WHY IS DATA MANAGEMENT YOUR RESPONSIBILITY?

dOdata: Why is data management your responsibility?

dOdata is a gathering of decision-makers, business leaders and captains of the digital arena who bring queries, solutions and experience to an intimate gathering willing to share their knowledge on data, digital and effective implementations of both.

The most recent dOdata event centered around information management and why the responsibility for an organisation's data and security lies with everyone, all the time. But surely if you're a CEO paying the big bucks for a CIO, all you need to do is sign off on his or her decisions?

Not so. Without buy-in from the C-suite and training that enhances every staff member's knowledge of the value of data and its security, a breach could happen at any time. Then, you're "herding water", which creeps in everywhere and looks for places to leak out, says SSA. So, what does your organisation need to know about your data so they can be part of your armour?

There is no silver bullet - data security not just a single solution that can to be implemented once and forgotten about and each organisation requires tailored solutions. It's also vital for everyone involved in data to understand that the question is not "When will there be a data breach?", but "What action do we take when there's a data breach?"

Agility in reaction and restorative actions

A data breach could come from the outside (malware, ransomware, hackers) or from within, inadvertently or with intent. Given that this is not a new topic, solutions that can be mapped out in your digitalisation blueprint should be both proactive and reactive.

Here are the questions the C-suite, governance and data teams should be asking:

Have we included reactive capability in our digital blueprint?

- What are your current reactive capabilities?
- How will all relevant teams be alerted?
- Will teams be reminded to alert stakeholders timeously where GDPR or other regulations require this?
- Do all staff members understand the importance – with regard to regulation and company reputation – of not sharing any information about a breach with any other parties?
- Who will be the spokesperson for the company in the event of a breach?
- Who will take the lead in ensuring business continuity, where required?

If you have all these answers in the positive and in the bag, you've done well so far. If there are still some leaky information management areas in your organisation – and there usually are – here are some steps you can take to protect your data assets:

- Define your crown jewel, the data that is the most important to your business
- Start armour-plating the outermost perimeter that could allow access to the jewel and move inward
- Review recent data breaches around the globe and understand that they, too, thought their crown jewel was protected; see what learnings you can gather from their mistakes or hackers' ingenuity

SSA believes the key areas to focus on with regard to managing and securing your data include:

Awareness – Make sure your teams are alert to the possibility of a breach
Process – What are the immediate actions that must be taken in the event of a breach, and who is responsible for taking them?
Diagnostic capability – Has this been mapped out in your blueprint and built into your system? Who is responsible for maintaining its efficacy?
Develop internal skills – It takes one staff member who doesn't understand your processes or data security to create issues that could cost you time, money and reputation. Is everyone trained to the best of their capabilities?
Preventative software solutions – Do you have an off-the-shelf solution? A partnership with an organisation adept at dealing with data and security management? If your solution is proprietary, do your governance and business continuity teams have access to the system?

We hope we've got you thinking about potential issues and their solutions. If you'd like to speak to an SSA data expert, we'd be happy to set up an appointment to ensure your organisation has the armour it needs for robust data management.

In SSA's next dOdata session, we'll be discussing information management as the competitive edge, rather than a grudge purchase.