**Table of Contents**

## 1. Introduction

The 2011 Standard of Good Practice for Information Security (SOGP) has been published by the Information Security Forum (ISF) as an international reference source for information security. It comprises tools, techniques and best practices, organizations could adhere to when planning and designing the information security approaches. SOGP not only helps to identify and manage information security risks inside organizations but also within their supply chains as well. These best practices help the companies meet the requirements of global standards like ISO, COBIT, NIST, ITL, and PCI/DTS. The following report includes a description of policy statements covering two selected subdomains CF9.2 Physical network management and CF9.5 Remote maintenance from the controls of SOGP 2011. Further, it includes proposals for strategic and execution plans to implement the selected policies in an organization.

An attack tree is a graphical representation of how an attack might succeed; hence it helps the analysis of possible threats to information systems. This report also includes an attack tree assuming that an information system being designed is vulnerable to stealing and destruction. A brief description of two possible attacks based on the attack tree is described further. As the final section of the report, a summarization of the federal law, Cybersecurity Information Sharing Act (CISA) has been included.

## 2.The ISF and SOGP 2011.

The ISF is an independent body on information security and risk management. As a non-profit organization, it provides tools, techniques, and best practice guidelines on all areas of information security. ISF issues various products, from guidelines, tools, activities to research-based publications. SOGP is one of such products by ISF which focuses on identifying information security risks and how to manage them in organizations and within the supply chains as well. ISF is a paid membership organization and SOGP is updated annually. SOGP 2011 is based on analysis of a wide range of material, in-depth research, and the extensive knowledge and practical experience of ISF Members worldwide (Chaplin & Creasey, 2011). The main inputs to SOGP 2011 were an extensive work program involving the expertise of a full-time ISF global team, that performs research into hot topics in information security (Chaplin & Creasey, 2011), analysis and integration of information security-related standards, and legal and regulatory requirements (Chaplin & Creasey, 2011) and inputs from ISF Members.

While developing SOGP 2011 many information security-related standards were reviewed such as several series of ISO/IEC, BS 25999-1, COBIT v4.1, PCI DSS v2.0, Cloud Security Alliance (CSA) Controls Matrix, IT Infrastructure Library (ITIL) V3…etc. SOGP 2011 identified 50 types of information security threats that can have a significant impact on a business. These threat types are used in ISF's Information Risk Analysis Methodology (IRAM) and Benchmark tool (Chaplin & Creasey, 2011) to gather data about information security levels of organizations. According to the results, relevant security controls are selected to mitigate the risks.

The SOGP is presented in a modular format as well as in an aspect format. As mentioned in the report published by ISF, the default format for 2011 standards is modular. In the modular format, the best practices presented in SOGP 2011 are formed into four categories as security governance, security requirements, control framework, security monitoring, and improvement. These four are subdivided into 26 higher-level areas and further into 118 topics. In the aspect format, the best practices are presented in a more granular pattern, grouped into six major categories. The aspect format also consists of the same topics grouped into the six major categories however some topics are duplicated across the aspects.

2011 standard identifies the topics into another distinction as fundamental topics and specialized topics. This categorization identifies controls that are universal to businesses as fundamental and controls that are specialized only to some organizations as specialized.

### 2.1. Selecting the sub-domain and area of controls from SOGP 2011

Depending on all the above information, two topics (sub-domains) are selected for this report from the Modular format.

The first sub-domain is CF9.2 Physical network management from the category of Control Framework and area of Network Management. This subdomain belongs to the type of 'Fundamental' which indicates the controls under this sub-topic are universal to all businesses.

The second sub-domain is CF9.5 Remote maintenance from the category of Control framework and area of Network Management. This subdomain belongs to the type of 'Specialized' which indicates the controls under this sub-topic are specialized to some businesses.

## 2.2. Policy statements for the selected controls.

CF9.2 Physical network management

What controls need to be applied for this subdomain is stated in the Principle section of ISF the report. According to that, all the networks including voice networks need to be protected and should be documented and labeled accurately. The process should be continuous and the documentation and labeling should be up-to-date. The protection should be in the means of physical controls such as locked rooms, cabinets, identification labels, ...etc.

The objective of this subdomain or the reason why these controls need to be in place is described in the Objective section of the ISF report. According to that, these control measures will ensure that all networks are configured correctly and is secured. Further, it will give the employees a clear statement of the security policies they are expected to follow.
This subdomain has four individual statements which define the security controls that need to be applied. Following all the above guidelines the policy statements for the controls in the CF9.2 section are as follows.

