CySure

SMEs: Is your MSP protecting your data? Cyber security questions to ask your IT service provider

A CySure white paper

Winter 2019

Executive Overview

Managed Service Providers (MSPs) are often charged with safeguarding their customers' IT systems from cyber attacks. However, new research has revealed that cyber criminals have identified MSPs as a high value target and are systemically carrying out attacks. Typically, MSPs have access to the systems of multiple customers, enabling hackers to launch malicious attacks on many organisations with just one hack. The research showed that 74% of MSPs themselves have suffered at least one cyber-attack, with 83% reporting that their SME customers have suffered an attack[i].

The extent to which MSPs have come under attack in previous years has slowly come to light following a long investigation into a hacking campaign, known as 'Cloud Hopper'. Eight of the world's biggest technology service providers were hacked by Chinese cyber spies in an elaborate and sustained attack over a period of years. Teams of hackers, now known to be connected to the Chinese Ministry of State Security, had penetrated MSPs' systems and used it as a launchpad to attack customers[ii].

The invasion, which exploited weaknesses in the MSPs systems, enabled hackers to gain access to customers. Government prosecutors in the U.S. say the theft of industrial and commercial secrets, the very lifeblood of a company, was for the purpose of advancing the Chinese economy.

The Cloud Hopper campaign highlighted how security vulnerabilities in MSPs can be exploited. Whilst outsourcing can deliver many benefits it is vital that SMEs do their research and uncover any risks. Partnering with third parties can deliver many security benefits but it's important to understand responsibilities and potential liabilities.

In this new white paper, we outline 12 questions for SMEs to ask their MSP.

Where is cyber security on your MSP's priority list?

The business landscape is constantly evolving, with technology and regulation changing how business is conducted. The right managed services provider can be an asset to any size company. They can ease the regulatory burden, add an extra level of security to a business's data and present a cost-effective solution for IT. However, in today's technology centric world, a cyber-attack should be expected. When investing in Managed Services, it is essential to find a provider that is prepared for the inevitable.

A Vanson Bourne report for Continuum revealed that 80% of MSPs say they have experienced difficulties when selling cyber security solutions to their clients/prospects. A third of respondents claimed this difficulty came from not having the right skills, certifications and/or knowledge to articulate their offering.

Before working with an MSP, or any provider for that matter, SMEs should sit down with them and find out what they are really bringing to the table. Any MSP worth its salt will be ready to talk through their breadth of security knowledge and ability to protect clients. If your MSP does not have an answer it is time to move on to the next potential partner?

80% of MSPs say they have experienced difficulties when selling cyber security solutions to their clients/ prospects.

Source: *Vanson Bourne report for Continuum; Under attack: The State of MSP Cyber security in 2019*

Is security designed into the services and tools that the MSP offers?

Are the services offered by your MSP designed and developed with security in mind? There are a number of different architectural models that can be used to design the administration approach for IT systems. It is important to understand what model your MSP uses to manage your infrastructure and services as some designs can be riskier than others.

The National Cyber Security Centre (NCSC) has published the NCSC System Administration Guidance[iii] which provides a structure to help companies understand the various risks. As well as the technical architecture used, you should also understand how your MSP ensures separation between their customers, ensuring that compromise of one does not allow compromise of all.

What systems are in place to defend against cyber-attack?

Your MSP's corporate network should be separated from the infrastructure used to provide services to you. As part of your assessment, ask how the MSP's own corporate network may bring risk to your systems and data and how they manage that on your behalf.

The services should be able to identify and mitigate security threats. Solution offerings that do not have security baked in may be vulnerable to threats which could compromise an SME's data, cause loss of service or enable other malicious activity.

MSP knowledge and expertise: Certifications and skills

It's important to find out what percentage of the MSP's staff are security professionals with specific technical skills and what certification they have. These may seem obvious questions but it is surprising how many MSPs do not require certifications of their staff.

The VansonBourne/Continuum report found that nearly three in ten MSPs do not currently have basic, foundational cyber security certification. Around four in ten MSPs surveyed do not have the deep technical certifications needed to effectively operate, administer and support cyber security technologies. The growing skills gap affecting companies from recruiting trained technical staff is also impacting MSPs. Around four in ten MSPs say their organisation is not always able to obtain and/or retain the level of in-house cyber security skills needed to deliver security services.

It appears that the trend of MSPs outsourcing services may continue. 28% of MSPs outsource their network operations centre (NOC) services, with 32% planning to outsource this function in the future. Additionally, 23% currently outsource their security operations centre (SOC) services, while 38% have plans to outsource this function in the future.

