Data assets at risk from IT Security mis-valuation

Ponemon research finds that IT Security underestimates the value of business assets by over 50%

Atlanta, United States, 11:00 GMT/6:00am EST, 28 November 2018: IT Security departments are incorrectly estimating the value of business information, leading to insufficient investment into the availability, protection and security of the most commercially valuable types of documents a business holds, according to new research from the Ponemon Institute.

The research, which was commissioned by leading data management company DocAuthority, surveyed 2,827 professionals in the United States and United Kingdom across seven functional areas. The results found that when asked to estimate the monetary value of different types of business information, IT Security departments undervalued documents including R&D and financial reports, whilst excessively prioritising less sensitive PII-related data.

This increases the chance of a major data breach, the mishandling of access rights for employees and the application of incorrect levels of security to low value documents:

- IT Security departments estimated the value of R&D documents at less than 50% of what the business would estimate their worth, predicting that it would cost $306,545 to reconstruct an R&D document compared to $704,619 as estimated by the R&D department itself
- IT Security departments also underestimated financial impact of a financial report being leaked, at $131,570 versus the $303,182 that the Finance department believes it would incur from this incident
- In contrast, IT Security departments overvalued monthly salary lists at $94,148, compared $57,477, the value attributed to the same asset by HR

"Typically, the security and protection of business data is considered to be the responsibility of the IT Security department. Yet it's clear from this research that IT Security does not have the vitally-important context required to understand the true value of that data, and in turn create an effective strategy for defending it," says Doctor Larry Ponemon, Chairman and Founder of the Ponemon Institute. "Rather than being relegated to IT, data and its protection should be the concern of not only management level, but the business as a whole."

Steve Abbott, the CEO of DocAuthority comments: "Only around 5% of data retained by businesses will be crucial to running the current and future organisation. Despite this, most businesses still apply unrepresentative, or 'one size fits all' levels of security to their data assets. Businesses need to consider how they can take a more strategic and cost-effective approach by identifying critical data that is worth security investment. Whilst a manual scan of unstructured data held by a typical 5000 seat organisation could take up to 400 years, Artificial Intelligence (AI) tools can help businesses identify and categorise data with an unprecedented level of accuracy, in a rapid timeframe."

Steve Abbott adds, "It's important to consider that obscurity around data could have far reaching ramifications. Despite company data being a hugely valuable business asset, organisations rarely have a clear view of what they own and what it's worth. As a result, within the context of a sale for example, data assets are likely to be overlooked as part of a business's valuation. We are confident that this will change as the business world starts to understand how data can impact a business's bottom line."

Notes to editors

Ponemon has developed a framework of six criteria to more accurately assess the value of corporate data. By assigning a rank of the importance of each element on a scale of 1 = not important to 10 =

essential, they have a better chance of aligning their security strategy with their most valuable assets:

- **Intrinsic value -** Pertains to how correct, complete and exclusive is this data
- **Business value** - Relates to how good and relevant is this data for specific purposes
- **Performance value** - Pertains to how does this data affect key business drivers
- **Cost value** - Refers to what would it cost the organization if the data was lost or leaked outside
- **Market value** – Links to what your organization can earn from selling or trading this information
- **Economic value** - Pertains to how the information contributes to the organization's bottom line

Download the full report here

About DocAuthority

DocAuthority is a leading document control solutions company. It offers organisations a broad, yet business-friendly, security policy utilising AI to help automatically discover and accurately identify unstructured and unprotected sensitive documents to help prevent them from falling into the wrong hands. DocAuthority works with enterprise-size organisations in all sectors including the healthcare, retail, technology, energy, public sector, telcos, services and financial services sectors to help these businesses understand the risk they face and design an effective mitigation plan to improve the security of sensitive data. Founded by Ariel Peled and Itay Reved in 2013, DocAuthority is a global company headquartered in Raanana Israel and is managed by the people who pioneered DLP.

To learn more about DocAuthority, visit www.DocAuthority.com.

DocAuthority Contacts

General enquiries:
Mike Quinn,
DocAuthority
E: mike.quinn@docauthority.com

Media enquiries:
XXXX
E: XXXX
T: XXXX