Data Risk Management in 2018: What to Look for and How to Prepare

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for IBM

May 2018

EMA™

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

Navigating the threat landscape in 2018 is complicated, not only by the ever-changing tactics of attackers, but also by the looming enactment of the European Union's General Data Protection Regulation. As security practitioners attempt to steer clear of such complications, they will have to find ways to interact effectively with executives and boards of directors who are increasingly taking a more proactive role in understanding the risks associated with their organizations' digital assets. The effort to better manage those data risks requires greater coordination across organizational boundaries, an examination of what constitutes the company's crown jewels, where they exist, and how they are handled across the organization. With those insights, security practitioners can more effectively prioritize their protections (and budgets) instead of trying to boil the ocean and protect everything.

Introduction

The face of data risk management in 2018 appears to be a bit older and more mature thanks to changes in the threat landscape, looming legislation that promises to bring greater focus to the practice, and an increase in the amount of attention being paid to cyber security by the C-suite and board of directors. Among many security practitioners, it's understood at this point that it is not a question of *if*, but *when* sophisticated attackers will breach their security defenses. If cyber security was not already a board-level issue for some companies, epic security failures on the part of certain large organizations in 2017 cemented that fact. From failure to patch critical vulnerabilities in a timely manner to a lack of visibility or awareness of who is doing what with the organization's crown jewels, the big breach headlines brought increased scrutiny on security and risk management practices from the board of directors. Some of these failures even caused a few C-suite players to lose their jobs. If it's true that the past is a prologue to the future, more CEOs could lose their jobs over such fiascoes in 2018.

Among security practitioners, it's understood that it is not a question of *if*, but *when* sophisticated attackers will breach their security defenses.

Is GDPR on Your Radar?

One of the big unknowns of 2018 is how the enactment of the European Union's forthcoming General Data Protection Regulation, due to go into effect on May 25, will impact organizations that handle personal data about European citizens. The industry hasn't seen any significant compliance mandates as far-reaching as GDPR since the adoption of the PCI DSS standard in 2007. The GDPR's prescribed fines for violations are very stiff, and many organizations are behind in preparing to satisfy GDPR mandates. Although audits for compliance are not quite as likely, any breach that exposes European citizen data, or any complaint filed by a European citizen, could result in serious monetary damage to the company held responsible for its exposure. What's not clear is whether European regulators will seek to make an example of any U.S.-based company responsible for such data loss, or act with leniency if the organization shows it made a good faith effort to comply.

In addition are the ongoing risks associated with the continued popularity of ransomware attacks, such as Wannacry, increasingly sophisticated phishing schemes, and the rise of nation-state attacks.

Asking the Hard Questions

As executives and boards of directors increase their scrutiny of security practices and controls designed to protect against all these dangers to critical data, what questions are they–and should they be–asking to ensure protections are adequate?

For an increasing number of large organizations, boards are asking such questions as:

- What are our critical assets?
- Do we know where our most sensitive assets are?
- Do we know who's accessing them?
- Do we know if we have enough controls protecting these assets?

Board members should ask CISOs if they know what the most critical business assets are in each line of business.

Although that is a good start, there are additional questions board members and CEOs should ask to better understand whether existing controls and practices are enough, whether they are focused on the right data sets, and whether processes need to be altered to improve the organization's security posture. Here are a few examples of questions board members should ask:

- Does each line of business understand what their most critical business assets are?
- Does our cyber security program line up with our business objectives?
- How do we measure the efficacy of our cyber security efforts?
- How are we doing compared to our competitors?
- Are our priorities for spending on cyber security appropriate?

The Accountability Gap

The answer to that first question is usually no, and there are a multitude of reasons why that's the case. The primary reason is because there is an accountability gap in who's responsible for protecting the organization's most critical data, or its crown jewels. Although the CISO is viewed as having that ultimate responsibility, he or she does not actually own that data. Nor is the CISO privy to what that data is, where it is located, and who has access to it.

More often than not, custodianship of critical data assets is lodged within a large organization's lines of business (LOB), and the leadership of each LOB is charged with determining acceptable risk levels for that data. Unfortunately, without a big-picture view of critical data risk, the risk is equated with not meeting financial or other business objectives rather than avoiding data threats. Spreading the task of managing data risk across multiple units, departments, and stakeholders means there is no clear line of accountability.

At the same time, the diffusion of responsibility for managing data risk also makes it impossible for the CISO and his or her team to prioritize securing the organization's crown jewels. Few cross-organizational security teams actually know where the most critical data is located, and they often lack a complete understanding of the data that would do the most damage if it were compromised. Without that insight, security teams have to treat all digital assets equally, essentially taking a boil-the-ocean approach to data protection.

Executive leadership members, including the CEO, CIO, Chief Risk Officer, and CISO, can take a more proactive approach to managing data risk by determining who should be responsible for managing data risk, evaluating how that responsibility should be divided, and establishing clear lines of responsibility. Such an effort requires collaboration among multiple groups to determine and agree upon the following set of questions:

1. Who owns the organization's critical data/crown jewels?
2. Who knows where that critical data resides?
3. Who manages the security of that critical data?
4. Who decides which data is considered critical versus the data that is deemed non-critical?
5. Who is accountable if the data is exposed?

Once armed with answers to these questions, participants can team critical data owners with IT security practitioners to prioritize protection. Data owners can take responsibility for creating the policies for what the data risk level should be, and to what extent data should be protected. The CISO's team can then take responsibility for the technical implementation and communication of these data security and privacy policies. Sharing that context allows the security team to understand what they are protecting and begin the process of prioritizing discovery, classification, hardening, and monitoring mission-critical data. Executive leadership should also be involved at a high level in tracking the status of data risk via analytics that will explain it in business terms in the context of the organization's business objectives.

