ROUSE
CONSULTING GROUP

Cybersecurity Essentials

Address these 30 items to secure your organization

Use this checklist to help ensure your organization is accounting for privacy concerns, compliance issues, and the policies and procedures critical to maintaining a secure organization embracing a cybersecurity culture.

Security and Privacy Program

1 □

Risk Assessment

Conduct an annual risk assessment that includes a complete inventory of digital assets, discovered vulnerabilities, known risks, and the potential business impact of each.

Security and Privacy Program

2 □

Internal Privacy Policy

Your internal privacy policy should include the protection of sensitive and confidential information as well as govern how this information is protected across all modes of access or communication. Prepare now for the need to have a public-facing privacy policy if you do not already have one in place.

Security and Privacy Program

3 □

Internal Policy for Data Retention

Creating a policy for data retention dictates how long your company will retain specific data. This policy can minimize the impact of a data breach and reduce ongoing data storage costs.

4 □

Clean Desk Policy

A clean desk policy is designed to protect sensitive and confidential information present in a workspace by requiring removal or secure storage of this data whenever the employee is away from their area. Adoption and enforcement of this policy enhances the integrity of sensitive and confidential data.

5 □

Visitor Policy

Having a clearly stated visitor policy and escort program is vital to the security of workforce personnel, clients, physical assets, and data. The type of visitor policy required is wholly dependent upon the nature of your building, office, workspaces, and location.

6 □

Privacy Policy Training

After creating a privacy policy, it is necessary to train your staff to ensure they understand the content and consequences of policy violation.

7 □

Security Awareness Training

Subscribe to and utilize a security awareness training service tailored to your organizational needs. This training will prepare employees and contractors to recognize and respond appropriately to potential cyber or physical security threats.

8 □

Phishing Awareness Training

Phishing is the practice of threat actors who send fraudulent messages in an attempt to penetrate your network, install ransomware, or defraud your company. Training your employees to recognize phishing attempts through randomly generated and controlled test phishing emails is highly recommended.

9 □

Multi-Factor Authentication (MFA)

MFA is an authentication method that employs answers to a combination of prompts that involve something you know, you have, and/or you are, to access a system. These prompts can range from a personal question to biometric methods like fingerprints and can combine passwords with technology by using text messages or emails as an additional authentication step. At least two of the three criteria must be used to achieve MFA.

The contents of Cybersecurity Essentials is provided for informational purposes only and is not a warranty or guarantee, express or implied, of the services or products represented and is intended solely for the use of organizations distributed to directly by Rouse Consulting Group and shall be held as confidential by the receiving party. No part of this publication or accompanying documents may be disseminated or reproduced in any way or for any purpose without the express written consent of Rouse Consulting Group, Inc.

ROUSE
CONSULTING GROUP

Cybersecurity Essentials

Address these 30 items to secure your organization

Use this checklist to help ensure your organization is accounting for privacy concerns, compliance issues, and the policies and procedures critical to maintaining a secure organization embracing a cybersecurity culture.

Tools **Tools** Tools Tools

10 □

Virtual Private Network (VPN)

Use a VPN or other secure, encrypted method when connecting to your network remotely. A VPN is an encryption-based communication method that connects a remote device to the private network of an organization through an external network. The encryption effectively creates a secure tunnel for data transfer and renders it indecipherable to an eavesdropper.

11 □

Secure Wi-Fi / Wireless Networking

Securing your Wi-Fi is a vital component in protecting data and ensuring the security of critical business systems. Be sure to address these items when implementing Wi-Fi:

- Change the default router password.
- Update router firmware to the latest stable version.
- Create a strong passphrase using multiple criteria.
- Enforce MAC address filtering.
- Create a guest Wi-Fi network.

12 □

Secure Email Gateway (SEG)

Email remains the primary means of internal/external communication and data transfer for most organizations. It is also often the least secured, and therefore the primary target of threat actors who have consistently increased the sophistication and targeting of these attacks. An SEG can help secure your systems by providing detection and quarantine of emails with malicious intent.

13 □

Firewall Auditing

Ensure that logging is enabled on all firewall appliances and that the logs are reviewed periodically to identify activity patterns that may indicate potential compromise or ongoing attacks.

14 □

Backup Solution Configuration

Data backup, one of the least properly implemented and maintained essentials, is the safety net needed when security fails. Be sure your backup solutions are configured for redundancy and consistent air-gapping.

15 □

Backup Solution Testing

Regularly test your backup restoration procedures to ensure the data is retrievable and reliably accessible if needed for disaster recovery.

16 □

Content Filtering

Filter internet content and block sites known to pose a high risk of malware or malicious activities by using Domain Name System (DNS) filtering. The firewall in your office may include this feature but an additional layer of protection, a cloud-based filtering service, is needed to ensure protection of all devices, including your mobile workforce.

17 □

Endpoint Detection and Response

Installing an Endpoint Detection and Response (EDR) solution will better secure your systems by continuously monitoring the environment for suspicious and abnormal activity, locking down any suspect processes before they can cause serious damage.

