Solution Showcase

Micro Focus Aims Its Lens on Business Drivers for Data Privacy

Date: August 2018 **Authors:** Edwin Yuen, Senior Analyst; and Monya Keane, Senior Research Analyst

Abstract: With the arrival of major U.S. and international regulations that have touchpoints to data privacy, organizations must turn more attention to data discovery. They need to know what they're storing digitally, exactly where that information resides, and how much of it is subject to which regulatory retention/preservation rules. In other words, they need a secure content management system that helps them discover and classify their data, retire it as appropriate, and ultimately, meet all data privacy obligations. Done wrong or not at all, the risks can be frighteningly costly. But done right, the operational rewards can be high.

Introduction

Compelling business needs and clear, basic logic are forcing organizations to be very thoughtful about how to effectively protect the sensitive, high-value data they create, collect, and manage. To comply with data privacy regulations that are here and that will inevitably arise, it is vital that these organizations adhere to a process *that begins with data discovery* to identify areas of information risk.

At almost every company these days, a lot of data is "out there" in all sorts of locations, sitting on traditional on-premises storage, on SharePoint or other cloud-based apps, on tapes offsite, on users' endpoints, and so on. Some of the data might be old, obsolete, and have no privacy-related characteristics. Other data might be newly created and/or must be secured according to regulation(s).

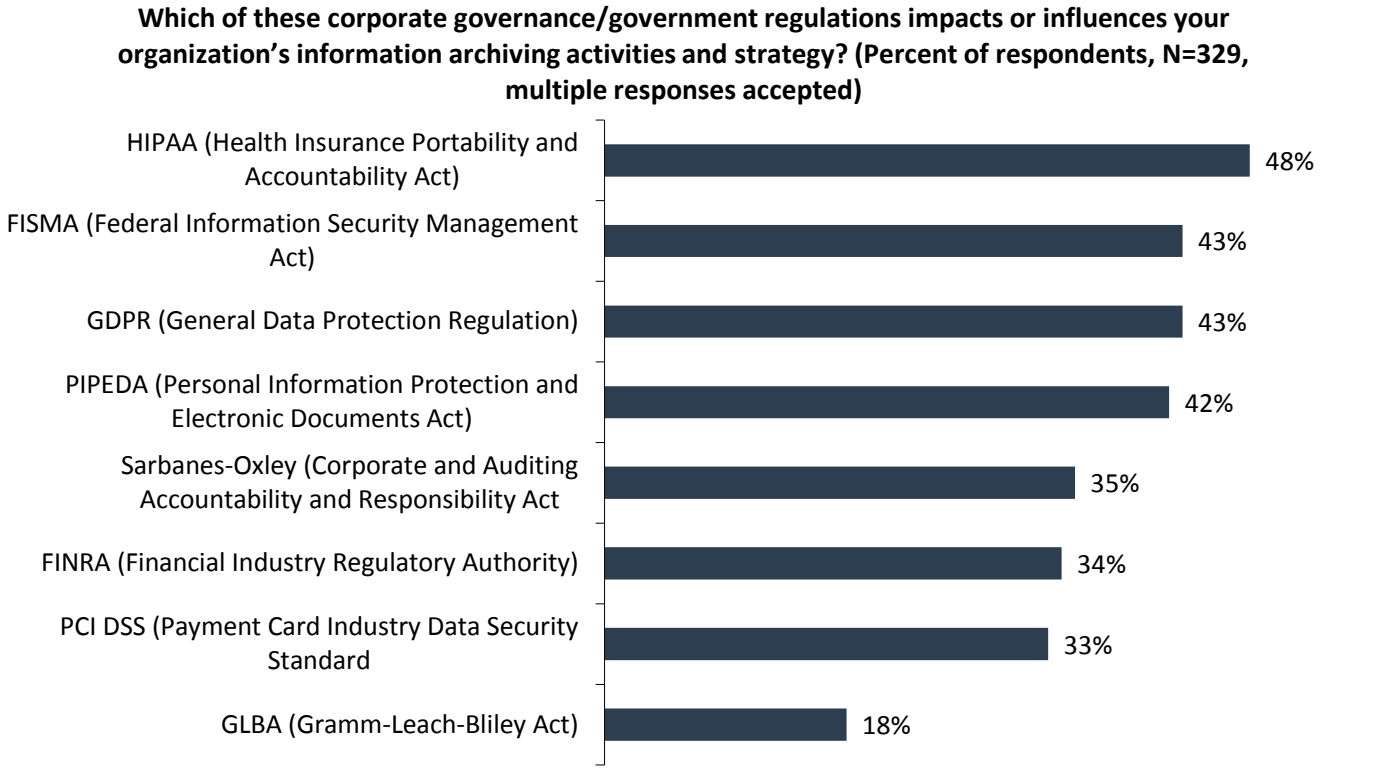
Many data privacy and retention rules (from official laws to internal audits) tell organizations to identify "everything" applicable. That demand can be difficult to satisfy. A lot of companies, for example, aren't sure where every piece of their Payment Card Industry (PCI) or Personally Identifiable Information (PII) data might be stored. It's a real problem because before an organization can protect its data, it has to have a complete picture—it needs to know not only where all the data resides, but also what its privacy-related characteristics are. So, the following activities have to happen:

- The first step in overcoming the problem is to initiate a data discovery effort, preferably with the help of a system powered by artificial intelligence and machine learning.
- Step two centers on parsing through those discovered data stores, formally classifying which pieces of data apply to a given regulation, and which pieces of data aren't important and thus don't require special protection handling.
- After finding, categorizing, and filtering the data, the organization's third step should be to use its secure content management solution to help analyze, manage, and govern that data on an ongoing basis to mitigate risk and preserve and protect the information appropriately for the long term.

Still More Work to Be Done

Most of the IT managers surveyed by ESG in late 2017 felt they still had more progress to make before they could feel confident about the compliance status of their organizations. For example, only 11% of them reported they felt fully prepared for the May 2018 arrival of GDPR.[1] That regulation has received an overload of press coverage, but it's only one of many regulations affecting decisions about organizational data privacy and archiving strategy (see Figure 1).[2]

Figure 1. A Sampling of Corporate Governance Regulations Influencing Data Privacy



Source: Enterprise Strategy Group

Notably, in 2018, California's legislature enacted tough new rules that are practically guaranteed to have a sweeping, far-reaching impact. The California Consumer Privacy Act (CCPA) goes into effect in 2020 and will cover any company that:

- Does business in California and collects California residents' personal information in the course of business.
- Has annual gross revenues of more than $25 million.
- Buys, receives, sells, or shares the personal information of 50,000 or more California consumers, households, or devices.
- Derives 50% or more of its revenue from selling consumers' personal information.

Those companies could actually be based in Miami, Sydney, or Tokyo; it doesn't matter. If they receive personal data from California residents and meet even one of the criteria above, they will have to comply with CCPA. Companies that do not may have to pay damages between $100 and $750 per California resident, which, in the case of a major data breach, could amount to fines in the millions.

