DEVELOPING A RISK-BASED INFORMATION SECURITY PROGRAM

IN 8 STEPS

@Chidambaram-narayanan

1. Identify

Identify and list all the types of information your business stores and uses.

2. Record risks for each type

• What would happen if this information was made public?

• What would happen to my business if this information was incorrect?

• What would happen to my business if I/my customers couldn't access this information?

3. Map technology to type

• Record what technology is associated with the info identified.

• Include cloud and any protection technologies you have in place such as firewalls.

• Include technologies used for remote work.

• Include the make, model, serial numbers, and other identifiers.

• Map location for each such product. In case of software, map the machine(s) the software has been loaded onto.

4. Threats and vulnerabilities

➢ Map threats and vulnerabilities each technology may face;

➢ Estimate the likelihood & impact of each threat and vulnerability.

5. Vulnerability scan

❑ Conduct a vulnerability scan or analysis at least once a month.

❑ Document the results and check for potential gaps to fix;

❑ Fix the gaps in a timebound manner

6. Policies and procedures

- Create a cybersecurity policy for your organization, including a "work from home" protocol.

- Implement procedures for the same.

7. Train, train and train

Train all employees on the details of the policy and have them sign documents acknowledging their role in continuously upholding your organization's cybersecurity by adhering to the policy.

8. Protection plan

Develop a protection plan against insider threats, including enterprise-risk assessment and access control management.

Thank you!

Like, subscribe, follow (why not all 3?)

- ✓ Auditing of financial and systems
- ✓ Cloud awareness
- ✓ Certified Information Systems Audits