18 □

Security Incident and Event Management

Security Incident and Event Management (SIEM) actively logs security alert information generated by applications and hardware on your network. When coupled with a Security Operations Center (SOC) service to analyze these logs in real-time, you have an added layer of protection that can identify, investigate, and remediate potential malicious activity.

ROUSE
CONSULTING GROUP

Cybersecurity Essentials

Address these 30 items to secure your organization

Use this checklist to help ensure your organization is accounting for privacy concerns, compliance issues, and the policies and procedures critical to maintaining a secure organization embracing a cybersecurity culture.

System Hardening

System Hardening System Hardening System Hardening

19 □

Remove Unused Applications

Application vulnerabilities are continually discovered and exploited by hackers. No program is fully secure and if no longer in use or needed should be uninstalled to minimize the inroads to your systems.

20 □

Active Directory and Group Policy

It is important to only assign appropriate users to clearly defined groups with rights to modify Microsoft Active Directory and Group Policy. Misassigned modification rights can lead to exposure through accidental misconfiguration and user opened gateways.

21 □

Secure Endpoints

Properly configure endpoints (e.g. desktops, laptops, etc.) to utilize embedded firewalls and enforce user account control.

22 □

Perimeter Security

Implement properly configured firewalls, routers, VPNs, Intrusion Detection and Prevention Systems (IDS/IPS), and ensure all unused ports on your firewall are closed.

23 □

Patch Management

Operating systems and applications are constantly prodded by hackers looking for a means of access. Regularly auditing and patching of software is critical in maintaining a secure environment by remediating known vulnerabilities.

24 □

Cloud Monitoring

Monitor your cloud-based applications for abnormal user behavior such as suspicious email inbox rules, repetitious failed logins, or user login attempts from unrecognized geographic locations.

Vulnerability Management and Assessment

Vulnerability Management and Assessment

25 □

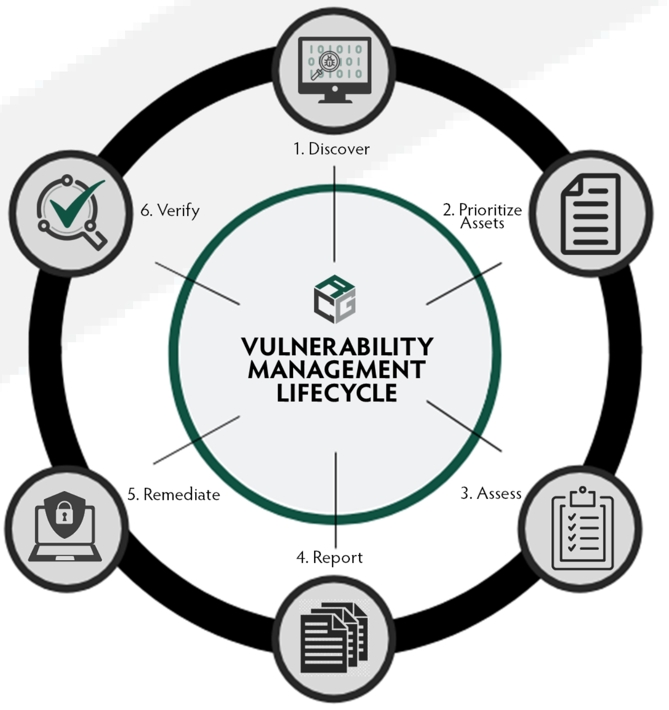
Vulnerability Analysis

Take the time to understand the purpose and functionality of all software used in your environment. Most vulnerabilities are software "bugs" that can be exploited by hackers to gain access to your network or install malware.

26 □

Vulnerability Management

Identifying and managing vulnerabilities is a key component in quantifying organizational risk. Regular assessments* help determine environmental weaknesses and provide an opportunity to plan for remediation, including Patch Management.



*Including quarterly networks vulnerability scans, cloud based application assessments and penetration testing.

Use this checklist to help ensure your organization is accounting for privacy concerns, compliance issues, and the policies and procedures critical to maintaining a secure organization embracing a cybersecurity culture.

Response Response Response Response

27 □

Incident Response

Implement an incident response policy to your organizational standards and expectations, including:

- Statement of Management Commitment
- Purpose and Objectives of the Policy
- Scope of the Policy
- Organizational Structure and Definition of Roles, Responsibilities, and Levels of Authority
- Severity Ratings of Incidents
- Performance Measures
- Reporting and Contact Forms

28 □

Incident Response Procedures

Implement step-by-step incident response procedures that detail processes to be executed in an incident response scenario; these procedures should govern the investigation and remediation of active attacks targeting your organization.

29 □

Incident Response Roles and Responsibilities

Document identified incident response stakeholders, detailing their roles and responsibilities for each determined incident response type.

30 □

Your Trusted Security Partner

Security is a shared responsibility. As attacks continue to grow in frequency and sophistication, it is important to know you are protected. RCG diligently reviews the latest cybersecurity threats, trends, and technologies to deliver the most reliable and proven solutions to secure your environment. Partnering with us will bolster your confidence and peace of mind, knowing your security is in good hands.

Contact us today to discuss how we can help secure your future, together.