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 II

**PHASE THREE: Planning**

Before moving to the Cloud it is important to make sure you have classified every type of data your company uses based on its sensitivity and criticality. Doing so will help to ensure that the right levels of protection are put into place, such as:

- **Strong authentication systems:** In other words, only authorised individuals can access systems and data and they do so in a manner that protects their login credentials. Just as important here is the provisioning and de-provisioning of access rights. An employee, for example, may change role, function or department and it's critically important that they do not retain privileges which are not necessary to fulfil the current job role.

- **Encryption technologies**: To preserve the confidentiality of data as it travels from point A to B; when it is stored on disk or removable media or when it is being processed by any form of tech. You also have to realise that decryption will require the safe storage and management of encryption keys. Where these keys are stored is critical point. Best practice usually dictates that they are stored separately from the vendor – perhaps on your own network or another trusted 3rd party, despite the latency this causes.

- **Data masking, anonymisation or tokenisation:** This is to avoid any form of unauthorised disclosure by 'de-identifying' the data. For example, any information that helps to identify an individual might be removed or replaced with a senseless value.

- **Logical segmentation:** We have already noted that in most Cloud environments, resources are shared with other tenants. As such, our data must be isolated from others or even those within our organisation who do not have the necessary security clearance. It is possible for the CSP to achieve such segmentation programmatically.

- **Data loss prevention systems (DLP)**. These systems will examine what is trying to leave the cloud environment and decide whether or not this should be the case. Of course, this decision is based on scanning the data or labels associated with it and applying rules created by an administrator or the software vendor. For example, if the data contains a credit card number, it will not be allowed to leave the network.


DLP solutions are usually found on exit points or perimeter technologies. Whilst popular, they have some thorny problems:

1. Data in the cloud tends to move around and replicate this presents many challenges for any DLP implementation. Where are the end points? How do we find the data and label it?

2. The scanning of data creates latency.
3. There will be many 'false positives'. In other words, the system will often block access to files because it thought there was a problem when there wasn't. This is exacerbated when the data is not properly classified or segmented into specific repositories.
4. Once the data has left the network, the DLP system has no control over what happens to it.

- **Information Rights Management (IRM)** Enables an organisation to control what happens to a file even when it has left the network. Unlike DLP, IRM offers persistent protection. It is possible to monitor who accesses the files, when they do so, and whether anybody tries to access them without permission. IRM will also tell you whether the files are inside or outside the organization and will enable you to set up granular permissions such as who can read, edit, print, copy and paste files. You can even revoke access to files in real time if you don't want certain people to access them again. IRM is obviously a game changer in cloud computing.

- **Device security:** The biggest challenge here is that employees may use a wide range of different personal devices to access company data - which is a security nightmare. You must think carefully about how to protect your information on these 3rd party systems. Read our BYOD article here for more information.

- **Staff training:** Not only should you be teaching you staff basic cyber hygiene (good password management, using multi-factor authentication, updating devices as soon as possible, recognising social engineering from a mile away) you must also address security concerns specifically related to mobile working (theft of devices, the dangers of public Wi-Fi, the importance of using a VPN, or a privacy screen to prevent 'shoulder surfing').

In summary, the design of data security strategies requires an understanding of the key technologies at play, and collaborating closely with your cloud partners. How will data be encrypted? How will masking preserve the formatting of data? What sort of tunnelling is available? What backup arrangements do they have in place? And so on.

**In short: be choosey**

An organisation will want to engage with multiple CSPs and carefully evaluate their services, processes and support models to fit with their business requirements. For example, a fully managed CSP model may provide end to end implementation and be more convenient, but it will also be more expensive and won't provide complete visibility and control of the cloud environment.
Finally, never forget that where the data is stored and whether the vendor is GDPR compliant could mean the difference between using them and continuing your search.

**PHASE FOUR: Execution**

While moving to your cloud, you must always keep in your back pocket your business continuity plan (BCP) and your disaster recovery plan (DRP). The former is about keeping operations going when the IT resources you depend upon are not available and the latter is about getting these resources back up and running as quickly and as securely as possible.

