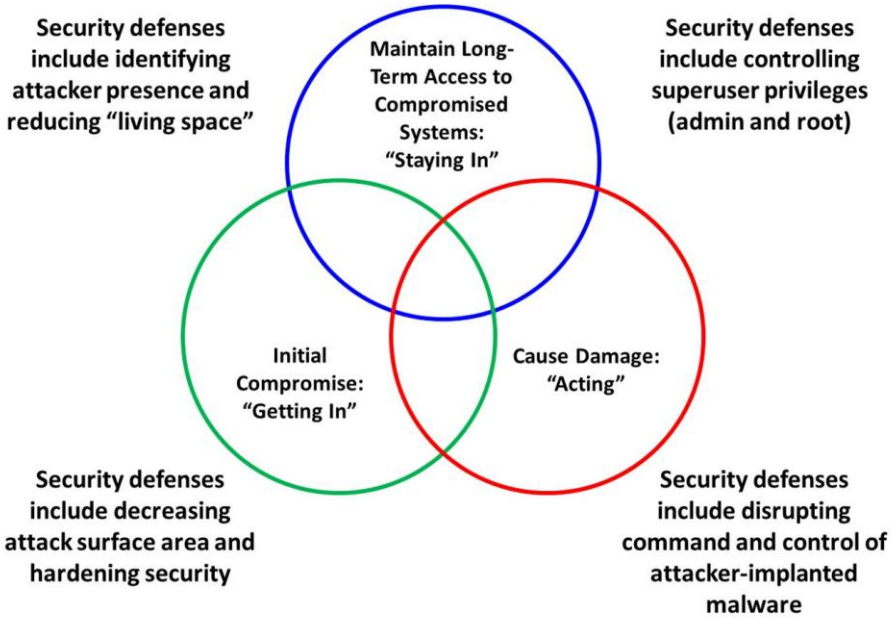


Figure 1: Computer Attacker Activities and Associated Defenses

6. The top 20 controls are as follows. The SANS CAG3 document provides details in each case:

   a. Inventory of Authorized and Unauthorized Devices

   b. Inventory of Authorized and Unauthorized Software

c. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

d. Continuous Vulnerability Assessment and Remediation

e. Malware Defenses

f. Application Software Security

g. Wireless Device Control

h. Data Recovery Capability (validated manually)

i. Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually)

j. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

k. Limitation and Control of Network Ports, Protocols, and Services

l. Controlled Use of Administrative Privileges

m. Boundary Defense

n. Maintenance, Monitoring, and Analysis of Security Audit Logs

o. Controlled Access Based on the Need to Know

p. Account Monitoring and Control

q. Data Loss Prevention

r. Incident Response Capability (validated manually)

s. Secure Network Engineering (validated manually)

t. Penetration Tests and Red Team Exercises (validated manually)

7. Work is ongoing through the TM Forum (www.tmforum.org) to combine the three documents into a single set of CSOM that can be mapped to the four Levels of Assurance. These can then be mandated in contracts and reflected in international standards.

Annex B - Benefits and Challenges to Information Sharing

Benefits

1. The numerous benefits of enhanced cyber SA through information sharing are of three types:

   a. *Reduced Risk.* Organisations can manage most, but not all, of their internal cyber risks, but they cannot manage shared cyber risks by themselves. By collaborating and sharing information, organisations reduce both their internal and external cyber risks.

   b. *Reduced Costs.* Organisations benefit from the collective action. Experience and knowledge from one organisation can be re-used by another without incurring additional cost. The overall cost of improving capability is shared, reducing costs to each individual organisation.

   c. *Increased Agility.* This same re-use can be applied across organisations and internally. Such agility enhances each organisation's effectiveness and its efficiency.