SMEs should ask what certifications the service provider's employees have and what ongoing training requirements are in place. Employees change jobs, therefore your service provider should be ensuring any change in personnel doesn't impede and the quality and security of your service.

26% of MSPs with 1-9 employees do not have any type of certifications

Source: *Vanson Bourne report for Continuum; Under attack: The State of MSP Cyber security in 2019*

What governance framework does your MSP follow?

Your MSP should have a security governance framework which coordinates and directs its management of the service and information within it. For example, any SMEs operating in the EU will require an MSP to comply with the General Data Protection Regulation (GDPR).

Equally if HIPAA (Health Insurance Portability and Accountability) or PCI DSS (Payment Card Industry Data Security Standard) are important to your business, your MSP should be able to prove it has the tools and certifications to meet with the legal requirements of the regulation. Any technical controls deployed outside of this framework will be fundamentally undermined so SMEs should check what framework the MSP is adhering to and that it meets their needs.

MSP personnel: Screening and access control processes

Where MSP employees have access to your systems and data it is vital to have a high degree of confidence in their knowledge, expertise and trustworthiness. Ask questions about your MSPs personnel screening process. How do they hire employees and what checks do they carry out?

Enquire after the personnel security policies and what operational restrictions are placed on the people who perform day-to-day activities within the MSP. What procedures do they have to prevent unauthorised personnel accessing your systems/data? Ask about how they store and manage access to your key credentials. How do they monitor and manage audit for their customer system accesses, ensuring only authorised personnel have access?

People are the first and best line of defence, when adequately security trained, so check what your MSPs policy is on training their staff. These steps reduce the likelihood of accidental or malicious compromise by MSP personnel.

What percentage of cyber security does your MSP outsource?

The General Data Protection Regulation (GDPR) requires organisations to take appropriate technical and organisational measures to protect the personal data they process. Organisations remain legally responsible for the security of the data and for protecting the rights of the individuals whose data is being processed even if using an MSP (or any third party).

In deciding what security measures are appropriate, SMEs need to consider the sort of personal data that is being dealt with, the harm that might result from its misuse, the technology that is available to protect the data and the cost of ensuring appropriate security for the data.

GDPR requires organisations to ensure that any third-party data processor that is being considered will be capable of carrying out the processing in a secure manner. In addition, there should be arrangements in place, such as regular reports or inspections, to check the processor is processing the data in an appropriate manner.

The fact that an MSP is handling data does not absolve SMEs from responsibility in the event of a breech. The MSP should be able to evidence that any outsourcing partners satisfactorily support all of the security principles which the service claims to implement.

There should be arrangements in place with the MSP, such as regular reports or inspections, to check the processor is processing the data in an appropriate manner.

SMEs will continue to be responsible for the security of the data and the protection of the data subjects' rights. This responsibility is not only to the data subjects themselves but also to the Information Commissioners Office (ICO), which has shown it will not hesitate to take punitive action in the event of a breech.

23% currently outsource their security operations centre services, while 38% have plans to outsource this function in the future

Source: *Vanson Bourne report for Continuum; Under attack: The State of MSP Cyber security in 2019*

65% of UK Small Businesses do not have plans in place to deal with potential supply chain disruption, including cybercrime

Source: *Federation of Small Business*

Does your MSP offer cyber security awareness training?

Teaching SMEs about the best practices they can follow in achieving strong cyber security hygiene is highly beneficial to both complying with GDPR and reaching the desired result of protecting data. An effort to change the cultural expectations and norms around data protection is a major component of GDPR, and this requires an education that MSPs can provide.

Some SMEs may look at their options and believe that compliance measures are beyond what they can afford. Achieving safety and compliance doesn't have to be a costly or complex project. Cyber Essentials is a UK government and industry backed scheme to help all organisations protect themselves against common cyber-attacks. In collaboration with Information Assurance for Small and Medium Enterprises (IAMSE) they set out basic technical controls for organisations to use which is annually assessed.

SMEs should enquire if their MSP is aware of Cyber Essentials and can assist in gaining certification. CySure provides an online information security management system that incorporates Cyber Essentials. By utilising this online tool, SMEs can undertake a certification route guided by a virtual online security officer (VOSO) as part of a wider information security management system. This will help your organisation to coordinate all security practices in one place, consistently and cost-effectively.

Being fully Cyber Essentials compliant is said to mitigate 80% of the risks faced by businesses such as phishing, malware infections, social engineering attacks and hacking.

Source: *Cyber Essentials NCSC*

Cyber Hygiene practices

The fundamental cornerstone of good security is good cyber hygiene. Systems that use default passwords, are not patched regularly, or are misconfigured, often become compromised. SMEs need to check with their MSP that the service is operated and managed securely in order to impede, detect or prevent attacks.

