WEBROOT
Smarter Cybersecurity™

5 STEPS TO HELP MSPs CREATE A SECURITY PLAN THAT ACTUALLY WORKS

A strong security plan is crucial. Follow these tips to build a framework you can apply to all your clients.

STEP 1: ASSESS RISK

Assessing your clients' risk allows you to jointly determine the proper security policies and procedures to put into place. To effectively assess risk, you need to examine threats, vulnerability, and assets. Start with a vulnerability assessment, in which you define, identify, and prioritize vulnerabilities in your client's infrastructure. You may use automated testing tools, such as a network or application security scanner, to help you identify risks.

STEP 2: DOCUMENT AN ORGANIZATION-WIDE SECURITY PLAN

Here are some baseline components.

1. SECURITY POLICY PROCEDURES, GUIDELINES, AND STANDARDS

This includes management controls (risk assessment, review of security controls), operational controls (personnel security, physical security), and technical controls (identification and authentication, access controls).

2. SECURITY AWARENESS TRAINING

Security awareness training should be conducted at least annually, preferably more often than that. It might seem unnecessary, but given how much employee turnover there can be, you really can't have too much training. Plus, the more regular it is, the more effective it is. After 12 months of consistent security awareness training, end users are 70 percent less likely to fall for a phishing attempt.[1]

3. INCIDENT HANDLING

Central management and reporting of all incidents is key for understanding an organization's security posture and for coordinating a response to a potential attack.

4. COMPLIANCE REVIEWS AND ENFORCEMENT

Compliance reviews consist of annual reviews of applicable security systems and documentation including security plans, risk assessment reports, contingency plans, etc. Additionally, the company's data may also be subject to third party compliance requirements, such as PCI for financial transactions or HIPAA for healthcare information.

STEP 3: ESTABLISH A SECURITY MANAGEMENT STRUCTURE AND CLEARLY ASSIGN SECURITY RESPONSIBILITIES

The organization's executive management team needs to determine if they require a senior security leader, such as a CISO, and how that person should interact with the rest of the teams. Build the team out from there, so that, in the event of a breach, each person knows their role and how to handle it.

STEP 4: IMPLEMENT EFFECTIVE SECURITY-RELATED PERSONNEL POLICIES

- **Require background checks** on employees and contractors.
- **Ensure personnel have completed and signed non-disclosure agreements** (NDAs).
- **Enforce termination and transfer procedures** including:
  - Returning equipment, ID badges, access keys, etc.
  - Terminating user IDs and passwords
  - Identifying non-disclosure period effectiveness

STEP 5: MONITOR THE EFFECTIVENESS OF YOUR SECURITY PROGRAM

Your clients' security programs need to be reviewed and updated regularly in order to keep pace with today's ever-evolving cyberattack methods. You can counsel your clients to conduct regular scans of technical controls and system vulnerabilities to help stay up to date with new threats. Performing annual penetration tests can simulate the threat of someone trying to break into their organization's network and determine the effectiveness of their response procedures.

[1] Webroot Inc. "2019 Webroot Threat Report." (February 2019).

About Webroot

Webroot, a Carbonite company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.