- Protection of telecommunication cables – This section includes policies that should be adhered to when managing telecommunication cables.

1. Attach identification labels to communications equipment and cables
2. Cabling must always be concealed when installing.
3. Use armoured conduit for cabling.
4. Inspection and/or termination points should always be locked.
5. To prevent cable failure, provide alternative feeds or routing.
6. When cabling, avoid routes through publicly accessible areas.

- Protection of network access points - This section includes policies regarding network access points.

1. Locate the network access points in secure environments.
2. Disable the devices on the network until it is required or used.

- Supporting the networks with documentation - This section includes policies regarding documentation related to networks' software, hardware, and peripheral devices.

1. Produce network configuration diagrams depicting nodes and connections in the network.
2. Document the details about services and software provided by external parties with links (if available).
3. Document the inventory of communication equipment provided by the third party suppliers.
4. Prepare and maintain documents about in-house cable runs for all physical locations.
5. Document settings and configurations on in-house telephone exchanges and cabling/wiring for telephones.

- Managing the documentation – This section includes policies for managing the documentation.

1. The document should be kept up to date.
2. Documents should be readily accessible to authorized individuals.
3. Documents should be supervised and reviewed continuously and timely by supervisors.
4. Use software and tools to generate documentation.

CF9.5 Remote maintenance

The Principle section of ISF the report for this section describes what controls need to be applied regarding remote maintenance of critical systems and networks. According to that, maintenance of such systems should be restricted to authorized personnel and should be subjected to reviews. Also, the sessions related to the maintenance of critical networks should be confined to authorized individuals rather than groups of individuals.

The objective of this subdomain or the reason why these controls need to be in place is described in the Objective section of the ISF report. According to that, these control measures will prevent unauthorized access to critical systems and networks through the misuse of remote maintenance facilities.

This subdomain has four individual statements which define the security controls that need to be applied. Following all the above guidelines the policy statements for the controls in the CF9.5 section are as follows.

- Managing the access of external individuals – This section includes policies that should be adhered to when managing access of external individuals to critical systems and networks for maintenance purposes such as testing, remote debugging, and software updating.

1. Clearly define the objectives and scope of the work and make agreements on the work plan before starting.
2. Authorize sessions individually.
3. Give only the required privileges to access systems to perform the planned work.
4. Document and log all the activities taking place while the remote session is conducted.
5. Revoke privileges and reset passwords immediately after the planned sessions are over.
6. Review independently about the session conducted considering the outputs and future security of the systems.

- Managing the Diagnostic ports – This section states the managing of diagnostic ports.

1. Protect the diagnostic ports used for maintenance for the network using physical locks or passwords.

- Initiating and maintaining agreements – This control is about agreements made before maintenance sessions.

1. Prepare non-disclosure agreements or confidentiality clauses.
2. Obtain the agreement signatures from third parties.
3. Incorporate the agreements into the employment contracts.

- Protection of dial-up connections – This section is about protecting dial-up connections using dial-back security which can verify the source of dial-up connections.

1. Configure mandatory dial-back to verify the source of the connection.
2. Disconnect the host to temporally suspends all monitoring activities.
3. Disable call forwarding for the dial-back line.

**2.3 Strategic and execution plans to deploy the above policies for an organization**

Before the formation of an execution plan, it is needed to define important roles related to information technology ad information security of the organization and their responsibilities to define and handle strategic plans.

**1. Defining the roles and responsibilities.**

Chief Information Officer (CIO)

The Chief Information Officer has overall responsibility for the security of the organization's information technology. Implementation of security policies is delegated throughout the organization to various services, departments, and other units under CIO's direction. The organization must clearly define the responsibilities under CIO before developing a policy execution plan.

Chief Information Security Officer (CISO)

The Chief Information Security Officer is responsible for the overall data and information security of the company. The physical, network, and software security of the organization comes under CISO's direction. While CISO is responsible for overall data security, CIO is overlooking the security of information technology systems. Therefore, a fine line between the responsibilities of the CIO and CISO should be defined.

Information Technology Security and Policies Team

This team is responsible for the security of the services provided by the IT teams. The policies formed by the team must ensure the protection of all the software, hardware, networking, and data resources throughout the process in the organization and within the supply chains as well.

Computer Security Incident Response Team (CSIRT)

The responsibility of responding to potentially catastrophic events and significant security risks faced by the systems in the organization is on the CSIRT team. This team must be able to respond quickly and effectively to guide the management and employees to prevent or minimize the damage in any critical situation.