SMEs should ask:

- What are your cyber hygiene practices?
- Do you patch systems regularly?
- Are cyber security assessments, vulnerability scans and password management part of the existing service offering?

Good operational security should not require complex, bureaucratic, time consuming or expensive processes. Good cyber hygiene is about getting the basics right and performing them regularly. A good MSP should be able to demonstrate they are carrying out these tasks regularly and keeping your systems secure.

Cyber-attacks: Accountability and liability

When outsourcing anything you need to ask what responsibilities fall to your MSP and what falls to you. Questions to ask are:

- Who would be held accountable in the event of a cyber-attack?
- Who would bear the financial liability if our data and systems are impacted?

There needs to be a clear delineation between when the SME is responsible in terms of security and what the MSP is accountable for. This is one area where there should be no ambiguity or wiggle room. A clear set of service level agreements should be in place because the cost implications of an attack is no small matter.

Should a cyber-attack happen, understand how your MSP will help in investigating any potential impact on your systems and data. It is vital to understand how willing they will be to work with you on remediation and future uplifts in the security of the service they are providing. The answer to this question should be part of your assessment into whether the existing relationship with your provider will continue into the future. MSPs who are unwilling to work closely with customers or share information to remedy an issue should be treated with extreme caution.

Outsourcing the role – but not the responsibility

Managed services providers can help an SME accelerate its business growth - if there is a good fit and the relationship is handled properly. The right MSP can give your in-house IT team their valuable time back and reduce the stress on business owners. It is important to find an MSP that does not see all SMEs as one homogenous mass. Look for an MSP willing to customise its services and solutions in ways that will best support your business and deliver effective and efficient results.

Future safe guarding is vital and SMEs should ensure they have clear service level agreements in place that address how issues will be handled and escalated. Without a clear agreement on roles and responsibilities you could be left with unexplained downtime, reputational damage and unhappy customers.

A point to note is that outsourcing IT doesn't mean handing over the reins to external experts and being absolved of all responsibility. It is the responsibility of the SME to ensure their MSP has security credentials which stand up to scrutiny, especially in the event of a cyber-attack.

Being fully Cyber Essentials compliant mitigates 80% of the risks faced by businesses such as malware infections, social engineering attacks and hacking. The Cyber Essentials scheme aims to provide businesses with a strong base from which to reduce the risk from these prevalent cyber-attacks. SMEs that have engaged an MSP without maintaining some independent auditing and monitoring are unlikely to be able to manage their risk effectively.

When choosing a dependable MSP, you're investing in the stability of your business - so it's worth doing the research and asking the right questions.

[i] Vanson Bourne State of MSP Cybersecurity 2019
[ii] https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/
[iii] https://www.ncsc.gov.uk/guidance/systems-administration-architectures

How to assess your MSPs cyber capabilities – checklist of questions to ask

No.	Activity	Status
1	Where is cyber security on your priority list?	
2	Is security designed into the services and tools that you offer?	
3	What percentage of your staff are security professionals with specific technical skills? What certification do they have?	
4	What is your personnel screening process? What procedures do you have to prevent unauthorised personnel accessing my systems/data?	
5	What governance framework do you follow?	
6	Do you have a cyber security certification?	
7	What percentage of your cyber security do you outsource?	
8	Do you offer cyber security awareness training?	
9	Do you patch systems regularly? Are cyber security assessments, vulnerability scans and password management part of the existing service offering?	
10	What systems are in place to defend against a cyber-attack?	
11	Who would be held accountable in the event of a cyber-attack?	
12	Who would bear the financial liability if our data and systems are impacted?	

About CySure

CySure is a cyber security company founded by experts with extensive experience in operational and risk management. The company has offices in London (UK) and California (USA) and CySure's flagship solution – Virtual Online Security Officer (VOSO) is an information security management system (ISMS) that incorporates GDPR, US NIST and UK CE cyber security standards to guide organisations through complex, emerging safety procedures and protocols, improve their online security and reduce the risk of cyber threats.

VOSO

VOSO is a simple to use web-based solution that incorporates a comprehensive range of features such as remote monitoring and secure configuration of all networked devices, asset mapping, vulnerability scanning and patching, dashboards to display compliance progress against selected standards including General Data Protection Regulation (GDPR) as well as online security training videos for continual staff training. Costing from just a few pounds sterling per month, VOSO reduces the requirement for expensive cyber security consultants or compliance officers, mitigates the risk of law suits and regulatory fines and ensures employees are trained regularly and kept informed of the latest cyber security updates.

Contact Us:

United Kingdom

+44 (0) 808 189 3226

United States

+1 (1) 844 258 2001

Visit us online:
www.cysure.net