2. The ultimate result of an improved cyber SA is better prevention and more adequate responses to cyber threats. This also supports better decision making due to better (shared) information, for four reasons.

   a. *Quantity*: Sharing information and knowledge can lead to a better and more complete overview of all the developments in the cyber domain. A group knows more, collectively, and has more robust information than an individual.

   b. *Quality*: Sharing valuable, relevant and multi-source information can lead to better and more complete insights into the developments in cyberspace. Ultimately, this leads to better and more accurate information for decision-makers.

   c. *Timeliness*: Timely information sharing enhances cyberspace SA while enabling more complete preparation before malicious activity occurs or quicker responses once it does. The information system must take into account the need for real time information dissemination and the request for a repository/library for best practise and other documents, including non-technical issues such as legal.

   d. *Resilience*: Information remains available for community use even if one member is no longer participating.

3. Crisis response and incident handling: Collective crisis and problem reduction within the information sharing community. Incident handling process plays an important role within information sharing, as this process ensures that the information sharing process remains active in the event of an attack or breach. The founding and development of an information sharing community allows the members to gain a mutual understanding of each other. This understanding leads to more commitment to each other and the entire group, and sometimes even leading to sharing responsibilities. The ultimate result is that crises and problems among the members of the community will be collectively resolved. Establishing procedures and processes that pre-emptively detect and mitigate attacks or breaches, will assist in the recovery of compromised information systems. Crisis response plans are comprised of six phases:

   a. Preparation;

   b. Identification;

c. Containment;

d. Eradication;

e. Recovery;

f. Lessons Learned.

4. Additionally, the organization should have a cyber-information sharing continuity plan. This plan should ensure that the critical network hubs and nodes remain operational during an attack or breach. The plan should be executed in parallel with the recovery plan.

5. These are all cyber information sharing benefits. There are also second order benefits that appear at the business level, which contribute significantly to the overall business case for shared cyber SA.

Challenges

6. There are many types and categories of barriers that might hinder information sharing and these barriers need to be addressed and managed effectively. The issue is to determine how to overcome such obstacles as policy, culture, governance, resources, and technological restrictions, so that sharing of data and information is enabled, allowed, endorsed and encouraged throughout the extended enterprise.

a. Policy Barriers:

(1) Liability issues.

(2) Achieve global agreement.

(3) Policy issues could restrain systems inter-connection.

b. Management Barriers:

(1) Mechanisms may not be in place to allow for information sharing.

(2) The method for marking documents, even from one organization to the next within the same community lacks clarity and standardization. Red tape and other bureaucracy will lead to overregulation and prohibition of information sharing.

(3) Improved ways to stimulate dialogue are needed.

(4) Private sector needs to “practice what they preach” in demonstrating sharing of information.

(5) Unequal participation or fear of ‘free-riders’.

(6) Lack of or obsolete Service Level Agreements.

(7) Poorly informed, and understood decision making about the risks and benefits of participation. Senior management is usually of a different technological generation than the workers, so clear information passage can assist matters. They are usually not up-to-date on current threats and vulnerabilities.

(8) Lack of trust between participants.

c. Legal Barriers:

(1) Lack of a General Security Agreement: legislation, cyber meta laws, and other legal issues vary from nation to nation.

(2) Depending on the federation's agreed legal system (e.g. most restrictive, least restrictive) legal obstacles can be constraints as well as restraints.

(3) Information sharing depends highly on local / legal requirements (Freedom of Information Act (FOIA) issues, Personal privacy concerns).

(4) Policy issues could restrain systems inter-connection.

d. Business Barriers:

(1) Financial issues.

(2) No incentives of cooperating industry-wide.

(3) Time taken away from business activities.

(4) Competitive pressures increase the reluctance of companies to invest in info sharing.

(5) There is no built-in guarantee in the information sharing system that protects critical business information and prevents it from being leaked to competitors and the public.

(6) No direct return on investment.

(7) Vulnerability information is in most cases too commercialized to be effective for specific cases and incidents.

e. Resource Barriers (includes technological):

(1) Inefficient use of existing technologies.

(2) Need for available facilities to share and store information. Within modern data centers, the more info that is shared, then the more data must be retained and is generated in meta-data, and therefore the more hardware that is needed. The larger the facility to house it, the more power needed to run it. Large scale info sharing can be very costly for infrastructure, huge amount of data.

