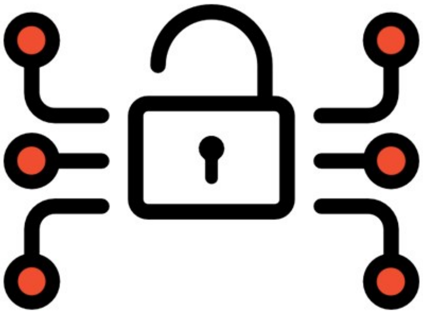
Assess and Reduce Cybersecurity Risk with FileFacets

According to a recent report, despite a 79% increase in IT security spending, 67% of global enterprises (71% in the U.S.) have been breached at some point in the past. In fact, nearly half (46%) of U.S. respondents and 36% of global respondents reported a breach in just the past year.

Today's businesses face challenges of securing vital proprietary information, determining the risks of data breaches, and developing a workforce culture that understands the greatest threat to data loss: privileged users (insider threat). According to this same report, global companies rated insider threat as the most dangerous threat actors, even more than dedicated cyber criminals (58% versus 44%).

Corporations must invest in effective and efficient electronic data protection and risk assessment technologies and processes. FileFacets' unique, first-to-market software streamlines discovery in a cloud-based, AI-backed, reusable solution to deliver:

- **Mitigated risk**
- **Increased efficiency and effectiveness**
- **Increased value**



Why Is Cybersecurity Important?

The lifeblood of every business in the Information Age resides in the data within the files it manages and secures. Safeguarding organizational and client data from origination through archive is of the utmost concern for ensuring protection of the business, its clients, data, and proprietary information—regardless of industry.

The impact of a cybersecurity breach is monumental. A look at breaches in just the past seven years reveals an exhaustive and expensive list of companies that have suffered massive data loss. From breaches at the U.S. Office of Personnel Management to Yahoo, from Uber to Home Depot, data losses have affected billions of people, eroded public trust in corporate and government entities, and cost billions in lost value, fines, and reparations.

In one notable example, Yahoo's breach was discovered during the company's sale in 2014 and dropped the value by $350 million. In another example, Uber's valuation dropped $20 billion after discovery of a breach in 2016 (though not the only reason for the devaluation).

Clearly, businesses must effectively manage and protect their data, systems, applications, and the risks associated with them all. Deliberate investments in file management and data protection solutions will reduce risks and increase value.

How Do FileFacets' Solutions Lead to Greater Security?

Not merely an issue for the IT team, data security deserves C-level scrutiny because data is critical to every aspect of an organization. File management is an enterprise-wide concern and should be a vital objective supported across the executive boardroom. You can't protect what you don't know you have.

FileFacets' file management solution provides multiple data security and risk assessment advantages:

- ✓ **File Profiling:** FileFacets identifies document types and assigns risk profiles based on the type of document and the probability it may contain personally identifiable information (PII—to protect your clients) or proprietary information (to protect your organization). AI based, the more files the solution scans, the more accurate the profile process becomes.
- ✓ **Risk Assessment:** FileFacets' solution assigns financially quantifiable risk levels to specific document types: contracts, invoices, research, legal memos, etc. For example, an employee has a contact list on her computer with 400 names (including phone, email, address info). The company may set the value of each contact as $10,000 worth of business; thus the contact list is worth $4 million.

  Furthermore, organizations using this risk framework can determine the value of information on individual laptops should anything happen to the data—and assign limits to the amount of risk acceptable for specific employees based on position and tenure.
- ✓ **Mitigating Insider Threat Risks:** When discussing insider threats, many people immediately think of actors like Edward Snowden—agents embedded into government or corporate institutions who deliberately expose data harmful to the organization and its employees. But much of the insider threat results from accidental or unsuspecting employees who share or expose data via inattention or honest mistakes. Companies that employ deliberate and rigid security protocols for data can help mitigate risks from both deliberate and accidental actions.

The power of FileFacets' solution resides in the data within the cloud. Each data scan added to FileFacets' Feature Matrix helps to refine the definition of file types. This cumulative and continuous learning combined with distributed processes allows more applications and clients access to the benefits from AI and machine learning.

This solution does not transfer files off resident network. Instead it scans files within your entire IT architecture (cloud networks, file shares, enterprise content management systems, user endpoints) to identify, encode (with hash codes), and encrypt before transmitting the code to the Feature Matrix in Microsoft Azure®*. This matrix is analyzed to build a Document Type Prediction Model specific to each customer.

Regardless of industry or organization, data security through deliberate and successful file management is the superior approach to increased value, efficiency, and security while reducing risks. Invest in FileFacets and leverage our solution across your security protocols to protect your data, your employees, your clients, your reputation, and your business.

At FileFacets, we believe in helping our clients maintain and optimize their file management solution. We provide organizations with a state-of-the-art, automated, and intelligent, cloud-based solution to help protect their data. Learn more about how we can help at www.filefacets.com.

*****Microsoft Azure® is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through a global network of Microsoft-managed data centers.