Once the chief roles and responsibilities are defined, it is needed to delegate the responsibilities to middle and lower-level management so that every employee from top to bottom is aware of their responsibilities precisely.

**2. Aligning information security with strategic plans**

The higher management must decide on how the information technology security should align with the overall strategic plans of the organization. The timelines, roles, and responsibilities need to be defined with the goals, vision and mission kept as final targets.

After all the preparation and planning, the relevant execution steps for CF9.2 Physical network management can be listed below.

<u>CF9.2 Physical network management- Execution Plan</u>

| Implementation Task | Action Steps |
|---|---|
| Protection of telecommunication cables | Make a cabling plan depicting the nodes, switches, cables, and other endpoints.<br>Plan for secure concealing process and use armoured conduit for cabling.<br>Do the cabling avoiding publicly accessible area routes.<br>Identify and list all the communication equipment and cables.<br>Attach identification labels to the listed equipment and cables.<br>Create facilities for locked spaces and once the execution happens keep the termination points and inspection points in the locked spaces.<br>Once the<br>Make a plan for alternative feeds or routing and keep it up-to-date. |
| Protection of network access points | Identify all the access points to the network.<br>Locate the network access points in secure environments such as locked rooms or cabinets.<br>Monitor timely and disable the devices on the network using network switches until they are required or used. |
| Supporting the networks with documentation | Produce configuration diagrams with all the nodes and connections as in the network layout and keep it up-to-date.<br>Identify the need to obtain third-party tools or services.<br>Document the third-party details with links if available and monitor it frequently. |

| | |
|---|---|
| | List all the in-house inventory of communication equipment.<br>Keep the third-party equipment documented and up-to-date.<br>Prepare documents and diagrams about in-house cable runs for all physical locations.<br>Document settings and configurations on in-house telephone exchanges and cabling/wiring for telephones. |
| Managing the documentation | Assign responsibilities for personnel to keep the documents up-to-date and keep them under supervision to maintain quality.<br>Use tools and technologies to make the documents readily accessible to authorized individuals.<br>Keep the documents supervised and reviewed continuously and timely by supervisors.<br>Use software tools to generate documents other than building them from scratch by the staff.<br>Research and find the newest software/tool that is applicable and suggest them in frequent meetings.<br>Keep the documentation alive while maintaining an archive of information for outdated documentation. |

The execution plan for CF9.5 Remote maintenance is as below.

CF9.5 Remote Maintenance - Execution Plan

| **Implementation Task** | **Action Steps** |
|---|---|
| Managing the access of external individuals | Make a cabling plan depicting the nodes, switches, cables, and other endpoints.<br>Plan for secure concealing process and use armoured conduit for cabling.<br>Do the cabling avoiding publicly accessible area routes.<br>Identify and list all the communication equipment and cables.<br>Attach identification labels to the listed equipment and cables.<br>Create facilities for locked spaces and once the execution happens keep the termination points and inspection points in the locked spaces.<br>Once the<br>Make a plan for alternative feeds or routing and keep it up-to-date. |
| Managing the Diagnostic ports | Make a list of diagnostic ports and identify them with unique ids.<br>Keep the ports is a place where physical locks available for security.<br>Secure the ports with passwords. |
| Initiating and maintaining agreements | Prepare non-disclosure agreements or confidentiality clauses consciously and precisely aiming at the maintenance activities and privileges granted to external parties.<br>Obtain the agreement signatures from third-party information security and information technology staff personnel before the remote maintenance begins. |

| | |
|---|---|
| | Incorporate the agreements into the employment contracts before the planned work and ensure it is completed before granting access to networks. |
| Protection of dial-up connections | Make lists and keep tracking of the accounts that are authorized to connect through an access point.<br>Configure mandatory dial-back to all the authorized accounts to verify the source of the connection.<br>Monitor the usage of lines and disconnect the line at the hosts (not the clients) so that it temporally suspends all monitoring activities and assures more security to the system.<br>Disable call forwarding for the dial-back line. |