(3) Technology itself, many systems simply cannot inter-connect due to various technological issues. Properly designed and implemented systems will not generate a technological barrier. Although, organizational restrictions placed upon the use of technology can form barriers.

(4) Barrier management must begin in the design of the technology system that delivers the information.

(5) Systems using incompatible computer programming languages. Every program designed to operate in a specific operating system environment would qualify. Areas of consideration would be, for example, MS Access vs. Oracle formats, and database field formats.

(6) No common lexicon -taxonomy (operational, legal, technological etc. terminology).

(7) Unavailability of knowledgeable, experienced employees to support relevant business processes.

(8) Incompatible encryption technology due to different government regulations.

f. Confidentiality Barriers:

(1) Issues with anonymity, confidentiality and proprietary information.

(2) Culture of secrecy within Government.

(3) Sharing information with non-cleared executives who do not have proper credentials for information access within private sector federations.

(4) Potentially embarrassing information.

(5) Over-classification.

(6) No specific regulations for accountability.

g. Humanistic / Cultural Barriers:

(1) Diversity across participants (culture, language, legal systems, etc.). Cultural context is everything in data analysis. Misinterpretation of data can cause severe issues.

(2) One natural or sociological constraint to federation is that individuals tend to work alone.

(3) Some communities, e.g. security organizations, do not have a history and a reputation for sharing information.

(4) One way street syndrome which will take place in reality in contrast to the considered genuinely respected two way stream by all involved parties.

h. Risk Barriers:

(1) There are some real challenges associated with more information sharing, especially in regards to classified information. Due to the risk of information leak, Intelligence services are often reluctant to share sensitive information. By sharing information with anyone other than purely equal (& allied) organizations, one must be prepared for the information to be leaked to the media and made public. With today's access to information through electronic media this can happen quickly and become a threat to operational security.

(2) Another danger of greater information sharing is that the sharer decides what is shared and who gets it. The author, or originating organization, defines a documents security caveat. The result can be sub-environments within operations that share between different systems (for example, 3-4 eyes only). This risk must be weighed against the possible benefits of greater information sharing.

(3) For the private sector, companies are prohibited through laws from divulging certain information and reluctant to share details about its operations for fear of leaks to competitors. Such fears must be allayed through building of trust and established guidelines for public-private partnerships.

(4) Information asymmetries: critical parties in an information sharing community are not sharing the same level or set of data.

(5) Information unavailability: some participants in the information sharing community might lack the means to research a cyber-incident leading to a delay in incident response and incident reporting.

(6) Information misuse: Leaks in the information sharing system might lead to availability of (secured) information to unauthorized entities. Likewise a wide dissemination might lead to information misuse.

(7) Information overload: Too much information gathered - sometimes in combination with irrelevant information - might lead to indecisiveness or dismissal of the information received.

Annex C - Main functions of Hub & Node during an incident

Function	Nodes	Hubs
Incident management	Yes	No, only strategic
Vulnerability coordination	Yes	Yes
Data repository	Limited	Yes
Alert	Yes (support)	strategic coordination between hubs and nodes
Triage & Analysis	Organisational communication	strategic triage
Reporting	yes, originate, share (Post Incident Report)	yes, originate & share, lessons learned, policy change
Prevention, Trust fabric-Federation controls, Taxonomy	Yes, integrate (from Hub), create, spread and enforce.	Yes, create, spread and enforce (nodes /hubs level).
Responsibility	Maintain Information Sharing Agreements Ensure info quality within the node Communications with hubs and nodes Support orgs for all stages and operational readiness	Maintain Information Sharing Agreements Operate information repository Ensure maintenance of information quality Ensure communications between hubs and support for nodes
Decision (authority)	membership of community / organisations	membership for nodes, inter hubs agreements Enforcement decisions, including revocation, law enforcement involvement, criminal investigation, trust restoration and commendations for legal and regulatory changes
Policy	Behaviour, best practice, way of working, standards, certification, enforcement	Behaviour, best practice, way of working, standards, certification, enforcement

Annex D – Information Sharing Agreements

1. A community should have an Information Sharing Agreement (ISA), which describes what information can be shared, how it should be shared and the overall governance to ensure compliance. For example, an ISA should aim:

   a. To guide Partner Organisations on how to share personal and sensitive information lawfully.

