WEBROOT
Smarter Cybersecurity™

16 QUESTIONS TO ASK CLIENTS IN A VULNERABILITY ASSESSMENT

To create a security plan that actually works, MSPs need to start by assessing their clients' risk.

By working with clients to examine and inventory threats, vulnerabilities, and assets, MSPs can create an effective baseline to help determine the proper security policies and procedures to put into place.

First, you'll need to discuss the following four threat profiles with your clients to help them pinpoint the threats they are most likely to experience.

MALICIOUS INSIDER

Someone associated with your client's organization who wants to create harm, such as a disgruntled employee or contractor.

MALICIOUS OUTSIDER

A hacker or someone involved in industrial espionage. Per the Ponemon Institute, these are the most frequent types of threats SMBs face, and typically the most expensive.*

ACCIDENTAL INSIDER

A client's employee or contractor who is poorly trained in security practices. Examples include an employee who uses his birthdate as a password, and shadow IT, in which a department (such as marketing) bypasses IT to set up their own Dropbox account with a shared password.

NATURAL DISASTERS

Companies with facilities on a flood plain, in a tornado zone, or in an area that is susceptible to wildfires or other natural disasters can be at risk for losing critical assets.

Once you've discussed threat types, it's time to do the vulnerability assessment. After all, the best cybersecurity in the world won't protect your clients if they don't address existing vulnerabilities within their organizations.

Run through this 16-question checklist with your clients to determine which areas need attention, so you can help them build out a robust security plan.

* Ponemon Institute. "2017 Cost of Data Breach Study." (June 2017)

16 QUESTIONS TO ASK CLIENTS IN A VULNERABILITY ASSESSMENT

- Do you have a security plan in place? Who has access to it?
- Does your organization have a resource dedicated to enforcing and maintaining security policies, such as a Chief Information Security Officer (CISO)?
- Does your company have a bring-your-own-device (BYOD) policy?
- Do you have a password policy for all company-issued devices? What about two-factor authentication?
- Do you have account management and access controls in place?
- Do you give employees and contractors only enough access to do their jobs (i.e., least privilege necessary, "need to know", etc.)?
- Does your organization have session controls in place?
- What security products do you already have (e.g., firewall, intrusion detection, encryption)?
- How often do you review your audit logs?
- Do you have antivirus protection? How often do you update it?
- Do you perform regular backups? All data or only business critical? How often do you test your backups?
- Have you applied all applicable security patches?
- What are your policies for data segregation and encryption?
- What method do you use to dispose of sensitive data, or equipment that may have had sensitive data on it?
- Where are your servers located? What access controls do they have?
- Are your employees and contractors trained in security best practices?

About Webroot

Webroot, a Carbonite company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers to protect small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. 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. Headquartered in Colorado, Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.