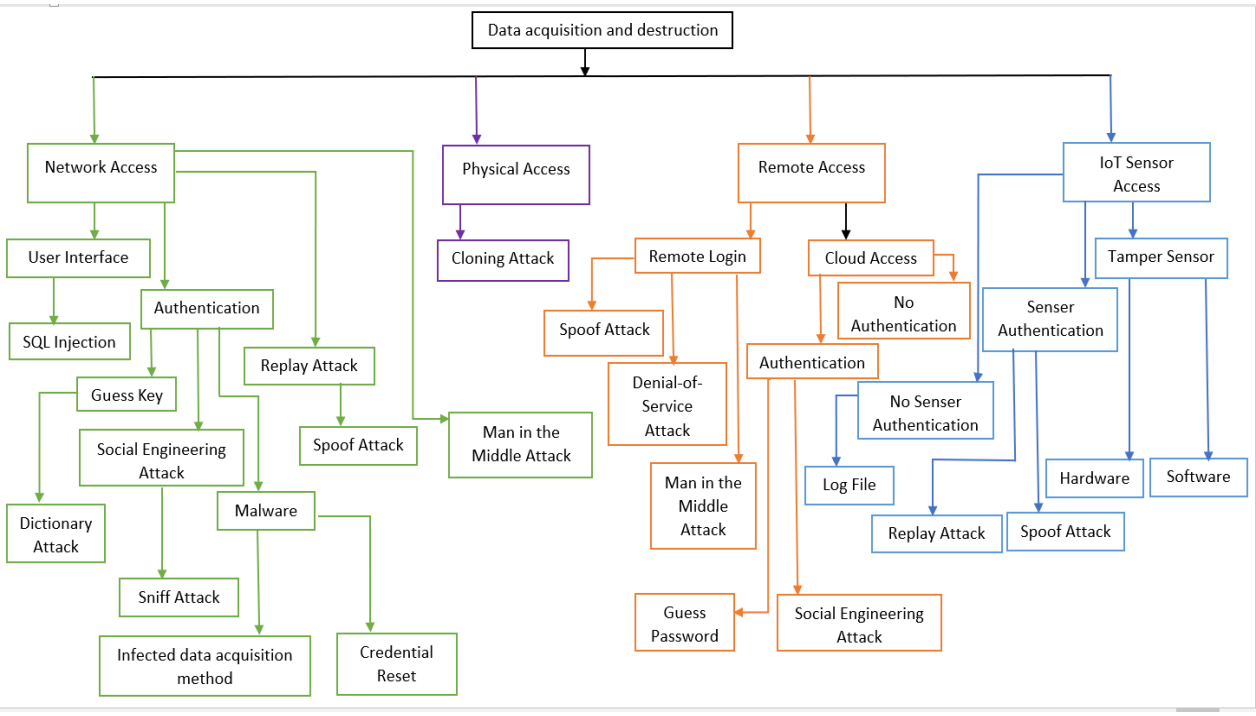
## 3. An attack tree on stealing and destruction of information.

### 3.1 Introduction

An attack tree is a way to understand an attack from the perspective of an attacker. Attack trees provide a methodical way of representing the security of systems. They allow you to make calculations about security, compare the security of different systems, and do a whole bunch of other cool things (Schneier, 2004). It is an attack against a system represented in a tree structure with the goal as the root node and different ways of attack as branches of the tree. By assigning values to nodes, calculations can be made if needed. The values can be "yes" or "no", "possible" or "impossible", "easy" or "difficult", "expensive" or "inexpensive", or any other values depending on the nature of the attack. To create an attack tree, it is needed to identify attack goals at the first step. The attack goal makes a separate attack tree. After identifying the goal, identification of different methods to reach the goal must take place. Each method is added to the tree. This is a recursive process, brainstorming the possibilities and adding and modifying the tree until all the areas are covered.

### 3.2 Attack tree representation

Following is the attack tree is drawn against stealing and destruction of information and data of the organization.




### 3.3 Brief description of two possible attacks.

Sniff Attack

Sniffing in general terms means investigating something secretly to access sensitive and restricted information. In the field of information security and specifically in network security sniffer attack or sniffing attack means capturing network traffic using packet sniffer software to steal or interpret data in the network packets.

There can be several reasons for sniffer attacks such as identity theft, obtaining usernames and passwords, spying on messages, getting access to confidential information, etc. Sniff attack can be of two ways; passive sniffing and active sniffing. Passive sniffing can happen in the networks connected via hubs. Hubs receive network traffic at one port and transmit it to other ports. Hence a hacker can place a device connected to the hub and receive network traffic. Active sniffing mostly happens by flooding the switch content address memory table which holds MAC addresses to destinations. A hacker floods a switch with requests so that the table gets full and the switch retransmits the packets to all the ports. This way an intruder can sniff

the packets to their interest. Usually, protocols like HTTP, TELNET, FTP, POP, SNMP are considered vulnerable to sniffing attacks. To avoid sniff attacks, it is needed to avoid such protocols in network communications. Also encrypting data, network monitoring, and scanning and connecting only to trusted networks can be useful.

