**OPSEC Applied to Your Small Business**



**Introduction:**

OPSEC, short for operation security, is an analytic process used to deny an adversary or competitor information which would harm you and benefit them. This process not only benefits military operations but can also be critical to businesses concerned about their cyber security. OPSEC teaches you to think like your adversary and explore avenues which they could gather information about your security posture without you knowing and prventing them.

**Process:**

**Step 1:** Development

**Q & A:**

What data, if lost, could be harmful to your business?

A:

What measures are currently in place to protect this data?

A:

How could the current measures be circumvented?

A:

**OPSEC Measures to Implement.**

Policies:

Use our templates to create policies for mobile device & social media use, network use, and company device use.

Restrict Network Access (Firewall) :

Separate the network into at least two local networks. One for company devices and the other for visitors and non company devices. Using a password manager create a secure “random” password for any wireless access points in use on the internal network. Create a secure backup of this password.

Least Privilege (Access Control Lists) :

Create user accounts for employees, managers, and supervisors who need them. Assign these accounts only access to the resources needed for their job. Lock down the “admin” account with a strong password. Only use admin account when absolutely necessary.

Info-sec (“loose lips sink ships”) :

Create policies for social media usage, info sharing, and phishing awareness. You may already be divulging information that can be used to plan a successful attack on your business. For example if someone was planning to rob your business they would love to know when the owner is away and knowledge about supervisors in order to plan a social engineering attempt.

Incident Response (Clear Action Plan) :

You need a plan to mitigate damage if/when a breach occurs. If an attack is discovered in progress this may be as easy as unplug the network cable(s) from the device(s) with sensitive data. Robbery in progress? Lock the building down and call police.

Disaster Recovery:

Have multiple backups, one local (External Drives, NAS) and one off site (cloud).

**Step 2:** Design

**Draft: Create a list of options for implementing each of the earlier measures.**

**Policies:**

(choose policies I.e. mobile device, appropriate use of work computers, sensitive document handling)

**A:**

Restrict Network Access:

(choose a firewall: our pfsense config or configure your own opnsense, create a secure internal wireless password if needed)

**A:**

Least Privilege:

(create a list of each employee who may have access to sensitive data and/or company computers. What is the minimum that each need to do their work responsibilities? Create user accounts for each and give those accounts access to only the programs & folders that they require)

**A:**

Info-sec:

(think like an adversary, what information would they like to know about. Perhaps when the boss is on holiday or when the least staff is on hand. Also what information is line of sight if photos were taken by workers.)

**A:**

Incident Response:

(How will you discover and react to cyber attacks? How will you discover and react to a physical security breach?)

**A:**

Disaster Recovery:

(How will you create secure backups? How will you test that you can recover from your backups?)

**A:**

**Scrutinize and Structure:**

What reasonable extra measures could you add in order to secure company devices and facilities?

(antivirus / malwarebytes, intrusion detection / security onion, endpoint security / wazuh, )

A:

Choose the options you wish to implement and structure your list.

**Finalize:**

Write an op-sec action plan based on your list. It needs a table of contents, purpose, scope, policies, procedures, and enforcement actions. Have it proofread.

Finally add this to your employee handbook / operations manual.

**Step 3:** Implement

**Training**

Set a time and date for all employees to meet and learn about the newly developed plan. Create, or add this to, a employee handbook for training new hires henceforth.

**Accountability**

Have each employee sign an acknowledgment of the new policies and procedures. Have supervisors enforcing measures.

**Incentive**

Create an incentive program for compliance. Small bonus, extra vacation, better raises, etc.

**Step 4:** Verify

**Test**

Have management watch employees to judge practicality of measures. Have individuals follow guidelines and report any conflicts or struggles that may need revision. If necessary to revise repeat steps 2,3, & 4.

**Compliance**

Create a monthly checklist in order to confirm the functionality of backups, of social media policies, of your UPS, to confirm no ex-employee accounts exist, to update all devices, and to ensure all new employees have received opsec training.