2. To explain the security and confidentiality laws and principles of information sharing.

3. To increase awareness and understanding of the key issues.

4. To emphasise the need to develop and use Information Sharing Agreements.

5. To support a process that will monitor and review all information flows.

6. To encourage flows of information.

7. To protect the Partner Organisations from accusations of wrongful use of personal or sensitive information.

8. To identify the legal basis for information sharing.

9. To address any liability issues.

10. Example ISAs cover various requirements for sharing sensitive information:

11. Leicestershire County Council Information Sharing Protocol, which is focused on sharing sensitive and privacy information. Many UK local government and police organisations have similar agreements.
http://www.leics.gov.uk/information_sharing_protocol.pdf

12. US DOD is defining an ISA template for cyber information sharing with the Defense Industrial Base (DIB).

Annex E – Federation and Levels of Assurance

1. Each Level of Assurance (LoA), defined in international and national standards, describes the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity claiming a particular identity is in fact the entity to which that identity was assigned. For the purposes of this ISF, LoA is a function of the process and technical controls that have been implemented by each Credential Service Provider (CSP), Identity Providers (IDP) and Identity Proofing & Verification Provider (IPVP) for each entity.

2. In a federation model, all providers (CSP, IDP, IPVP) and user organisations comply with the federation common policy that underpins federated trust.

3. Four Levels of Assurance are defined in ISO 29115 based on US SP800-63-1 and US OMB (Office of Management and Budget) M0404. They are:

   a. *LoA 1 – Low Assurance*. Little or no confidence in the asserted identity. This usually involves self-assertion and is most commonly used in social networking.

   b. *LoA 2 – Medium Assurance*. Some confidence in the asserted identity. This usually involves the local validation of some form of government-issued ID but only to satisfy Anti-Money Laundering (AML) legal requirements for consumer financial activities.

   c. *LoA 3 – High Assurance*. High confidence in the asserted identity. This usually involves greater validation of some form of government-issued ID with face-to-face interaction. The primary use case is employee authentication, particularly in regulated industries and government organisations.

   d. *LoA 4 – Very High Assurance*. Very high confidence in the asserted identity. Additional processes and controls are applied. The primary use cases involve danger-to-life and national security situations.

4. Four types of entities can be authenticated:

   a. *People*: Citizens, consumers, government employees, industry employees.

   b. *Organisations*: All credentials are affiliated to an organisation in some way, so an organisation has to be trusted to the same LoA as the credential.

   c. *Devices*: Computers, laptops, smartphones, storage, network devices etc. Trusted Platform Module (TPM) is the dominant standard and widely deployed, if underused. TPM is also used to ensure BIOS health and to defeat malware in the BIOS and operating system.

   d. *Software*: Secure Content Automation Protocol (SCAP) is the standard for validating software and its provenance.

5. MNE7's main interest is in LoA 3 and 4 to ensure:

   a. The protection of LoA 3 and 4 federated authentication systems.

   b. All staff involved in Cyber SA possess and use compliant LoA 3 or 4 credentials to authenticate in the course of sharing sensitive information.

6. Public Key Infrastructure (PKI) is the dominant technology for High Assurance federated authentication. Such PKI federation requires the existence of one or more PKI bridges to enable different PKI credential providers to trust each other's credentials. Some nations and industries are already operating PKI bridges to enable a mesh of trust across international

supply chains and government organisations. The sharing of cyber SA depends on nations adopting PKI federation. See http://www.idmanagement.gov.

Annex F – Taxonomies for Cyber SA Information Sharing

1. Various taxonomies exist for cyber SA information sharing, but most are either not suitable or take no account of federation requirements. Two approaches are of interest.

   a. ENISA is developing at least two taxonomies, either of which might prove useful. The current ENISA taxonomy is described in the Good Practice Guide for Incident Management. http://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management

   b. IETF's IODEF (Internet Engineering Task Force, Incident Object Description Exchange Format) RFC 5070. http://www.ietf.org/rfc/rfc5070.txt. This is currently the standard that will likely to evolve to meet MNE7's taxonomy requirements, in IODEF V2, for the higher level Hub and Node collaborative approach to cyber SA.

