HOW TO IMPLEMENT AN INFORMATION SECURITY PROGRAM IN 9 STEPS

BARR ADVISORY

TABLE OF CONTENTS

INTRODUCTION

WHAT IS AN INFORMATION SECURITY PROGRAM?

A solid information security program is an essential component of running a business in the digital age—a time when the number of data breaches and security incidents are increasing exponentially. Without a security program, you leave your company, customers, and data at risk.

Let's explore the components of an information security program, and walk through a step-by-step guide on how you can implement one at your organization.

Think about your organization's information security policies, procedures, standards, and guidelines. Together, these elements create a documented security program by outlining how your organization plans for and acts when it comes to security management.

The purpose of the program is to make certain the data and information you're responsible for is safe. By safe, we mean your organization ensures three vital principles: confidentiality (secured from unauthorized access), integrity (accurate and free from tampering), and availability (accessible in a timely manner) of its private data.

INFORMATION SECURITY PROGRAMS NEED TO:

Establish a benchmark for security

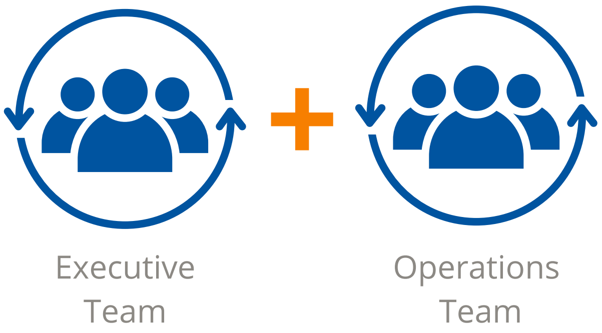
Measure against that benchmark

Enable informed decision making

Support the execution of decisions

STEP 1:
BUILD AN INFORMATION SECURITY TEAM

Before you begin this journey, decide who needs a seat at the table. One side of the table holds the executive team, made up of senior-level associates responsible for crafting the mission and goals of the security program, setting security policies, risk limitations, and more. On the other side of the table sits the group of individuals responsible for daily security operations. As a whole, this group designs and builds the framework of the security program.



DATA BREACHES BY THE NUMBERS

$3.92M
average total cost of a data breach (global)

$8.19M
average total cost of a data breach (USA)

$5.86M
average total cost for financial services companies

$5.05M
average total cost for technology companies

25,575
average size of a data breach

$150
per record (global)

$242
per record (USA)

Source: Ponemon Institute: Cost of a Data Breach Study (2019)

STEP 2:
INVENTORY AND MANAGE ASSETS

With your team assembled, their first job is to understand what assets they have, where those assets are located, ensure the assets are tracked, and secure them properly. In other words, it’s time to conduct an inventory of everything that could contain sensitive data, from hardware and devices to applications (internally created and third party) to databases, shared folders, and more. Once you have your list, assign each asset an owner, then categorize them by importance and potential risk/cost to your organization should a breach occur.

STEP 3:
ASSESS RISK

To assess risk, you need to think about threats and vulnerabilities. Many organizations perform vulnerability scans against their systems. While an important input, keep in mind that your risk assessment does not stop after the scan. Start by making a list of any potential threats to your organization's data, then categorize and assign values (high, medium, low) to these threats based on their level of danger. From there, think about what vulnerabilities exist within your organization, then categorize and rank them based on potential impact. These vulnerabilities can consist of people (employees, clients, third parties), processes or lack thereof, and technologies in place.

Look at the two lists you've created and find where threats and vulnerabilities may intersect, showing you where your greatest levels of risk exist. A high-impact threat with high vulnerability becomes a high risk, for example. Contact us if you need assistance putting together a risk analysis like this.

STEP 4:
MANAGE RISK

Now that you have your risks ranked, decide whether you want to reduce, transfer, accept, or avoid each risk.