**Business Continuity Plan**

The key ingredients of a successful BCP include:

- **A business impact assessment**: This identifies


- Mission Critical Functions (MCFs:) These are the things your business must achieve to survive.
- The identification and prioritisation of activities that contribute to these bigger goals.
- An assessment of what resources these activities depend upon (such as hardware, software, data and facilities).
- An estimate of how long the business can survive without these activities before irreparable harm is done (known as the Maximum Tolerable Downtime (MTD)).
- An estimate of how much data must be preserved to carry out these functions (known as the RPO).
- The methodology used to determine criticality.

- **A statement of importance:** Why the plan has the backing of the CEO and Board of Directors.
- **Guidelines:** On how and when to use the plan.
- **Contact list:** Of key personnel and 3rd party support as well as a description of responsibilities.
- **Communication strategy:** To disseminate important messaging and updates horizontally and vertically across the enterprise as well as to external agencies and partners. The strategy usually requires close collaboration between legal teams, public relations and senior management.
- **Step-by-step procedures:** To implement workarounds. This is the 'who' does 'what' and by 'when'.
- **A schedule:** For reviewing, testing and updating the plan.

**A disaster recovery plan**

Can be similar and will also include:

- **The scope of the plan:** To determine when the plan is relevant and necessary.
- **Roles and responsibilities:** Of the Disaster Recovery Team
- **Step-by-step strategies, processes and procedures:** To recover prioritised services. This means for each critical business function you outline:
  - Preventative/recovery actions that should be taken to back up or restore the CBF
  - Resources/equipment required to facilitate those actions
  - Recovery time objective (so you know how you quickly actions must happen)
  - Responsibility (who is in charge of making sure the actions happen)
  - A checklist that is used to assess the extent of the damage after a disaster and monitor the recovery process
- **The communication plan:** To facilitate the reporting of accurate information to the right people (which often depends on the type of disaster experienced)
- **A schedule:** For reviewing, testing and updating the plan.

**PHASE FIVE: Operations and maintenance**

Cloud governance embraces a number of different areas. For example:

**Risk monitoring**

Operating in the cloud requires the ongoing monitoring of risk.

A risk assessment usually involves the careful analysis of threats and vulnerabilities to determine the impact of a negative event on the business as well as the likelihood of such an event occurring. Unfortunately, lacking access to the CSP's security implementation strategy will make this difficult.

To mitigate the problem, a number of organisations adopt a cloud security standard, which provides detailed guidance regarding top security risks and the selection of controls. In no particular order we have, for example,

1. **ENISA:** Which covers risks such as vendor lock-in, compliance challenges, shared technology risks, and even hostile state actors.
2. **The Open Web Application Security Project (OWASP):** Offers the top 10 cloud security risks derived from open source intelligence
3. **NIST Cloud Computing Synopsis & Recommendations**: SP 800-146. Which is exceptionally comprehensive.

**Shadow IT**

Employees will often turn to shadow IT when they are prevented from accessing resources deemed necessary to do their job. Given that most cloud vendors make self-servicing quick and painless, it is essential that senior leaders introduce a framework for managing requests from the get-go. Good governance will require the implementation of a transparent process enabling the approval or rejection of requests based on compliance, cost-benefit and alignment with business goals and priorities.

**Base lining**

It is the responsibility of the cloud consumer to monitor cloud delivery. Typical metrics include:

- **Uptime**: Interestingly, an uptime of 99.9% translates into 42 minutes of downtime per month, during which you cannot provide a service to your customers. The Uptime Institute defines 4 tiers, each more stringent then the next to provide reliable, redundant systems for security, connectivity and fault tolerance. A Tier 4 certificate would be used by organisation who cannot tolerate any form of downtime.

- **Reliability:** The Mean Time Between Failures (MTBF) is the average time a service runs before failing. Meanwhile, the Mean Time to Repair (MTR) is the average time required to fix a failed service and return it to full functionality. Operational performance improves the more you know about these two key metrics, their causes and how to mitigate their risks. Paying attention to MTBF and MTTR will help you reduce overall cost of cloud services and increase overall efficacy.

- **Response time:** Response time is the time it takes for any workload request to be completed. This metric leads to better performance and has an impact on application performance and availability.

- **Security:** Cloud computing security refers to the set of controls based technologies and policies

You should try to document such baselines and confirm that they are consistent with the performance specified in the Service Level of Agreement (SLA).

## 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).