IETF IODEF

2. Organizations require help from other parties to mitigate malicious activity targeting their network and to gain insight into potential threats. This coordination might entail working with an ISP to filter attack traffic, contacting a remote site to take down a bot-network, or sharing watch-lists of known malicious IP addresses in a consortium.

3. The IODEF is a format for representing computer security information commonly exchanged between Computer Security Incident Response Teams (CSIRTs). It provides an XML representation for conveying incident information administrative domains between parties that have an operational responsibility of remediation or a watch-and-warning over a defined constituency. The data model encodes information about hosts, networks, and the services running on these systems; attack and associated forensic evidence; impact of the activity; and limited approaches for documenting workflow.

4. The overriding purpose of the IODEF is to enhance the operational capabilities of CSIRTs. Community adoption of the IODEF provides an improved ability to resolve incidents and convey situational awareness by simplifying collaboration and data sharing. This structured format provided by the IODEF allows for:

   a. increased automation in processing of incident data, since the resources of security analysts to parse free-form textual documents will be reduced; decreased effort in normalizing similar data (even when highly structured) from different sources; and

   b. A common format on which to build interoperable tools for incident handling and subsequent analysis, specifically when data comes from multiple constituencies.

5. Coordinating with other CSIRTs is not strictly a technical problem. There are numerous procedural, trust, and legal considerations that might prevent an organization from sharing information. The IODEF does not attempt to address them. However, operational implementations of the IODEF will need to consider this broader context.

6. About the IODEF Data Model.

   a. The IODEF data model is a data representation that provides a framework for sharing information commonly exchanged by CSIRTs about computer security incidents. A number of considerations were made in the design of the data model.

   b. The data model serves as a transport format. Therefore, its specific representation is not the optimal representation for on- disk storage, long-term archiving, or in-memory processing.

c. As there is no precise widely agreed upon definition for an incident, the data model does not attempt to dictate one through its implementation. Rather, a broad understanding is assumed in the IODEF that is flexible enough to encompass most operators.

d. Describing an incident for all definitions would require an extremely complex data model. Therefore, the IODEF only intends to be a framework to convey commonly exchanged incident information. It ensures that there are ample mechanisms for extensibility to support organization-specific information, and techniques to reference information kept outside of the explicit data model.

e. The domain of security analysis is not fully standardized and must rely on free-form textual descriptions. The IODEF attempts to strike a balance between supporting this free-form content, while still allowing automated processing of incident information.

f. The IODEF is only one of several security relevant data representations being standardized. Attempts were made to ensure they were complimentary. The data model of the Intrusion Detection Message Exchange Format influenced the design of the IODEF.

7. A draft document - IODEF-extension to support structured cybersecurity information – is being developed to extend IODEF to facilitate enriched cybersecurity information exchange among cybersecurity entities. It provides the capability of embedding structured information, such as identifier- and XML-based information, in such a way that will facilitate automation and system-system interaction.

Annex G - Priority Information Requirements[1]