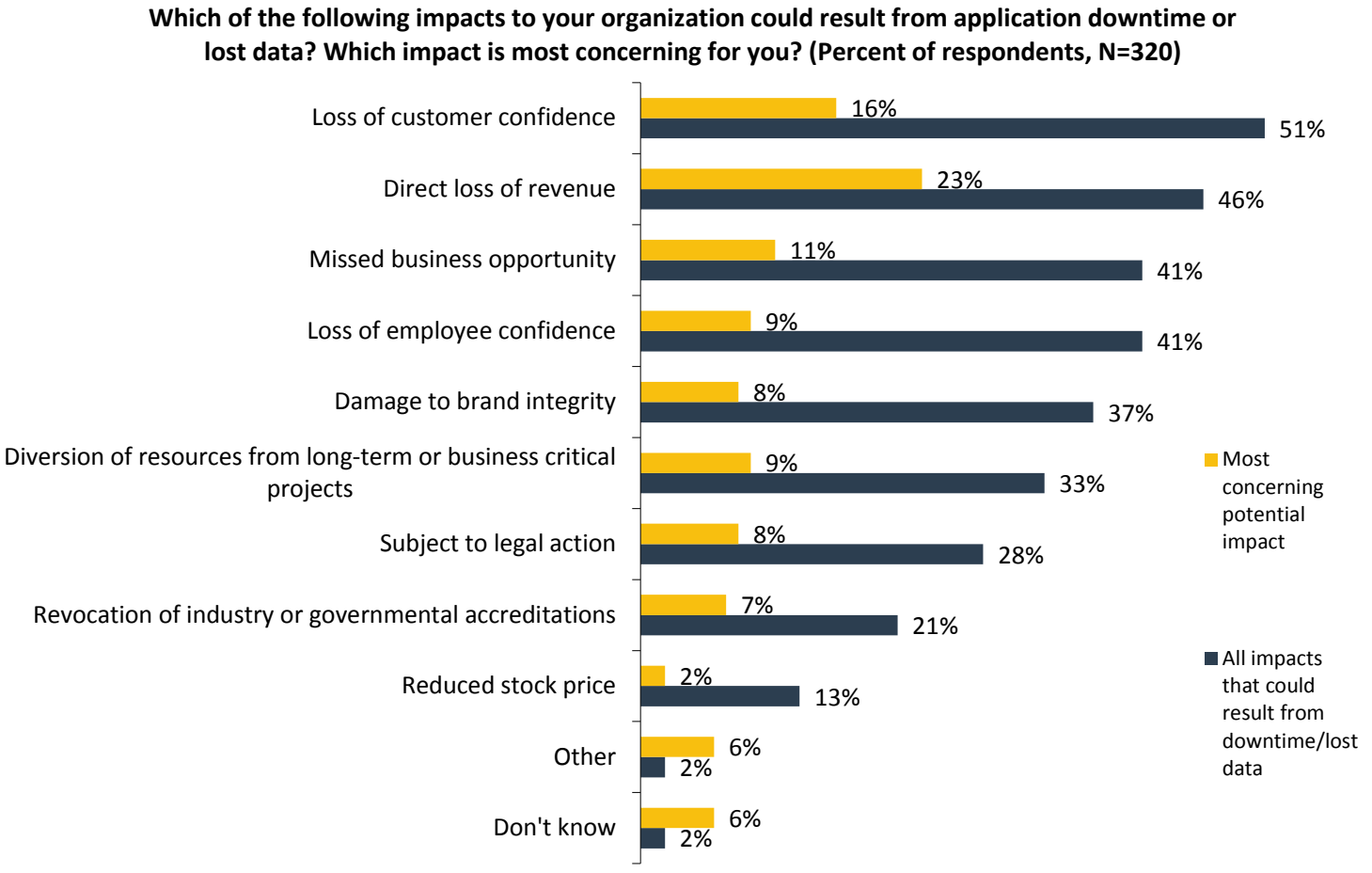
[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.
[2] Source: ESG Master Survey Results, *Copy Data Management Trends*, March 2018.

As mentioned, most organizations confronted with data privacy rules and regulations don't actually know where all their data is, how much of it is relevant to which regulations, and where potential risks might be hiding. What they do know is that it is imperative to do a better job of securing, identifying, classifying, and processing their data for privacy compliance. Consider that a combined 82% of IT managers told ESG their companies' senior executive teams were either concerned (51%) or highly concerned (31%) about GDPR and the exposure it could bring.[3]

The Risks of Non-compliance

When data becomes unavailable or is lost, hacked, or otherwise improperly exposed, regulatory non-compliance can result. Failing to properly protect, secure, and encrypt everything effectively carries significant risks of sanctions, fines, reputational damage in the media, and general business disruption. For example, the potential outcomes resulting from non-compliance stemming from excessive downtime or lost/leaked data are quite serious and damaging—even extending to negative legal exposure or the revoking of accreditations a company might need to stay in business (see Figure 2).[4]

Figure 2. The Negative Outcomes of Application Downtime or Data Loss



Source: Enterprise Strategy Group

The Rewards of Compliance

The good news is that if an organization dedicates itself to using high-quality technology to help it remain compliant, that organization will also enjoy some nice ancillary benefits—enhanced operational efficiency and a better revenue outlook.

