PHOENIX

Protecting Data in the UK Public Sector

Data is one of the most valuable assets that any organisation has. With the vast amounts of data that are held within the UK Public Sector, organisations can start to better use this data to improve the design, efficiency and outcomes of services that they deliver on a daily basis across government, healthcare, education and more. This data should therefore be at the forefront of your digital strategy ensuring that it is all protected and backed up to prevent any potential leaks or data loss when it comes to both staff, organisation and citizen information.

Data drives your organisation - How do you **protect** it?

Phoenix, in partnership with Dell Technologies, the Public Sector Executive and Bournemouth, Christchurch and Poole Council (BCP Council), set out to understand the challenges organisations face of 'where', 'how' and 'when' to secure their data. How does the Public Sector ensure that the correct systems and processes are in place to identify, protect and enable them to deploy consistent best practice.

Here's what we found ...

Classifying your data

Data classification is a vital component of any information security and compliance programme, especially if an organisation stores large volumes of information. It's impossible to maintain proper control if you don't know what information you have and where it resides and you cannot ensure the highest level of protection for your most critical assets if data is not classified according to its level of sensitivity and value. The first step is to develop a Data Classification Policy to define sensitive data and establish rules for its protection.

A Data Classification Policy is a document that includes a classification framework, a list of responsibilities for identifying sensitive data and descriptions of the various data classification levels. It does not include requirements for how the data must be handled. Rather, you should develop a separate document that defines the requirements for protecting each class of information.

23% of surveyed organisations **do not** have a Data Classification Policy

Where is your data **located?**

42% Cloud

45% On-Premise

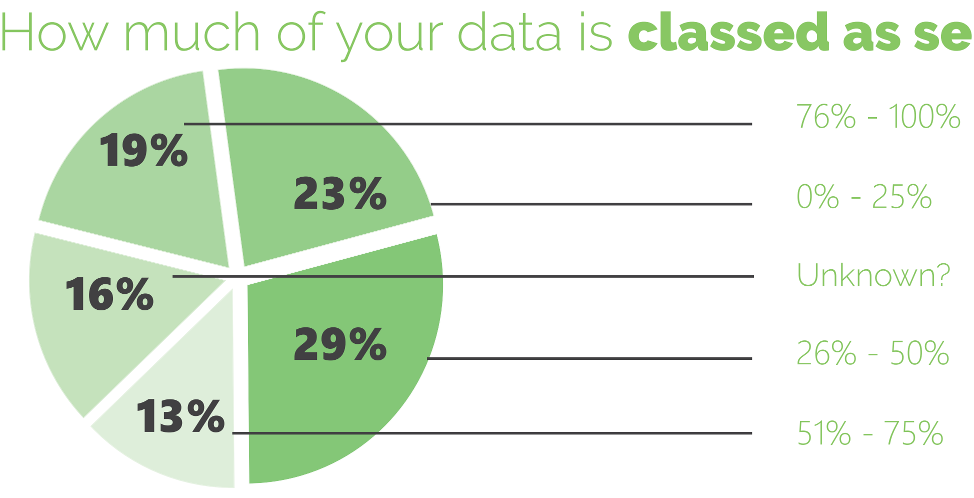
13% Unknown

Where is your data **managed** and **secured?**

35% Cloud

65% On-Premise

How much of your data is **classed as sensitive?**



How can you create a good Data Classification Policy?

- The classification criteria have to be straight forward to avoid ambiguity, but generic enough to apply to different assets in various contexts.
- It should contain point of contact for any possible edge cases and situations your employees may face. Depending on the organisation structure, it can be a Security and Risk Manager, a Data Protection Officer, a Compliance Committee or any other relevant person.
- It should be clear and written in simple language.
- It should fit in with the organisation's business
- It should be just a few pages in length and have no more than three or four classification levels.
- Finally, a good policy should contain a review schedule. Usually an annual review is enough, unless there are any external events, like new regulations coming into effect.

30% of Public Sector organisations **do not isolate data protection copies** as a preventative measure against malware

Cyber attacks have become a common occurrence, the worst of which often result in extended downtime that can bring operations to a standstill for days and even weeks – costing millions. While many large organisations have strong cyber security and anti-malware detection capabilities in place, the impact of not being able to recover business processes and data in the event of a successful ransomware or destructive cyber attack can be devastating.

By not isolating data protection copies, any requirement in the event of Disaster Recovery (DR) will simply carry forward any malware/ ransomware. By protecting the data protection copies, restores can be assured as virus free.

Business Continuity Planning is vital to ensure that your organisation can keep operating when disaster strikes. COVID-19 was a major example of this, where organisations had to adapt rapidly to new ways of working and at the same time a lot of Public Sector organisations saw a huge added demand on their services and expertise. COVID-19 highlighted the importance for all organisations to have a thorough, well tested and up-to-date Business Continuity Plan. Despite this we found that of those surveyed:

At least **1/3** have **no Business Continuity Plan**

68% **have not** conducted a **tabletop/audit** on their data BCP since the outbreak of COVID-19

In addition:

79% of Global Executives rank **cyber attacks** among the **highest risk-management priorities** for 2020[1]

Quickly recover your **data** and **systems**

With Dell Technologies Power Protect Cyber Recovery Solutions and Services you can rest assured that you are receiving the highest levels of protection, integrity and confidentiality for your data. With total assurance that if the worst was to happen and you were hit by a cyber attack, you could quickly recover all of your most critical data and systems. Modern data protection where and when you need it most.

Secure Data Isolation

Adaptive Analytics, Machine Learning and Forensic tools

Accelerated Data Recovery

Cyber Recovery Planning

DELL Technologies
TITANIUM PARTNER

PHOENIX

01904 562200 | hello@phoenixs.co.uk | www.phoenixs.co.uk

[1] https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html