- **Reduce the risk:** Identify and apply fixes to counter the risk (e.g., setting up a firewall, establishing local and backup locations, implementing multi-factor authentication on all systems).
- **Transfer the risk:** Purchase insurance for assets or incorporate non-insurance agreements such as contracts with indemnification provisions.
- **Accept the risk:** If the cost to apply a countermeasure outweighs the value of the loss, you can choose to do nothing to mitigate that risk.
- **Avoid the risk:** This happens when you deny the existence or potential impact of a risk, which is not recommended as it can lead to irreversible consequences.

STEP 5:
DEVELOP AN INCIDENT MANAGEMENT AND DISASTER RECOVERY PLAN

Without an Incident Management and Disaster Recovery Plan, you put your organization at risk should any security incident or natural disaster occur. This includes things like power outages, IT system crashes, hacking, supply chain problems, and even pandemics like COVID-19. A good plan identifies common incidents and outlines what needs to be done—and by whom—in order to recover data and IT systems.

DID YOU KNOW?

Cloud assets were involved in about 24% of breaches this year.

Source: Verizon 2020 Data Breach Investigation Report

STEP 6:
INVENTORY AND MANAGE THIRD PARTIES

Make a list of vendors, suppliers, and other third parties who have access to your organization's data, then prioritize your list based on the sensitivity of the data. Once identified, find out what security measures high-risk third parties have in place or mandate necessary controls. Be sure to consistently monitor and maintain an updated list of all third-party vendors.

STEP 7:
APPLY SECURITY CONTROLS

You've been busy identifying risks and deciding on how you'll handle each one. For the risks you want to act on, it's time to implement controls to mitigate those risks. They can be technical (e.g., encryption, intrusion detection software, antivirus, firewalls), or non-technical (e.g., policies, procedures, physical security, and personnel). One non-technical control you'll implement is a Security Policy, which serves as the umbrella over a number of other policies such as a Backup Policy, Password Policy, Access Control Policy, and more.

DID YOU KNOW?

77% of cloud breaches involved breached credentials.

Source: Verizon 2020 Data Breach Investigation Report

STEP 8:
ESTABLISH SECURITY AWARENESS TRAINING

Security awareness training is more than just a checkbox—it's a part of a security culture that starts at the top of your organization with management. Conduct frequent security awareness trainings to share your information security plan and how each employee plays a role in it. After all, new security measures and policies do nothing if employees working with the data are not educated on how to minimize risk. Any time an element of your security program changes, your employees need to be aware. Other effective programs could include book club-style awareness trainings targeting specific groups (i.e., software engineers) to ensure training is a collaborative process. And be sure to document and retain evidence of trainings for future auditing purposes.

STEP 9:
AUDIT, AUDIT, AUDIT

An audit is table stakes in today's interdependent systems—a minimum requirement for organizations. Customers and stakeholders demand transparency and there are many frameworks and reporting options available to report on the effectiveness of your program. In some cases, this is mandatory to confirm compliance. Third-party assessors can perform vulnerability assessments, which include penetration tests to identify weaknesses in your organization’s networks, systems, and applications, along with audits against criteria such as ISO 27001, PCI DSS, FedRAMP, and HITRUST; as well as SOC 2® reports using the AICPA Trust Service Principles. Your company can also conduct internal audits to assess controls, policies, procedures, risk management, and more.

DID YOU KNOW?

Cloud breaches involved an email or web application server 73% of the time.

Source: Verizon 2020 Data Breach Investigation Report

ABOUT BARR ADVISORY

THE SECURITY YOU NEED. THE COMPLIANCE TO SUCCEED.

BARR Advisory is a cloud-based security and compliance solutions provider, specializing in cybersecurity and compliance for Software as a Service (SaaS) companies. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements in highly regulated industries including technology, financial services, healthcare, and government.

SERVICES INCLUDE:

- Unified Compliance Program Assistance
- SOC 1 Examinations
- SOC 2 and 3 Examinations
- SOC for Cybersecurity
- PCI DSS Assessment Services
- ISO 27001 Assessments
- FedRAMP Security Assessments
- HIPAA, HITECH, and HITRUST Services
- Penetration Testing and Vulnerability Assessments
- Virtual CISO Services

CONNECT WITH BARR

info@barradvisory.com

barradvisory.com/contact

With BARR, you can expect a partner on your path to security and compliance every step of the way.