[3] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, February 2018.
[4] Source: ESG Master Survey Results, *Real-world SLAs and Availability Requirements*, May 2018.

Reward: Enhanced Operational Efficiency

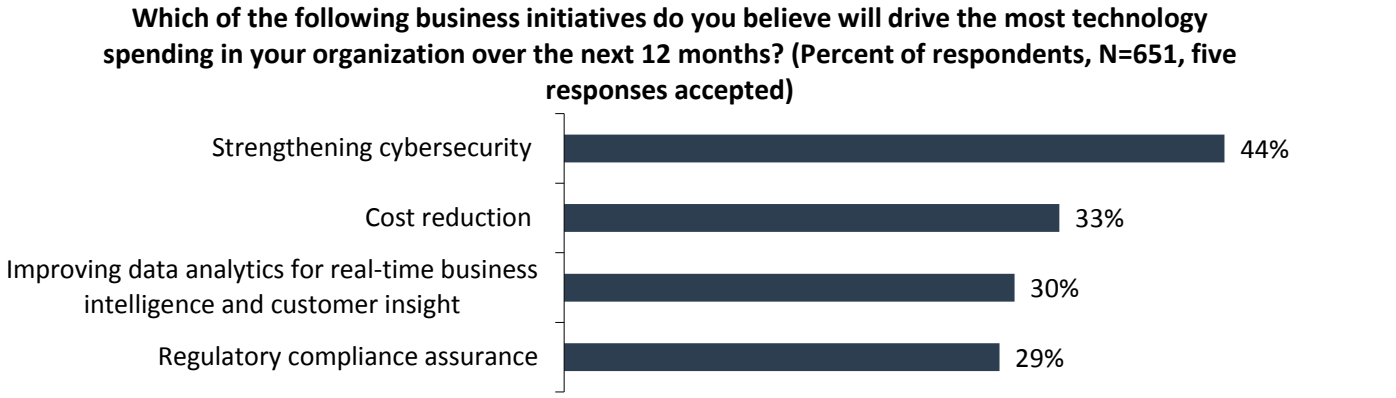
These organizations won't need nearly as much time to achieve and maintain compliance because their software tool does the hard work of fast, accurate identification and discovery of all affected data. The time saved can be used to accelerate other business activities: legacy-data cleansing efforts, cloud initiatives, mergers and acquisitions, etc.

Any time a business moves in a new direction through acquisition, digital transformation, or some other high-priority activity, it is usually necessary for it to absorb more data. Having the luxury of knowing exactly what and where all of that new data is would give the company substantial compliance *and* efficiency advantages.

Consider an acquisition, which is a complicated endeavor in itself. But, when the company doing the acquiring has to struggle to discover all the data its acquired company accumulated over the course of its existence, a complicated endeavor becomes impossibly intimidating. Having a good discovery tool at hand makes the whole effort simpler.

It is interesting to note that nearly three in ten ESG survey respondents (29%) cited regulatory compliance assurance as one of the five business initiatives most driving their organization's technology spending this year (see Figure 3).[5] These IT managers seem to appreciate that being as efficient as possible in assuring regulatory compliance brings many benefits and thus is a business initiative worthy of investment.

Figure 3. Top Four Business Initiatives Driving IT Spending in 2018



Source: Enterprise Strategy Group

Unfortunately, ESG uncovered another notable finding—namely, that an industry-wide skill shortage exists in the area of compliance expertise. Twenty-five percent of survey respondents said their IT organizations are encountering problems finding and retaining administrators experienced in compliance management, monitoring, and reporting.[6]

If those organizations lack enough in-house expertise, incorporating a good technology solution into their environment addresses the issue. If you can't find the right personnel, intelligent software can serve that function, in part, instead.

