ITGlue

IT Environment Security Review Checklist

In this age of rapidly evolving cyberthreats, it is important for all organizations to review and update their security systems. To help you maximize protection in your IT environment, we've put together this checklist that can serve as a starting point to improve your security posture.

Create a Security-First Culture

A security-first culture focuses on adhering to all the cybersecurity requirements throughout the organization. The primary goal here is to collectively work towards better security. You can do that by implementing the following measures:

- [ ] Document your security policies
- [ ] Enforce security policies with training and controls
- [ ] Ensure compliance with appropriate compliance frameworks with internal and external audits
- [ ] Have a dedicated individual/team for security-related tasks

Employee Security

Your employees are your first line of defense against cyberthreats. You can strengthen your security framework by taking the necessary steps to monitor and safeguard them. Following are some security measures to take:

- [ ] Enforce strong password policies
  - [ ] Use a password management tool to avoid writing down passwords on post-it notes
  - [ ] Prevent reuse of passwords across multiple sites
  - [ ] Define policies to change passwords periodically for critical documents
- [ ] Include security awareness training at the time of onboarding
- [ ] Conduct periodic security tests to identify vulnerable employees who may fall victim to social engineering
- [ ] Have an email phishing protection in place
- [ ] Enable Single Sign-On (SSO)

Client Security

It is the responsibility of MSPs to help their clients understand how to protect themselves. Use the following measures to keep your clients' network free from vulnerabilities:

- [ ] Enforce strong password policies
- [ ] Perform security audits and share them with your clients
- [ ] Restrict access of critical information to only key people
- [ ] Host security awareness training
- [ ] Have email phishing protection in place
- [ ] Enable Single Sign-On (SSO)

Password Security

Since most cyberthreats originate from stolen credentials, you need to educate your employees and clients about password security.

- [ ] Enforce host-proof hosting of sensitive passwords
- [ ] Control security access of passwords
- [ ] Create policies against simple passwords
- [ ] Use different passwords for all your main accounts
- [ ] Avoid entering passwords on computers you don't control

SaaS Security

While SaaS providers do handle many security features, it has its limitations. To ensure maximum security, you need to incorporate the following SaaS security measures.

- [ ] Ensure your software has SOC 2 Type II or NIST
- [ ] Enable Two Factor or Multi-Factor Authentication (MFA)
- [ ] Apply identity and access management to restrict unauthorized user access
- [ ] Turn on IP restriction (if available)
- [ ] Encrypt your critical data on the cloud
- [ ] Monitor employee collaboration in the cloud
- [ ] Enforce security groups and access

Endpoint and Network Security

Outdated endpoints and poor security hygiene are a deadly combination that attracts various threat actors. You can ensure maximum endpoint and network security through the following measures.

- [ ] Set up recurring tasks to keep remote management software up to date
- [ ] Use third-party patching to patch all the endpoints regularly
- [ ] Set up automated notifications for malicious or suspicious activities
- [ ] Restrict access to remote management tools
- [ ] Have a dedicated individual/team to periodically check and manage the network's settings and software upgrades
- [ ] Place firewalls between endpoints within a network to restrict host to host communication

Cybersecurity Insurance

Cybersecurity insurance can minimize your losses from unavoidable security incidents and data breaches. Take the following steps to get the most out of your cybersecurity insurance.

- [ ] Evaluate your risk before subscribing to cybersecurity insurance
- [ ] Identify the extent of your coverage
- [ ] Use sophisticated tools that ensure automatic compliance
- [ ] Personalize your insurance and update as and when needed
- [ ] Regularly review your requirements and conduct security audits

Backup

Backup is an absolute requirement for companies of all sizes. Choosing the right backup can save you a lot of time and help you resume operations instantly following a security incident. Make sure you incorporate the following measures in your backup.

- [ ] Use backup services that have operations in multiple geographic locations
- [ ] Ensure your data is being backed-up regularly
- [ ] Use the 3-2-1 strategy to backup multiple copies in different storage media
- [ ] Have a backup in place for your entire system (including hardware, software, servers, external files, tools, etc.)
- [ ] Regularly review and update your backup policies
- [ ] Test your backups regularly
- [ ] Have a disaster recovery plan that minimizes downtime following an incident