The average consolidated total cost of a security breach for a company, according to independent research group Ponemon Institute, is $3.8 million. In 2015 alone, breaches rocked the healthcare, financial, and higher-education industries, to name just a few. And while many data breaches are caused by cyberattacks, experts agree that many more are the result of human error. We all know how easy it is to leave an unlocked smartphone sitting unprotected on a store counter or send an email with the wrong attachment.

"The world has changed. We need tools to create a secure environment, but we also need to facilitate collaboration, growth, and the appropriate relationships that drive business forward."

-Information Security Service Area Leader, Global Consumer Packaged Goods Company
Risky Business

Security breaches due to these kinds of “oops” moments are likely to contain thousands of documents, but even if they contain only a few—and the few contain sensitive information such as a trade secret, research and development for an innovative product design, or strategic acquisition plans—their exposure can have dire consequences.

Meanwhile, the engine of productivity depends on sharing this kind of information. While locking it up might keep data safe, it would also stifle collaboration and growth. Even for companies that have invested millions of dollars in state-of-the-art manufacturing equipment and a top-notch global workforce, business data—whether personal identification customer data, proprietary information, or intellectual property—is still one of their most valuable assets.

Secure Business

This is the case for a one-hundred-year-old consumer packaged goods enterprise known for its universally loved confections. For a company of this size, with 75,000 employees in six distinct business segments across more than 74 countries, daily operations are complex, and collaboration is critical to innovation and service delivery. “The world has changed,” says an information security service area leader at the company. “We need tools to create a secure environment, but we also need to facilitate collaboration, growth, and the appropriate relationships that drive business forward.”

Unwilling to face what they considered a false choice between security and productivity, the company’s IT staff decided to raise both as priorities to the enterprise level and address them holistically. To do this, its top executives began using Microsoft Rights Management Services (RMS) so they could work easily and safely with highly confidential business information. “RMS lets us securely transmit, transfer, and store sensitive documents throughout the organization, especially if those documents need to be consumable at any time, whether by the board of directors, the presidents group, or any of our segments. It’s critical. We have to have security and accessibility at the same time,” says the company’s IT security service area leader.

Spreading the word

To influence user behavior and facilitate the same shared goals of security and productivity across the entire workforce, the company plans to expand RMS to all of its 75,000 associates over the next three years. The goal is to increase every employee’s awareness of universal data classification and data loss prevention policies, which means the company will have thousands of people working toward improving security.

Because RMS sets universal security policies and procedures beyond simple password protection and file zipping, employees can easily and securely manipulate, transmit, and store confidential information internally across what have traditionally been data-silo boundaries and externally with vendors, customer, and partners.


---

Industry: Consumer Packaged Goods
Country or Region: United States, United Kingdom, Russia, China, parts of Europe and South America
Employee Size: 75,000

Customer Profile:
This large consumer packaged goods company is based in the US with operations in 75 countries and 75,000 employees around the world. It has net sales of more than $30 billion and six business segments including confections and pet food.
“With the increased capabilities of Microsoft RMS, we can begin looking at ways to decrease the need for peer-to-peer federations when exchanging protected documents with third-party organizations,” says the IT security service area leader. By applying the same security controls, including two-factor authentication, for everyone, the company has a consistent and enterprisewide solution that works even across its segmented geographies and business sectors. This way, emails are protected against unauthorized access, and—because the file itself is protected—the information is safe, whether it is online or offline. The company’s IT staff can also identify, monitor, and report metrics pertaining to sensitive data.

IT security as collective effort

As employees understand the magnitude of their role in data security and the ways they can prevent data loss, they become agents for enterprise welfare and safety and, at the same time, remain productive. IT no longer has to address security on an individual use case. By deploying RMS and integrating data protection policies and protocols throughout the organization, the company can clamp down on security without clamping down on productivity.

Software

- Microsoft Rights Management Services

Here is the IT security service area leader again: “Security and IT have quickly become the forefront of business decisions. We are sought out for advice on technology strategies that now integrate with business strategies.” As a part of its data protection campaign, this global company is aligning security protocols to the needs of the business and redefining information security so that it is no longer merely an IT problem but a critical part of business strategy and an enabler of collaboration and growth.