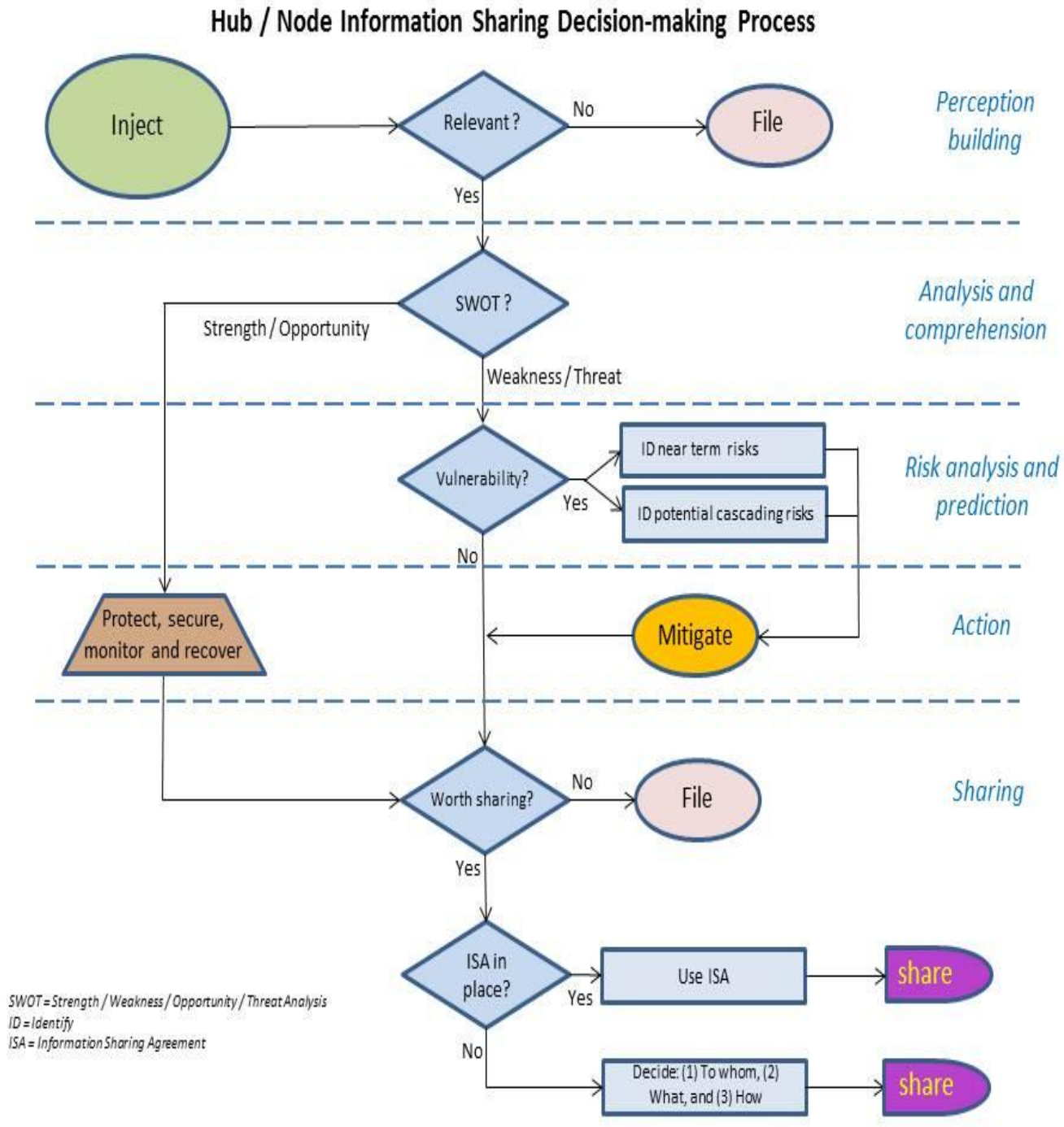
As introduced in the “Information Release – Traffic Light Protocol (TLP)” section (earlier), The TLP can be used in conjunction with information classification models, such as the Priority Information Requirements (PIRs) to relate kinds of information to releasability and to access control. The US CERT published PIRs are described here:

- *PIR 1*: Successful compromise of account or network.
- *PIR 2*: Successful exfiltration of data.
- *PIR 3*: Successful SQL injection.
- *PIR 4*: Successful root compromise of network.
- *PIR 5*: Successful compromise of any national leadership (president or prime minister) website or account.
- *PIR 6*: Success denial-of-service (natural or manmade) of any department, agency or critical government or industry asset, to include major infrastructure of any foreign government.
- *PIR 7*: Newly discovered malware affecting three or more departments, agencies or major government or industry organisations.
- *PIR 8*: Confirmed Zero Day exploit.
- *PIR 9*: A 100% or significant increase in incident reports from departments, agencies or key government or industry organisations, when compared to the average number of reported incidents. (Take into consideration the value of the average number).
- *PIR 10*: Web defacement of departments, agencies or major government or industry organisations.
- *PIR 11*: Malware impacting at least 50 workstations.
- *PIR 12*: Confirmed loss of cyber PII (Personal Identity Information) data for at least 5,000 individuals
- *PIR 13*: Loss of power in any Node, Hub, CERT, CSIRT or major cyber defence organisation.
- *PIR14*: Nuclear, biological, chemical or any other attack to any government department, agency or major organisation’s asset.
- *PIR 15*: Email from adversarial foreign governments or entity. (Advice from Hub required for before responding).

