East Midlands Special Operations Unit

**CYBER AND FRAUD PROTECT WEEKLY SECURITY ARTICLE**

*Thursday 21st January 2021*

**This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands to raise awareness among businesses and the public.**

**If you require any further information, assistance or guidance please contact the** EMSOU Protect Team

## Managed Service Providers

Sometimes an organisation will not have the technical expertise or resources to manage their own network and develop a robust cybersecurity posture. As such, Managed Service Providers (MSP) have grown rapidly over the past decade to fill the gap.

A well-chosen MSP can have a significant impact on enterprise success. A poor one will waste money and expose the business to dangerous risks. The answer, therefore, is to compare services and choose what works best for you.

**Industry Specific:** It is quite possible that the service provider will specialise in a particular industry sector such as academia, government, healthcare or legal services. Such specialism are helpful because it suggest existing familiarity with:

+ Mission critical functions
+ Organisational structure
+ Typical data collection and processing
+ Typical networking arrangements
+ Current level of expertise and knowledge about IT infrastructure and security

The more familiar the MSP is with the needs of your organisation and operating procedures, the more likely you will receive a quality service.

**References:** Of course, it also helps to learn about existing clients, especially if they are approachable and open to questions as to the quality of services rendered. Without such references, it is difficult to verify the claims of the MSP.

**Regulatory Compliance:** Many businesses deal with regulated data. This may take the form of personal identifiable information (PII), personal health information (PHI) or the processing of payment data. As such, a data breach could easily lead to regulatory fines and sanctions as well as civil litigation.


To prevent such issues, the MSP should understand how to introduce technical standards and operational procedures that will take the burden out of compliance with GDPR and PCI DSS.

**Security Frameworks:** Nothing will maximise the chances of downtime, loss of revenue and reputational harm as a security

incident. The best way to mitigate such risks lies firmly in the implementation of a framework such as; ISO 27001/2, NIST CSF, CIS v7 or CSA (for Cloud technologies). Any MSP that has had dealings with such frameworks is better placed to support your security posture.

**Service Level Agreements (SLA):** You need to understand what the MSP can and cannot provide and the SLA is the measure of such things. Experiencing a crisis at 5am on a Sunday? What does the LSA say about end user help and support? Raised a ticket 3 days ago and still haven't heard anything back? What did the SLA say about response times? Again, does the service include software patching, network monitoring, server upgrades, hardware installation or ISP issues? What is included in the flat fee and what services are deemed as additional? Knowing what is in scope could be a deal breaker for most organisations.

**Vendor Lock In:** Whilst we're on the topic of paperwork, let's consider another important feature of contract negotiation – the exit strategy. Think carefully about where and how your data will be stored and the services rendered so that you are not tied to a particular IT implementation which is managed by your provider. As your business evolves, you need to reserve the right to look elsewhere for more favourable terms.

**The Biggest Client-Facing Issue:** This is a tough but fair question to throw at any provider. They should be able to talk about their biggest challenges and how they faced them, even if they can't name names. Such discussions will also elicit a good understanding of the MSP's competencies.

**Incident Response Readiness:** At some point, your business will be attacked. How badly that attack turns out to be can depend on how prepared your organisation is to handle such problems. Incident response often relies on procedures that cover:

+ Preparation
+ Detection & Analysis
+ Containment Eradication and Recovery
+ Post Incident Activity

How will the MSP support the organisation through each of these stages? Will support be adequate? If this sounds too abstract, let's rephrase the question differently – how will the MSP support your organisation if you:

+ Discover an unauthorised administrator's account on your systems?
+ Discover that your webpage is offline because of a denial of service attack?
+ Wake up Sunday morning to find ransomware running rampant on end user devices?

**Client Interaction:** Many service providers often run networks remotely to save travel and the inconvenience of turning up on site. Such remote management certainly improves efficiency, however, it can also open exploitable doors to your network and data. It would be wise, therefore, to

identify the mechanics of such connections and the procedures that will be put in place to keep them secure.

**Vendor Security Posture:** Indeed, this begs the wider question of what the vendor will do to make sure that they are not victims of cybercrime either. Have they undertaken a risk assessment? Do they use security frameworks to develop defence in depth? Have they Business Continuity Strategies in the face of widespread disaster? How do they manage their own supply chains or outsourcing of services? These are important considerations because an MSP is a highly desirable target for cybercriminals who recognise that they have a hand in multiple pies. Look for certifications that demonstrate the organisation takes cybersecurity seriously.

The senior leadership team will no doubt ask important business related questions which may include:

1. **How will the MSP improve efficiency?**
   Because most organisation need more than a simple 'fix-it' type of service and instead are looking to see the implementation of tech that will improve access to operational data and reduce system downtime. This begs the next question:
2. **How will the MSP reduce costs?**
   Because they may take over functions such as the helpdesk, network maintenance and optimisation. If this enables the business to become more competitive, then it has a measurable financial impact.

However, never forget that security is not the unlucky passenger that failed to claim 'shot-gun' on your journey to a better, brighter future. Your organisation will stand or fall based on its willingness to identify and address security risks and if your MSP is a key player in this strategy, then you had better do your 'due care and diligence' on them.

**Reporting**

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.

Forward suspicious emails to report@phishing.gov.uk.

Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).