East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Thursday 28th January 2021

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

If you require any further information, assistance or guidance please contact the EMSOU Protect Team EMSOU Protect Team or your local Force protect team.

SECURITY SPECIAL: Everything You Need To Know About Moving To The Cloud PART 1

Migrating to the cloud offers multiple benefits including:

- **Broad Network Access:** Cloud services are device agnostic. It doesn't matter if your tech is a mobile phone, a tablet, a laptop or a PC. It doesn't matter if it's rammed with high performing hardware or stripped down to the bare essentials - as long as the device has internet capability, you can most likely connect. This makes mobile working, employing a diverse workforce, and increased collaboration not only possible, but entirely practical.

- **Rapid Elasticity:** It is also possible to quickly add IT infrastructure such as data storage, data processing and memory at a click of a button. Ditto the number of users that can access critical applications. IT resources, therefore, are closely aligned to business requirements – including seasonal fluctuations, peaks and troughs.

- **Metered Service**: One of the biggest benefits of moving to the Cloud is that you only pay for what you use. This reduces the chances of heavy overheads and under-utilised infrastructure during relatively quiet periods. Additionally, most Cloud Service Providers (CSPs) provide a simple web portal to track key metrics regarding usage and compliance with service level agreements.

- **Pooled Resources:** Most CSPs own vast pools of computing resources, helping many businesses to benefit from economies of scale - not only reducing energy bills but investment in hardware, IT maintenance and security services.

Clearly, there are more benefits to the cloud then there is space here to talk about them. However, the senior leadership team must be ready to articulate these in a way that everyone within the organization can understand and support if they wish to move operations to the cloud.

Services Available in the Cloud:

There are 3 key types of services:

- **Software as a Service (SaaS):** Provides applications you need. These are accessible through your browser or software client and usually requires licenses. SaaS gives the cloud customer the least amount of administrative work to do. Most organisations already run their own mailing systems based on such a model.

- **Platform as a Service (PaaS):** Allows organizations to build, run and manage apps without using any IT infrastructure. This is a popular option for software development companies.

- **Infrastructure as a Service (IaaS):** Delivers IT infrastructure over the cloud. This gives you the most control over your network and greatest visibility into what's happening. By the same token, however, the cloud customer has to be much more involved in the management of these IT systems.

Finally, we have public cloud computing and private cloud computing. The latter is exactly that – the organisation owns or has exclusive use of the technology. Whilst this often results in better oversight of IT systems and the handling of sensitive data, the expense can be entirely prohibitive. Public clouds, on the other hand, are cost effective because the underlying infrastructure is shared with others. It is the security issues and lack of oversight that make them unpalatable for some.

These days, most businesses operate a hybrid model, believing that this will provide the organisation with the right balance of risk and opportunity or sometimes because this is the only feasible solution available. Not all applications can be moved to the cloud, for example, necessitating some form of internal network. In any event, you should seriously consider hiring a Cloud Access Security Broker (CASB) if you wish to combine more than one vendor or service types.

Transitioning To The Cloud Successfully Requires:

PHASE 1: Preparation

Migrating to the cloud can often exceed budgets and deadlines and even cause unexpected business disruptions if not well handled. One way to avoid this is to ensure that senior leaders and heads of departments participate early in the planning process and to make sure that the move to the cloud aligns with long term business goals.

You should be asking:

- What business problem will the cloud be solving?
- Who are the intended internal and external users?
- When, where and how will the cloud be accessed?
- Will use of the cloud become mission critical?
- What will happen if the service goes down?
- How could our use of the cloud change over time?

You might also want to ask

- What legal, regulatory or contractual standards do we have to maintain?
- What internal regulations should be considered?

Cloud Readiness Assessment (CRA)

Some organisations will write a CRA to consider

- **People:** Moving to the cloud affects human resources in service, support and operations. Will there be unemployment, redeployment or recruitment? Are there skill gaps that must be filled?

- **Technology:** You cannot migrate systems if you don't understand what those systems are and how they work. For example,
    - What format is the data in?
    - How much storage do you need?
    - Which servers run which business applications and what condition are they in?
    - How many users are there on your network?
    - Can we determine cost / benefit?

- **Processes:** Migration will impact on business operations, processes and work flows, are we able to manage this change?

At this point, we are slowly developing our sense of what is and what is not feasible.

- What are we moving?
- Why are we moving it?
- Is the business culture and skill set aligned with this move?
- What will a successful move look like?
- Which compliance and security guidelines need to be followed?
- Who will own the applications and supporting infrastructure once moved?

Performing a cloud readiness assessment will provide a holistic review of your current business and IT environments, with a key focus on culture, compliance, resources and strategic goals.