Dictionary attack

A dictionary attack is, trying to track the real username and password by guessing the credentials. It is a brute-force type of attack yet hackers use a dictionary of words that are mostly used to try as possible credentials. The dictionary could contain common words that are used like pet names, sports teams, food, or numbers. Users tend to use easy to remember and simple passwords across multiple accounts is a way a system becomes vulnerable to such attacks.

The difficulty of dictionary attacks varies depending on the system is online or offline. If the system is online, after few attempts, the user will be automatically blocked or the system will be locked. So that the chances of success are limited. In the case of an offline system, such limitations are lower so the attacker might get a chance. Usually, the attacker plans for a dictionary attack by focusing specifically on the target and developing a dictionary of words specific to the target. To prevent such attacks, it is always needed to encourage the users to use strong passwords. Also, frequently changing passwords, device or account locking at failed logins and disabling root login are also good ways of avoiding this threat. Slightly delaying responses from the server prevent a hacker from checking multiple combinations within a short period so it is also a good way of preventing a dictionary attack.

## 5. Summary of Cybersecurity Information Sharing Act (CISA)

The Cybersecurity Information Sharing Act (CISA) is a law created to enhance the sharing of information about cybersecurity threats to improve cybersecurity in the United States. Signed by President Barack Obama on December 18th, 2015, this Act establishes a voluntary system for sharing cyber threat indicators and defensive measures for a cybersecurity purpose between federal entities and non-federal entities (Fenwick et al., 2016).

CISA includes how the public and private entities share cybersecurity information and establish provisions on how not to share personal data that are not relevant to cybersecurity. The cyber threat information defined in this act consists of two parts, cyber threat indicator, and defensive measure. Cyber threat indicator is information that is needed to identify a cybersecurity threat if disclosure of the information is not prohibited by law. A defensive measure is a measure

taken to prevent or mitigate such a threat in an information-based system. CISA only allows these two categories of information to be shared. The sharing mechanism should also be a concern as CIS allows only some methods as, automated indicator sharing, web form submissions, email submissions, or indirect sharing (indirectly through information sharing and analysis centers).

The foremost benefit of CISA is, companies can receive real-time cyber threat information provided by other parties so that it is faster to identify threats and share defensive mechanisms. As federal and non-federal institutions share information there is a vast amount of cybersecurity data organizations are open to from federal, state, local, and international intelligence agencies as well. Under this act, the organizations that are victims of cyber attacks are encouraged to share the information and are then allowed to receive similar information from other entities. But in the end organizations must consider whether the benefits would outweigh the burdens and disadvantages of the information sharing act. While some will benefit from the vast amount of information open to cybersecurity defense from CISA, others who consider their defensive mechanisms as an asset will see fewer benefits from the same.

## Conclusion

The first part of the report includes a description of the Information Security Foundation and the Standard of Good Practice for Information Security 2011. Two subdomains from the SOGP 2011 are described in the next section followed by policies developed on the selected controls and a brief execution plan. The second part of the report is about attack trees. An introduction to attack trees followed by an implementation of an attack tree against data destruction and theft with a short description of possible network security threats concludes this section of the report. The last section is a summary of the Cybersecurity Information Sharing Act which is a cybersecurity information sharing law signed in 2015 and is a legal Act relating to the technology of the United States of America.

## References

Chaplin, M., & Creasey, J. (2011). Standard of Good Practice for Information Security 2011. *Information Security Forum*. https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security-2020/

Fenwick, Chew, W. L.-H., & Newby, T. G. (2016, October 24). *The Cybersecurity Information Sharing Act of 2015: An Overview*. Lexology. https://www.lexology.com/library/detail.aspx?g=31bc698a-ec4d-4b9b-a8a9-46d893777a10 On December 18, 2015, President Barack Obama signed into law the Cybersecurity Information Sharing Act of 2015 (CISA), which establishes a voluntary…

Schneier, B. (2004, January). *Secrets and Lies: Digital Security in a Networked World | Wiley*. Wiley.Com. https://www.wiley.com/en-us/Secrets+and+Lies%3A+Digital+Security+in+a+Networked+World-p-9780471453802