11 Critical Questions To Ask Your IT Provider *(Before It's Too Late)*

AVALONCyber

WITH ALL THE DATA BREACHES being reported weekly and with over 60% of small to mid-size businesses (SMBs) going out of business once they suffer a breach, it is critically important that companies understand exactly what their Information Technology (IT) providers are doing to keep their corporate data safe. The biggest challenge most companies face is whether to invest the resources for a team of internal IT staff, or outsource the corporate IT function to a Managed Security Services Provider (MSSP) or third-party Cloud IT Provider.

Most people believe that their IT departments, third-party providers, or Cloud providers are providing adequate information security functions and keeping their data safe. In most cases, however, they are not. Unfortunately, a simple firewall, antivirus and malware subscriptions, and backups are no longer enough to provide adequate data security.

A Managed Service Provider (MSP) is very different from an MSSP. To find out if your IT department or provider is providing adequate information security functionality, ask them the following questions:

1. Do we have a robust patch management program in place?

Improper patch management exposes your corporate network to numerous vulnerabilities and avenues for attackers to exploit to gain access to your sensitive data. Everyone has been prompted to install a Windows security update or a specific software update such as Adobe, Flash, or Internet Explorer, and some of us are reluctant to do so out of fear that the patch is malicious itself. Leaving patch management to the end user results in unpatched systems across the corporate environment. As a result, attackers can easily exploit and take control of these systems. Deploying a Windows Server Update Service (WSUS) or other robust patch management systems can unify the downloading, testing, and installing of all necessary system, security, and application updates across the environment on a planned schedule.

Attackers can easily exploit and take control of unpatched corporate systems

2. Do we have a next generation or UTM firewall on our perimeter?

With the increasing sophistication and frequency of cyber attacks, having a simple stateless firewall on the perimeter of your corporate network is not enough today because they are typically configured to defend against a static list of IP addresses and typical network connection types attempting to gain access to your network resources from the outside. Having a "smart" Unified Threat Management (UTM) firewall security platform at your perimeter provides advanced security control features[1] in a single firewall device. This is a layered approach to information security deploying ten security protocols to protect you from attackers and adversaries. The cost of a UTM with advanced security features is extremely affordable for SMBs, especially compared to the cost of recovering from a data breach event.

1 Examples: application control, intrusion prevention Services (IPS), intrusion detection services (IDS), web filtering, data loss prevention (DLP), advanced persistent threat intelligence subscriptions (APT), content filtering, malware defense, quality of service (QoS), and encrypted antivirus

3. If we only have a stateless firewall, do we at least have extensive logging enabled?

The single largest challenge in conducting an effective data breach investigation after an event occurs is the availability of firewall and other system and network log data. The lack of this data prevents investigators from answering key questions needed to determine your corporate responsibility to notify or disclose the breach event publically. The inability to answer questions with a high degree of forensic certainty can often mean that public notification be given about the event.

4. Do we have end point monitoring in place?

End points (laptops, desktops, printers, copiers, and other devices connected to the network) are an easy first target for attackers—they are inside the environment, connected to the internet, and have credentials to the sensitive corporate resources. Most IT departments deploy end point monitoring, but most are only using antivirus and malware detection solutions on those end points. These solutions are necessary, but if they are not updated regularly or if an increasingly common zero day (an attack that the antivirus and malware solutions have not seen yet) is deployed, the network is at risk of a breach. There are affordable, behavior-based end point monitoring solutions that will also watch and alert on irregular and malicious behavior of an attacker exploiting a system or moving laterally across your corporate network. Managed Security Services are very different from your standard IT Managed Service, so be sure to ask the right questions and understand what you're getting—or not getting—from your service provider.

5. How do remote users access our corporate network?

Some IT departments still allow an unsecure default Windows remote desktop protocol (RDP) to allow users or third-party vendors to connect to their corporate environment. This connection protocol can be fine to use within the network, but it is extremely dangerous to have RDP open to external users. Using an up-to-date Virtual Private Network (VPN) connection protocol with encrypted tunnels is the preferred method of connecting remote users and third-party vendors that need secure access to your data and resources.