---

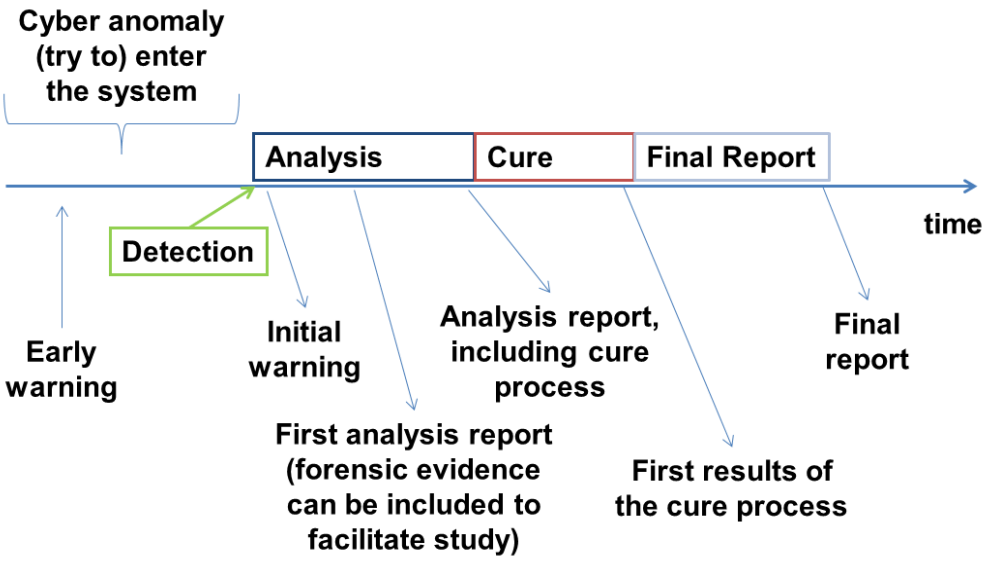
[1] Based on US CERT Priority Information Requirements

Annex H – Hub / Node Information Sharing Decision-making Process



Annex I – Generic Report Format for Information Sharing

Time frame for reporting:



Example of a final report:

From:

To:

DTG:

Location/Nation:

Description of incident:

- Target:
- Name and description source
- Used methodology by attacker
- Description of impact

Consequences:

- Direct effects
- Indirect (2nd and 3d order) effects
- Actions taken during the attack

Required follow-up action:

Assistance needed:

Acknowledge:

Name:

Position:

Organization:

Authentication: (Formulating Official)

Annex J – Types of Information

1. A wide range of cyber SA information is required, covering three major information components:

   a. How to build and govern a cyber defence community (stakeholder, risks, selection),

   b. How to ensure normal operation of cyberspace and prevent disruption,

   c. How to detect and manage incidents across the community and beyond.

2. Information relevant to normal operation and resilience include:

   a. Security Quality Management:

      (1) Methodology for enhancing cyber-resilience;

      (2) Business continuity and disaster recovery;

      (3) Security consulting reports;

      (4) Awareness building;

      (5) Education and training;

      (6) Product evaluation / certification;

      (7) Lessons Learned;

      (8) Management and Structure of information sharing.

   b. Prediction: Most information sharing participants would like to have predictions for their networks based on a mixture of current knowledge, historical analysis, trend monitoring and early warnings: “When are incidents likely or about to occur?”

   c. Some information might be based on best practice and lesson-learning of activities in the cyberspace domain, by:

      (1) Longer-term trend analysis of cyber threats (Identify developing trends; Drivers/motivating factors; Evolution),

      (2) Analysis of global threat trends

      (3) Experiences of allies and partners

3. Detection and management of incidents:

   a. Alerts on threats:

      (1) Incidents, product technical vulnerabilities and risks, protocol vulnerabilities, network intrusion information, probing attacks and network configuration issues that can be undisclosed or unpatched, contingency planning.

