SECURITY

What You Need to Know

80% of security comes down to doing 21 things in your organization. Most are simple.

To achieve excellent security, or any type of regulatory compliance or audit certification, you will need to do a lot more.

This document covers the 21 things to get you started and then points you in a direction to develop real and provable security.

"ALL COMPANIES NEED TO REVIEW THEIR SECURITY POSTURE AND STRATEGIES NOW."

Matt Konda
CEO Jemurai
March 2021

Companies depend on tools to provide security, but in reality, tools cannot eliminate risks. We must embrace a broader approach, starting with the biggest risks, in order to reasonably secure our organizations.

53%

EMPLOYEES PHISHED

Including technical employees across the organization.

32%

SYSTEMS UNPATCHED

Endpoints and servers often remain vulnerable.

71%

RESPONSIBILITIES UNCLEAR

Who does what?

Building a security *program* helps to establish a strong security posture.

It also helps you to close business with mature partners and pass audits.

Every company should have a security plan.

securityprogram.io

21 Actions to Improve Security Today

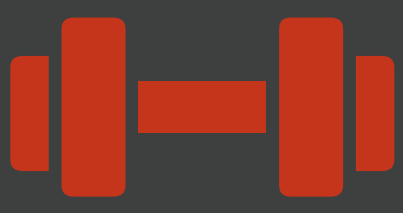
#1. Designate a person responsible for security.

This needs to be someone with the appropriate budget and executive responsibility to advocate and plan for security.

In the early stages, it doesn't need to be a security expert, provided they are seeking and getting guidance as appropriate.

#2. Train employees on security awareness.

Employees need to be trained to resist phishing scams, and they should be aware of common pitfalls (weak or shared passwords) and other realistic risks.



Training your employees is one of the most basic and important things you can do to improve your security.

#3. Create a security@ email account.

Having an easy-to-remember and published email address makes it easier for people (both internal and external) to tell you when you might have an issue. These are things you want to know about. It also provides a recognizably official address for communicating about potential security events.

#4. Rollout multi-factor authentication (MFA).

Everywhere it is supported, and definitely on company email and critical systems, enforce the use of MFA.

MFA makes it really hard for attackers to get access by guessing or stealing your users' passwords.

#5. Implement single sign on (SSO).

Everywhere it is supported, use SSO. Think "Log in with Google" or "Log in with Microsoft".

By signing in to other services with GSuite or M365 accounts that have MFA turned on, to other services, we can manage access in one place and have strong authentication everywhere.

#6. Implement password complexity and handling requirements.

First, we highly recommend using a password manager. In any case, ensure passwords are 9+ characters with complex chars or 14 without. Ensure passwords are not shared with people or across systems.

#7. Perform monthly user access audits.

Check to ensure that only current valid users exist in key systems and ensure that they are in the correct roles.

Failing to disable users is a surprisingly common and low tech way to lose or expose customer data.

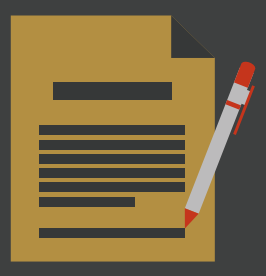
Learn more at www.securityprogram.io.

securityprogram.io

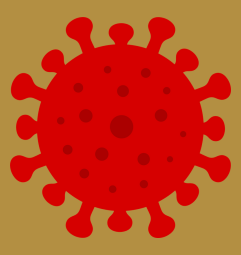
21 Actions to Improve Security Today

#8. Confirm Confidentiality Agreements

Ensure that employees and contractors with access to sensitive information or intellectual property have signed confidentiality agreements that explain their responsibilities.



#9. Implement Endpoint Malware Protections



Leverage a managed antivirus and malware solution to provide protection to end users.

#10. Implement Network Segmentation

Ensure that production systems are separated at a network level from non-production systems. Separate systems with different purposes (HR, Development, Finance, etc.)

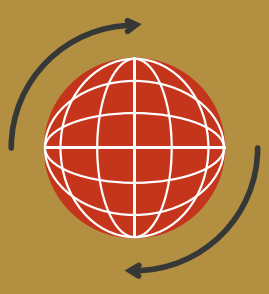
#11. Perform Network Vulnerability Scanning

Use a tool to scan the external and internal (if feasible) network for unknown, permissive or unpatched systems.

#12. Encrypt Data at Rest

Whether it is on a laptop, phone, server, or hosted cloud service, ensure data is encrypted at rest with AES-256.

#13. Encrypt Data in Transit



Protect data on the network. The easiest way to do this is to strictly use TLS 1.2+ or current SSH everywhere.

