What is Operational Security (OPSEC) and How Does it Protect Critical Data?

Operational security (OPSEC), which is also known as procedural security, was created by the US military during the Vietnam war. This application is widely used in business as a risk management plan for preventing sensitive data without malicious intent. OPSEC is a plan that challenges IT and security pros to look at their operations and systems from the view of a hacker. It includes analytical tasks and procedures such as social media, behavior monitoring, and security best practices.

OPSEC aims to close all security holes that allow threat actors to steal sensitive data from an organization. Robust security isn't about having the proper hardware or software; it's about knowing exactly how they work and where the gaps are. When used alone, not every type of information is regarded as sensitive. However, if a hacker combined this data, they could be able to use it for different things, such as creating convincing phishing emails or accessing user accounts.

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

Raising awareness of this problem can be a challenging task. The OPSEC approach will produce a framework for adopting policies and best practices. Allowing an organization to set out guidelines for employees depends on the detected vulnerabilities and threats to their business. This blog post will explain what OPSEC is, the five steps of OPSEC, and its best practices.

What is Operational Security?

OPSEC is a military term that refers to plans used to stop potential enemies from learning important information about operations. This concept has transferred from the military to other branches of the federal government, including the Department of Defense (DOD).

OPSEC plans are now used in corporate operations as information management and protection that have become key to success in the private sector.

OPSEC is all about how you secure your sensitive information in an organization. OPSEC employs specific governance techniques to manage risk continuously. Your enterprise uses OPSEC every day, even if you aren’t aware of it.

OPSEC can be as easy as placing a firewall between your system and the internet to aid the secure information and ensure the proper disposal of hardcopy.

Useful link: Datacenters at 'Vulnerability' to Climate Change

The location and type of your storage must be determined before you can deploy OPSEC. It keeps information in two categories: tacit and explicit. In terms of a company's productivity, both are significant liabilities.

OPSEC helps businesses to address corporate data, information security, and risk management. It is employed by a company keen to safeguard its valuable data.

The 5 Key Steps of Operational Security

The five steps combined in OPSEC allow companies to secure their data processes.

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

1) Detect Your Sensitive Information

The first key step in ensuring OPSEC security is understanding businesses' data and the sensitive information they maintain on their systems. This includes detecting user information such as client's data, financial information, employee details, and intellectual property. Companies need to concentrate their resources on protecting this essential data.

2) Detect Possible Threats

The next stage is to identify the potential threat matrix to your business. Companies must assess the potential threats once the sensitive data has been recognized. Identifying who can pose a severe threat allows you to evaluate the risk depending on the skill set of the possible opponent.

3) Analysis of Vulnerabilities and Other Security Holes

This is a key step in the information risk management process. The business must scour for any security gaps that might allow threats to display. Assess the current condition of your security to detect flaws that could be exploited to access your sensitive data.

This should combine software and hardware security solutions, including automated security patch updates, employee awareness and training, and best practices like 2FA and strong passwords.

4) Assessment of Threat Level

The following step is to ascertain the level of threat connected to most of the discovered vulnerabilities. Next, the organization ranks the risks depending on the factors, including the likelihood that a given assault would occur and the impact such an attack would have on operations. The system's low, medium, or high threat level is determined.

5) Create a Strategy to Eliminate these Threats

This data allows companies with everything necessary to create a strategy to eliminate the threats detected. The last step in OPSEC is implementing countermeasures to

eliminate threats and reduce cyber risks. These frequently involve developing policies for protecting sensitive data, upgrading hardware, and training staff members on security best practices and corporate data regulations.

Useful link: One Year for General Data Protection Regulation (GDPR): How Global Players Affected?

Best Practices for OPSEC

OPSEC applies risk management plans to detect potential threats and vulnerabilities before they are abused and pose business issues. A company can build and implement an effective and robust security plan by following the six best practices.

Headquarters: Veritis Group, Inc , 1231 Greenway Drive, Suite 1040, Irving, TX 75038

Phone: 972-753-0022 | **Email:** connect@veritis.com

1) Implement Specific Change Management Techniques

Companies must put the right change management plans in place for staff members to follow in the case that network modifications are performed. All modifications must be controlled and managed so that companies can audit and monitor the alterations.

2) Deploy Least Privileged Access to Network Devices

Allow the least access to network devices using authentication, authorization, and accounting (AAA). Employees must have the minimum access to resources, networks, and data to do their operations successfully.

This involves applying the principle of least privilege, which makes sure that every program, process, and the user has the minimal privileges necessary to carry out their tasks.

3) Implement Dual Control

Organizations must verify that the teams and individuals who manage security are not the same as those who work on your network. This strategy protects against issues like conflicts of interest and others.

4) Automation

When it comes to business security, people are often the weakest links for data. In addition, Human errors can result in detail, mistakes, critical processes, and forgetting things. Automation can reduce these errors.

5) Use Strong Passwords 2FA and VPNs

Data breaches frequently result from human error. It would help if you verified that strong passwords and two-factor authentication (2FA) are used on every user account and trained employees on potential phishing threats. VPNs should be used while transferring data or working remotely to ensure that the data is securely encrypted during transfer.

6) Disaster Recovery Planning and Incident Response

Making a solid disaster plan and incident response plan in hand is a key component of any security defense. Even with operational solid security measures, you still need a plan for identifying risks, dealing with them, and mitigating the potential risks.

Useful link: Cloud Security Automation: Best Practices, Strategy, and Benefits

Rules to Use for OPSEC

Let's explore some rules to use that can guide secure your data online.

- Don't share your personal information, such as IP addresses, emails, and cookies.
- Don't risk it by visiting online areas such as the dark web, etc.
- Sending encrypted data isn't recommended
- Don't reveal any personal information about yourself
- Don't believe untrustworthy websites

Final Thoughts on OPSEC

Risk management combines being able to detect flaws and threats before the issue arises. OPSEC compel managers to scrutinize their operations to detect any points where their information is vulnerable. IT Managers can detect flaws they might have overlooked by viewing processes from the view of a malicious third party. Then they can implement the appropriate countermeasures in place to secure sensitive data.

Veritis, the Stevie Awards winner, offers a wide range of solutions that guide businesses may enhance their most sensitive data, improve their data security, and ensure the constant security of their users and devices. We have enough expertise in providing security solutions in a dynamic environment. So, reach out to us and work without further ado to protect your proprietary data before it’s too late.

Services