CYBER DEFENSE MAGAZINE

eMAGAZINE

JANUARY 2023

In This Edition

4 Key Security Trends For 2023

New Threat Report Shows Attackers Increasingly Exploiting MFA Fatigue

The Future of Online Privacy

...and much more...

MORE INSIDE!

Does Your Company Have a Dark Data Problem?

By Dannie Combs, SVP and Chief Information Security Officer, Donnelley Financial Solutions (DFIN)

Don't let the name fool you: dark data is all too visible — to bad actors, that is.

Dark data is information that a company stores but doesn't need any longer. Businesses are often surprised by just how much of this data they have squirreled away in their computer systems — on laptops, file servers, smartphones and in suppliers' systems as well.

It consists of everything from ex-employee files, outdated customer records, phone numbers and email addresses to credit card numbers, SSNs, healthcare records and even old security videos.

Companies often treat this information like they would old boxes in the attic — something they'll deal with "tomorrow", if ever. That's a mistake. Dark data is extremely valuable to cyber criminals, who will go to great lengths to steal it for a variety of disreputable purposes. They might sell it, use it to perpetrate financial fraud, even commit blackmail. And when they do, your company could suffer substantial reputational damage and even be subject to legal liabilities.

There is evidence that businesses are beginning to realize the dangers. According to DFIN's new report — Understanding Risk: The Dark Side of Data — nearly 70 percent of enterprise leaders surveyed said that storing detailed information presents more risk than value to the overall enterprise. And more than half — 53% — of combined IT and C-Level respondents said dark data is an extremely pressing issue.

Enterprise leaders must identify dark data and decide whether to store it, protect it, or purge it. A few tips:

Shine a light on your dark data

The best way to understand the data you have and how it should be protected is to bring it to light. Choose software that explores the dark recesses of your enterprise to identify and surface dark data.

Foil phishing attempts

Phishing is becoming more prevalent, so much so that services now exist that allow scammers to easily target and exploit audiences. Indeed, 52% of our survey respondents said phishing incidents had greatly or somewhat increased and were also the most common form of potential breach. Ensure that your most sensitive information is properly secured and even redacted to safeguard it from falling into the wrong hands.

Scrub assets before disposal

When disposing of or donating dated hardware and devices, ensure that they are properly scrubbed of all business information. Familiarize yourself with Secure IT Asset Disposition processes and identify an appropriate partner to manage this for your organization.

Limit access to personal information

Avoid giving the keys to the kingdom to everyone. Increase security around and even redact sensitive information, like Social Security numbers and credit card information, making them only accessible to chosen high-level employees. Doing so helps decrease the chance that such dark data purposefully or inadvertently leaks.

Educate employees on potential cyber threats

No matter where you do business, data privacy regulations are tightening, and

enterprises can suffer multi-million-dollar fines for non-compliance. Protect your assets by raising awareness company-wide and by investing in software that automatically redacts personally identifiable information (PII) and other sensitive data.

Choose a partner that understands your security posture

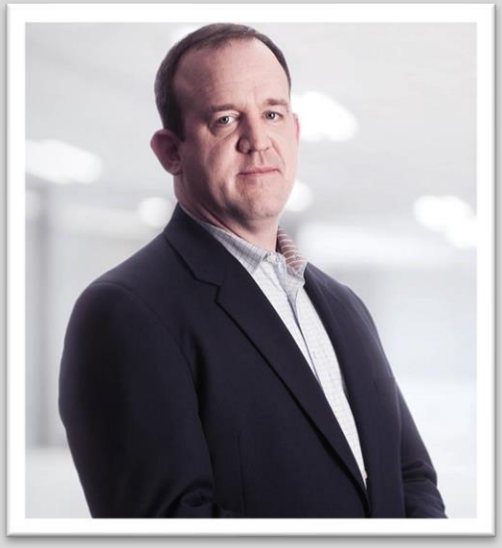
Cybersecurity software can augment your company's security professionals. Choose a software provider that understands and can meet and even exceed your cybersecurity needs.

For example, DFIN has a suite of solutions that is helping clients today.

- Data Protect Solutions automate the finding and redacting of PII.
- Venue virtual data room 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.
- eBrevia contract review software has AI engines for scanning contract language to ensure that expected controls are embedded in supply chain agreements.

Cyber-attacks are on the rise for a very good reason: they are very lucrative for the criminals who perpetrate the crimes. In the months and years ahead, we expect that these bad actors will increasingly target dark data. If you take appropriate steps now, your company can avoid becoming a victim.

About the Author



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 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 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 an advisory board member of ReliaQuest, FishtechGroup, and the Boy Scouts of America. He is based in Chicago. Dannie can be reached at dannie.combs@dfinsolutions.com, through LinkedIn at https://www.linkedin.com/in/danniecombs, and at our company website https://www.dfinsolutions.com/

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com

*** with help from writers and friends all over the Globe.**