Reward: Meeting or Surpassing Revenue Goals

In the past few years, ESG has observed with increasing frequency that connections exist between enhancing one's IT infrastructure with leading-edge technologies (including technologies for data discovery) and meeting or exceeding revenue targets. Specifically, such organizations are more likely to hit their revenue-related goals because:

- Other companies really want to work with them—they want to engage with partners and buy from sellers *who they are sure are compliant* and free from messy, looming issues related to regulatory adherence. Essentially, compliance can translate into competitive advantage.

[5] Source: ESG Research Report, *2018 IT Spending Intentions Survey*, February 2018.
[6] ibid.

- When an organization has a clear idea about the classification and characteristics of all its data, then that organization finds it easy to extract suitable data subsets from the overall datastore for use in activities such as machine learning or analytics/data mining. It's all about getting maximum use of all data assets. When the organization understands where its data is and what the data's distinctive qualities are, then that organization moves into a better position to leverage the information for all sorts of beneficial, revenue-boosting uses.

The Micro Focus Secure Content Management Suite

Pure-play software company Micro Focus was formed to help companies embrace innovation while managing risk. Its Secure Content Management Suite certainly seems to have potential to bolster the effort. The SCM Suite is composed of three offerings:

- ControlPoint—unstructured data file-analysis software to discover, classify, and automate policy adherence.
- Structured Data Manager—data archiving software to retire outdated applications and reduce data footprint.
- Content Manager—policy-based governance (enterprise content management) software to help the organization meet its regulatory and privacy obligations.

These products can work in combination to help an organization adhere to the "three axioms of managing risk" identified by Micro Focus:

1. You can't protect what you don't understand.
2. You can't protect everything all the time, nor should you.
3. Proactively protecting your data and organization with modern IT and analytics makes the most business sense.

The SCM Suite provides file analysis, structured data management, and governance-based enterprise content management, resulting in an offering that should satisfy all the organization's needs—not just collaboration and productivity needs, but also the crucial need to maintain data security, privacy, and compliance responsibly, without breaking the budget. According to Micro Focus, it deliberately engineered the SCM Suite in part to offload legacy systems and thus reduce TCO and contain costs.

This Isn't Traditional ECM Software

Enterprise content management isn't new, so what makes SCM different? Overall, it is the suite's enormous emphasis on security. But additionally:

- It is holistic—With the SCM Suite, organizations are able to understand, classify, and control virtually all types of enterprise data and secure it all within a single ecosystem.
- It is integrated—The SCM Suite was engineered to provide interconnectivity between file analysis, structured data archiving, and content management. That interconnectivity eliminates error-prone manual handoffs and allows for very low-risk, automated governance for legacy and new information alike.
- It is based on analytics—The SCM Suite disambiguates the data to deliver deep information insight and granular, intelligent classification.

Micro Focus SCM

A solution suite with risk management and analytics at its heart

- Content analysis identifies sensitive or high-risk data. That data is categorized and has policies applied to it to govern access and retention.
- A powerful search engine makes it easier to find the data you need, as permitted.
- Unstructured content can be managed in-place or moved to a secure repository.
- Structured (i.e., database) data has security and access controls applied prior to intelligent archiving.
- Real-time access and reporting are supported without the need to use legacy applications.

In general, pursuing and adhering to a secure, policy-based governance approach for legacy and active data using the SCM Suite to facilitate the effort should put an organization in a good position to deal with changing and evolving regulations, including the recent GDPR rules.

The Bigger Truth

A company using the SCM Suite gets a core benefit of regulatory compliance as well as all the good things that come with it: no fines, no media shaming, no lawsuits filed by people whose private data was exposed, etc. But in addition to improving its compliance stance, that company enjoys other business benefits, simply because it knows so well what it has.

The SCM Suite appears to deliver a nice range of benefits: It proactively prepares organizations to meet evolving worldwide requirements for protecting and governing data. It helps them achieve deeper insights into regulated and sensitive information. It automates policy enforcement using advanced analytics to protect the right data the right way.

But this is about even more than securing what matters most with an analytics-powered, integrated solution. The nice range of benefits listed above can, in turn, also give an organization more power to manage its bottom line and drive its top line for better business results.