Testing the Waters

The next step is to consider running a small pilot to identify the pitfalls when moving to the cloud. For example, you could just move your backups to the cloud or a low risk application - making sure you have the capability to roll back systems if things go wrong.

Making the Business Case

Now we report our learning experiences. We:

- Identify our desired outcomes and metrics.
- Identify our desired cloud operating model.
- Identify and prioritize the applications we wish to move.
- Estimate our timeline and budget.
- Identify our roll back capabilities and disaster recovery plan.
- Identify our security and our compliance requirements.

PHASE 2: Research

The SLA is a critical document as you go to market. It will:

- Describes the specific metrics associated with each service.
- Describe what will happen if the metrics are not achieved.
- Describe caveats such as planned outages.
- Details the ownership of data and rights of access, destruction or to have it returned to you.
- Describes the security standards maintained by the CSP, along with your rights to audit compliance.
- Describes your right to continue or terminate the service, as well as the associated costs of doing so.
- Details the roles and responsibilities of your organisation as well as those of the CSP.

A critically important footnote

If regulated data is exposed or suffers any form of harm in the cloud, regulatory bodies will knock on your door in the first instance to demand answers. This is because no matter how much you ask the CSP to take on in terms of managing the technology or in terms of processing the data, you will always be ultimately responsible for what happens to it. As such, you must interrogate the CSPs cyber security posture to make sure it meets your requirements.

Information Security Management System (ISMS)

Most CSPs worth their salt, will explain the security standards their systems or products align to. These standards will invariably help the CSP to:

- Identify cyber security risks that will affect the organisation
- Apply technical, administrative or physical controls to mitigate risks that pose an unacceptable threat
- Develop ongoing metrics to monitor the success of such controls
- Develop procedures for dealing with security failures.

Cloud vendors, therefore may offer:

- **ISO 27001:2013:** certification

Demonstrating that there is a holistic approach to managing enterprise risk and security.

- **NIST SP 800-53r5 Security & Privacy Controls for Federal Information Systems**

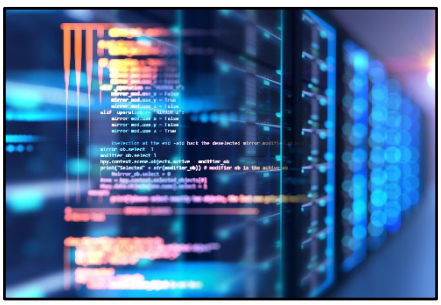
A freely available framework from NIST. Like ISO, this ensures a risk based approach to security and the implementation of controls to protect operations; assets, individuals and supply chain.

- **The Service Organization Control (SOC) audits:**
  For our purposes, there are 3 different types of reports that we are most interested in:
  - **SOC 2 Type II:** Evaluates the design and operating effectiveness of multiple security controls. Type II reports are hard to get your hands on, however, because they discuss the internal architecture of the CSP's systems.
  - **SOC 3:** A publicly available summary of the vendor's SOC 2 report, providing the AICPA SysTrust Security Seal. The report includes
    - The external auditor's opinion of the operation of controls (based on the Soc2 report)
    - The assertion from the vendor's management regarding the effectiveness of controls
    - An overview of the vendor's infrastructure and services.
  - **SOC for Cybersecurity:** Provides an independent entity-wide assessment of an organization's cybersecurity risk management program to meet the needs of a broad range of stakeholders.

The Information Technology Security Evaluation Criteria (ITSEC) are European-developed criteria designed to assure customers that the products they buy have been evaluated by a neutral 3rd party. Are the security claims made by the cloud vendor accurate?

A Note on Architecture: ISO 17789 Cloud Computing Reference Architecture (CCRA)

An architectural design will explain how a cloud environment is designed - such as what hardware and software has been used and how everything is integrated to form a complete system. You have zero chance of ever seeing such documentation, but it is comforting to know that industry standards have been followed.



Security Concerns Worthy of More Than a Passing Reference

1. The customer should check that in a public cloud environment, one's data is reliably isolated from other tenants sharing the same resources. This isolation must be present throughout all infrastructure components including: host, virtual machine, compute, memory, network, and storage. Encrypting data is prudent if you have concerns here.

2. Most cloud services use what is called 'software defined networking'. Think of this as a means to control every facet of the IT infrastructure programmatically. Of course, the administrators who have these capabilities are extremely desirable targets for cyber criminals. A lapse in security here puts every customer at risk. This is why an adherence to a security framework is critically important.

3. Hypervisors are at the heart of every cloud. They contain the systems used by customers' day in, day out. Therefore, are they
   - Based on a 'hardened' template?
   - Is this template tamper proof?
   - Is the hypervisor Type I or Type II? (The former is considered more secure because of the absence of a potentially vulnerable operating system)?
   - Is the management of these systems securely locked down?

Part 2 of this article will be published on the 4th February 2021

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).