      (2) Alerts, descriptions and analysis of current cyber threats, enriched by global data.

      (3) Regular and reactive threat reporting.

      (4) Information on single points of failure, dependencies, crisis management arrangements, incidents, exercises, etc.

   b. Proactive (Push) information:

      (1) Security-related information dissemination.

      (2) Announcements on all sorts related to Cyber Security.

(3) Trends / Early Warning.

(4) Security audits and assessments, including analysis of malicious activity (malicious identities, assumed intent of the attacker, etc.)

(5) Advices:

(a) Technology Watch.

(b) Legal developments.

(c) Configuration and maintenance security.

(d) Development of security tools.

(e) Intrusion detection services.

(f) Vulnerability assessment and handling.

(g) Vulnerability response and mitigation.

(h) Management Information.

(i) Best Practices and Processes.

c. Reactive / During Incident (Pull) information:

(1) Automated CERT surveillance system exchange mechanism, monitoring activity 24 hours a day.

(2) Alerts and warnings.

(3) Triage (the action of gathering all the incidents and prioritize them to ensure the most relevant are disseminated).

(4) Incident handling.

(5) Incident analysis: Incident response support and coordination (begin System Recovery).

(6) Incident response on site (takedown, for example) and notification

(7) Lessons Learned.

(8) Impact Analysis.

d. Artefact Handling (Proactive): Digital Artefacts are described as an anomaly introduced into digital signals as a result of digital processing (e.g. malware changing the code of a system program). One of many kinds of tangible by-products (secondary products) produced during the development of software.

(1) Artefact analysis and handling.

(2) Artefact response coordination.

(3) Lessons Learned.

Glossary

AAA:	Authentication, Authorisation, Accountability
Anonymisation:	Techniques to convert personal/organisational data into a form that is no longer identifiable
CAI:	Confidentiality, Availability and Integrity
CERTs:	Computer Emergency Response Teams
CIRCs:	Computer Information and Resource Centres
CSIRTs:	Computer Security Incident Response Teams
CSOM:	Controls for Security Operations Management
CSP:	Credential Service Provider
Cyber SA:	Cyber Situational Awareness
EAL:	Evaluation Assurance Level
ENISA:	European Network and Information Security Agency
EC:	European Commission
EU:	European Union
EUROPOL:	European law enforcement agency
Federation:	Shared use of common policies, procedures and mechanisms, which are based on international standards.
GC:	Global Commons
IDP:	Identity Providers
IEC:	International Electrotechnical Commission
IETF:	Internet Engineering Task Force
IODEF:	Incident Object Description Exchange Format
IPVP:	Identity Proofing & Verification Provider
ISA:	Information Sharing Agreement
ISF:	Information Sharing Framework
ISO:	International Organisation for Standardization
ISP:	Internet Service Provider
ITU:	International Telecommunications Union
JP:	Joint Publication
LoA:	Level of Assurance
MNE 7:	Multinational Experiment 7
NATO:	North Atlantic Treaty Organisation
NIST:	National Institute of Standards and Technology
OMB:	Office of Management and Budget
PIR:	Priority Information Requirements
PKI:	Public Key Infrastructure
SA:	Situational Awareness
SANS CAG3:	The SANS Institute is a private US company that specializes in

	internet security training. Twenty Critical Security Controls for Effective Cyber Defence (commonly called the Consensus Audit Guidelines or CAG)
SP:	Special Publication
T&V:	Cyber Threats and Vulnerabilities
TLP:	Traffic Light Protocol
TTP:	Trusted Third Party
UK:	United Kingdom
WARPs:	Warning, Advice and Reporting Points