6. Do we use two-factor authentication?

Single-factor authentication is defined as something that you know, such as your user name and password. A compromised user name and password pair is the most common way attackers gain unauthorized access to systems. Many providers, therefore, are implementing two-factor authentication—something you know and something you have. The something you have is typically a code that is either synced with the authentication system to generate a code that is sent to that user via text message to a mobile device or a program running on the user's computer. This ensures that the user who is trying to log in is, in fact, the same user who was set up to receive the special code. This significantly reduces the ability for an attacker who has merely obtained a user's credentials.

7. Do we employ encryption of our most sensitive data while at rest on our network servers and/or devices?

Encryption has become commonplace in today's IT environments. It is cost effective and not very difficult to roll out. Encrypting your critical data while at rest on your network blocks a potential attacker, even if they were able to infiltrate your system.

A compromised user name and password pair is the most common way attackers gain unauthorized access to systems

8. Do we routinely perform internal and external security scans to identify system vulnerabilities?

It is important to perform regular scans of your internal and externally facing network resources to ensure that your patch management program, system upgrades, and common security functions are in place and working properly. Depending on your industry, these scans may be a requirement to maintain relationships with your key customers. It is also an inexpensive way to lower your insurance premiums for Cyber Liability Insurance. It might beneficial to hire an outside Information Security provider to perform these scans, because your own IT company is not very likely to report back deficiencies on themselves.

9. Do we have a Comprehensive Information Security Program and Incident Response Plan in place?

In order to implement proper security functions, it is necessary to develop

and maintain a comprehensive information security program, as well as the policies and procedures to effectively administrator that program. The goal of the information security program is to set the guidelines and structure for the organization's IT security. Without proper policies, it is very difficult to have consistency and uniformity of your information security across the corporate environment and the various departments and functions.

Incident response planning is also important, as data breaches are more and more common among SMBs. The goal of the Incident Response Plan is to prepare a "playbook" outlining exactly how the organization reacts and responds to a breach event. The plan will identify who within the organization is responsible for responding, as well as when to engage outside vendors and legal experts to assist in data containment, remediation, and notification and disclosure obligations. You don't want to wait until there is a fire to build the fire department.

10. Do we have an employee awareness and Information Security Training Program?

Having a good Information Security Policy that includes an Information Security Training Program and continually educates employees and end users about good and bad security behavior can significantly reduce that threat to your business. Unfortunately, despite even the most secure technology, our employees and end users continue to be the biggest threat to data breaches.

11. Do we have Cyber Liability Insurance coverage?

According to the 2016 Ponemon study, the total cost of a data breach increased from $3.79 to $4 million per breach event. The average cost paid for each lost or stolen record containing sensitive and confidential information increased from $154 in 2015 to $158 in 2016. This is the single biggest reason why 60% of SMB companies go out of business within 6 months of a data breach—because they do not have the proper insurance coverage to cover the all the costs associated with responding, investigating, containing, remediating, disclosing, and defending all of the legal corporate responsibilities that follow a breach event. Depending on the state you do business in, and the states that the affected individuals reside, your disclosure obligations can be extremely significant. Insurance carriers will

deny coverage under most standard business insurance products such as Commercial General Liability (CGL), Errors & Omissions (E&O), Property & Causality (P&C), Crime, etc. If your company does not have a specific cyber policy, the expense can be detrimental to the business.

10 More Specific Questions to Ask Your Third-Party Cloud Providers:

1. What are the specs and certifications of the data center we use?
2. Do you have insurance in the case of a breach that will cover us?
3. Do you support encryption of our data and e-mail?
4. What type of firewall do you use to protect our data from the outside threat?
5. Do you have IDS, IPS, and robust logging of the firewall enabled?
6. Is our data automatically redundant across multiple data centers?
7. What is the recovery time if the systems hosting my data are completely destroyed?
8. Do you have documented data security policies?
9. What is the average total downtime for the services we are subscribing to?
10. Do you outsource your helpdesk?

Your data may already be at risk.

Download our free whitepaper, *7 Ways Your Employees Put Your Corporate Data at Risk* to learn how you can protect your company from a breach.

AVALON Cyber

QUESTIONS?

For more information on any of our services, please contact:

Ashley Hazlett
Director of Marketing
716.995.7777
ashley.hazlett@teamavalon.com