Five Strategies to Protect Your Company's Dark Data

This entry was posted in Cybersecurity | Data Protection | Guest Contributor *and tagged* Donnelley Financial Solutions *on December 12, 2022 by Editorial Staff*

By Dannie Combs, Senior Vice President and Chief Information Security Officer at Donnelley Financial Solutions

We're all familiar with the dark web and its treasure trove of stolen data, illicit products, and unsavory material. But what doesn't get as much attention, but is just as dangerous, is dark data.

Dark data is information that an organization collects, stores for compliance or other reasons, and then doesn't use, through neglect, lack of interest, or need. And the amount of data is rising exponentially. One estimate is that half of an organization's data may not be used for analysis. And as much as 80 percent of data is estimated to be unstructured, not analyzed, or used.

According to a recent report, in the first six months of 2021, there were 1,767 data breaches that exposed 18.8 billion data records. In addition, it's estimated that 25 percent of companies will incur a recurring material breach, costing an average of $3.8 million.

Few, if any, employees or executives may even know that dark data exists. It often consists of information that could be highly useful to criminals and profiteers, such as social security and credit card numbers, health data, addresses and phone numbers, emails, and old security videos. Phishing attempts and data hacks can easily expose millions of accounts to theft and resale on the dark web. And if that happens, a company can easily be exposed to lawsuits, blackmail, and a precipitous drop in positive public perception.

It's time for dark data to be exposed to the light of day.

In a recent report by Donnelley Financial Solutions, 70 percent of enterprise leaders surveyed believed that storing such data presents more risk than reward. And a majority—53 percent—of IT and C-level executives realize that dark data is potentially a great danger to their organization.

The good news is that there are steps that can be taken to mitigate the risk of dark data theft and even benefit from its presence. Here are five strategies that should be considered to harness, utilize, and protect your dark data from misuse:

Know what you have

If you don't know what data you have, you can't decide what to do with it. Employ task-specific software that can identify what dark data you possess and where it's kept.

Reduce the likelihood of malicious intrusions

Russian hackers have been able to penetrate government systems by scattering flash drives with the victims' company logo across a parking lot and mailing infected USB drives to unsuspecting employees. Educate your staff on phishing avoidance best practices. Ensure that all devices are updated with the latest operating systems. Scrupulously guard against phishing emails.

Follow government best practices for disposing of data storage devices

Ensure that any devices that store data, whether laptops, desktops, phones, or servers, are scrubbed before disposal. Alert all employees to the National Institute of Standards and Technology Guidelines for Media Sanitization as to how to overwrite, degauss and physically destroy media.

Educate your staff as to the dangers of dark data

While data theft is top of mind for many IT and C-suite executives, that's typically not the case for rank-and-file employees. The DFIN survey found that IT personnel are twice as likely as other departments to believe that storing dark data is riskier than the ultimate value it creates. Invest in software that automatically strips Personally Identifiable Information (PII) from your dark data storage.

Determine which dark data could actually be useful

Rather than simply eliminate all your unexamined dark data, set up protocols to determine which elements of it could actually be useful to be analyzed to improve your business.

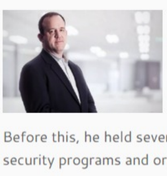
Employ new software tools to extract and protect your dark data

Look for a reputable and experienced provider of software solutions that can help harness and protect your dark data.

For example, DFIN offers a suite of solutions that includes:

- Data Protect Solutions that automate the finding and redacting of PII through pattern matching technology. Data can automatically be either redacted or anonymized.
- Venue virtual data room that secures the M&A process — which typically involves sharing thousands of documents — with an integrated auto-redaction software tool powered by AI and machine learning, securing data with 256-bit encryption, multi-factor authentication, and other tools, providing enterprise and supply chain security using multiple standards.
- eBrevia automated contract review software that uses AI to extract key provisions and data points from thousands of documents and employs bank-grade security and encryption to protect information.

Cyberattacks are only growing in frequency and severity. To prevent serious reputational and financial damage to your organization and your customers, it's imperative to take proactive steps now to educate your employees and institute automated controls that will protect all your data, both actionable and dark, from theft and misuse.



As Senior Vice President, Chief Information Security Officer, Dannie Combs has overall responsibility for cybersecurity, global data privacy, and IT Governance, Risk, and Compliance for Donnelley Financial Solutions (NYSE: DFIN).

Prior to joining DFIN, Dannie was the senior leader responsible for overall network security for U.S. Cellular, the fifth-largest U.S.-based wireless operator supporting over 20 million mobile subscribers. Before this, he held several senior leadership and consulting roles with a number of organizations to build and mature technology security programs and organizations as interim CISO, security architect, and more.

Most notably, Dannie is a 10-year veteran of the United States Air Force, where he served as a cyber threat specialist. During his time serving his country, he managed cybersecurity operations and information risk activities for military and governmental organizations as a member of the North American Aerospace Defense Command, National Security Agency, and Air Intelligence Agency, participating in missions ranging from homeland defense to offensive operations around the world. He served in the Balkans during the Yugoslav conflict, assisted with national defense efforts in South Korea, and supported intelligence and counterterrorism missions around the globe, including working in conflict zones such as Iraq and post-9/11 Afghanistan.

Dannie is an advisory board member of ReliaQuest, FishtechGroup, and the Boy Scouts of America.

He is based in Chicago.