#14. Track Data Sharing with Partners

Know who you share data with and ensure that they are following good practices to protect your data.

You can't keep data secure if you are giving it to insecure partners!

Learn more at www.securityprogram.io.

securityprogram.io

21 Actions to Improve Security Today

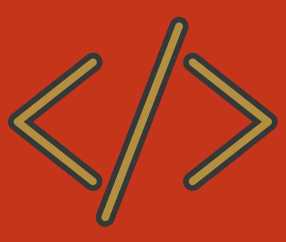
#15. Patch End User Devices #16. Patch Servers

Patch laptops and phones. Patch servers, container images, VM's, etc. with Operating System and other software updates.

Every patch represents a bunch of security holes that are being fixed. If we don't apply them, our systems have those holes.

It is probably best to set to auto-update and enforce with MDM(device management).

#17. Use a Source Control Management System



Track source code in a source code management system that has access controls, backups and ideally support for pull requests. Failing to do this can result in catastrophic loss of code, data or control. GitHub, BitBucket, etc.

#18. Define an Incident Handling Process

Write down what you will do in case of an incident. Who will track it, how will you communicate, how do you know you've handled it in a timely manner and involved the right people.

#19. Train on Incident Handling Process

Teaching the teams likely to be involved in an incident, helps to ensure that we follow the process in case there is one.

#20. Identify and Close Fraud Paths

How can you lose money? What would an attacker want from you? Some of these paths may be specific to your business, others might be true for everyone.

If you identify these things and take steps to protect them, it can have a significant impact!

#21. Review and Update Policies Annually

Have policies and keep them updated.

Having policies helps your teams to orient to security. You'll need them later anyway, and they set you on the right direction up front.

Learn more at www.securityprogram.io.

securityprogram.io

SECURITY

You can start reducing your organizational risk and improving your cybersecurity today by addressing the 21 things outlined in the preceding pages.

To go the next step, you may want to go deeper.

securityprogram.io is a SaaS based system that provides everything you need to build your own security program. We also offer tiers with expert assistance to help make sure you succeed.

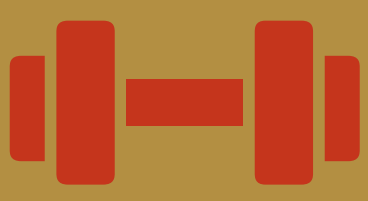
Program Core

Policies

You start with out-of-the-box security policies aligned to NIST 800-53 to ensure that you will have strong and broad coverage. It gives you a way to track policy approvals and even employee acknowledgement.

Training

A broad set of security training videos based on the policies, including General Security Awareness Training, "How To" Trainings, and even advanced developer training.



Tasks & Procedures

A big part of the "magic" of the program is the tasks that help you to actually implement the detail behind the policies. By completing the tasks, you can start off on the right foot and go one step at a time toward building your program.

Assistance: Our Team Helps You Every Step

Sometimes clients feel more comfortable with additional support because of a third-party audit, a partner/vendor questionnaire, or some other obstacle to their progress.

This is a cost-effective option that greatly improves your success. It provides the confidence and "security" (pun intended) of having a knowledgable coach working guiding you with access to subject matter experts as-needed for deeper technical discussions

Whether it is helping with questionnaires or navigating a SOC 2 audit, sometimes it is a relief to have a team behind you.

Security Tools

While tools by themselves can't provide complete security, they are helpful and necessary as part of a program. The securityprogram.io platform builds in the most necessary tools, and we're adding capabilities all the time to make your job easier.

Scanning

Meet your external vulnerability scanning obligations and identify potential security gaps.

Vendor and Risk Tracking

The vendor tracker helps you to identify and handle third party risk. The risk register fits into a framework for identifying, tracking and mitigating risks.

User Audit

Connect to Google Workspace, GitHub, AWS, and AzureAD and let securityprogram.io help make your user audits a breeze.

Visibility: Dashboards and Reporting

The securityprogram.io system also comes with dashboards and progress views aligned to different standards so that you can easily make a plan and report progress.

	Function/Category	Completed	Total	% Complete
>	ID: Identify Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	25	28	
>	PR: Protect* Develop and implement appropriate safeguards to ensure delivery of critical services	37	46	
>	DE: Detect* Develop and implement appropriate activities to identify the occurrence of a cybersecurity event	14	19	
>	RS: Respond* Develop and implement appropriate activities to take action regarding a detected cybersecurity incident	7	9	
>	RC: Recover Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	1	1	

**Current Standards Covered: NIST 800-53, NIST 800-171, CMMC, NIST CSF, CIS 20, ISO 27001, SOC 2

Learn more at www.securityprogram.io.

securityprogram.io