Sharing context allows the security team to understand what they are protecting.

Typical Data Risk Management Scenarios

The effort to define roles and responsibilities for managing data risk requires an examination of existing processes. Such an inquiry can uncover several common scenarios that introduce data exposure risks.

1. New applications that handle critical data may have been quickly deployed without cross-organization or executive awareness.
2. Critical data is added to the organization through an acquisition, and the custodian of that data no longer works for the company or access becomes available to others who don't understand the value of that data.
3. One department may put a new platform online without communicating it to the entire organization.
4. Workers handling customer data or HR personnel who are working with employee information may not fully realize the value or sensitivity of that data, and they may take well-meaning but dangerous shortcuts in managing it.

These scenarios illustrate just some of the difficulties in managing data risk. As enterprises leverage new computing capabilities, such as cloud and mobile to digitally transform their businesses, the obstacles to achieving better data risk management practices grow in size. Critical data is no longer confined to well-fortified mainframes. Over time, critical data has expanded out from structured databases to unstructured user systems, and then to file shares. The continued adoption of an ever-growing array of cloud services greatly exacerbates the problem of data sprawl. The easy availability of fast and cheap data sharing services, such as DropBox, makes collaboration using such services a highly attractive idea for employees. Such practices, although intended to boost productivity, greatly increase the risk of accidental exposure, unauthorized access, and data loss as a result of employees sharing data without thinking about where it will end up once collaborative projects are complete.

At the same time, a global business economy and e-commerce encourage data sharing across both political and geographical boundaries. That creates the potential for well-meaning employees to violate the growing library of local, state, federal, and international protection regulations–especially GDPR–without data owners and custodians aware of the exposure.

Which Approach Should You Take?

As organizations go down the path to secure mission-critical data, some of the most difficult and lengthy steps in the process are identifying and classifying what's "critical." Locating and categorizing both structured and unstructured critical data requires a methodical and diligent approach–one that leverages automation in order to scale the effort.

Discovering structured and unstructured data follows the same general process, but different tools are required for each type. Locating structured data requires the ability to find all existing databases, whether in use or idle, and then scan them for relevant data types. The same is true for unstructured data. Critical data can be located on user systems, private or hosted data centers, or in private or public clouds anywhere in the world. To be effective, discovery tools should be able to consolidate their findings to provide a single view of critical data of any type, regardless of the storage repository, in an effective, programmatic, and coordinated approach.

The next step after locating all critical data is to classify it. That requires determining which data belongs to a protected category and which does not. Subsequent subdivision into the chosen taxonomy is also a best practice. Most organizations need more than basic public and private data classifications. Classifying data also requires the identification of the data stakeholder, including owners and custodians, and the data users and consumers. Stakeholders can facilitate the identification of applications and flows they use. It's also important in this step to remember that both humans and applications are data users. At the same time stakeholders are identified, users should map applications, business processes, and data flows and put them into a business context.

Data is a growing organism, so discovery must be a regularly repeated process to identify new data types and repositories. Failure to locate both structured and unstructured critical data across all existing platforms leaves the company open to greater risk and potential fines.

Data is a growing organism, so discovery must be a regularly repeated process.

Structured, Unstructured, What's the Difference?

Structured data is easy to search and analyze. It includes length-specific data like social security numbers, as well as variable-length text strings, such as customer names, and exists in relational databases used by applications like airline reservation or inventory control systems. Unstructured data has no predefined schema and uses a variety of formats, such as emails, social media, text, or video files. It also represents the lion's share of data within an organization. When trying to determine the risk levels of each data type, what's key is the value that data represents to the organization, and the implications of the loss of that data for the organization. For example, intellectual property represents great value to the enterprise, is largely unstructured, and its theft or loss to a competitor or to cyber thieves holding it for ransom could eliminate the organization's competitive advantage and threaten its survival. On the other hand, structured data, such as financial or customer data, also holds great value to the enterprise. It is a small subset of the overall data within the organization. Because the organization and regulators have long recognized its value, however, it has greater security controls in place to protect it. Once it is taken out of a well-protected database and put into a spreadsheet, cloud service, or partner system to be manipulated and shared with others, that critical structured data becomes much harder to monitor and secure. Because of its pervasiveness and diffusion across the enterprise, cyber criminals often target unstructured critical data because they know it doesn't have the same level of protection.

Data Risk Management is a Team Sport

Given the democratization of data access enabled by a range of newer technologies, it's clear that any effort to locate, classify, and protect mission-critical data wherever it lives requires collaboration across organizational boundaries within the enterprise. It also requires that members of the C-suite drive the effort if it is to be successful.

IT, security and privacy practitioners, and risk management personnel all have a critical role in creating a programmatic risk management strategy. This requires having data management, retention, containment policies, and ongoing monitoring tools in place, and employee training on the processes and procedures for data management.

Executive-level dashbaords that convey a business centric view of data risk can help executives make strategic business decisions.

Each member of the organization is responsible for understanding the value and scope of the information he or she creates and receives. It doesn't necessarily require a monolithic effort or the application of some huge formula to determine a risk probability, but it does require that employees take the time to objectively determine when and where to store it, how to protect it, and how long to keep it. Data owners and custodians must be part of the risk management process. They are responsible for protecting data from accidental destruction or modification, exposure to inappropriate internal and external parties, and intentional theft by external cybercriminals or wayward insiders.

Line of business managers and data administrators also need a means to identify structured and unstructured data repositories, both on-premises and in the cloud, and the ability to classify that data by its level of impact should it be stolen, published, or destroyed. If these data stewards are unfamiliar with the data they are monitoring, they must have the ability to separate the more business-critical information from that of lesser value. After all, a core tenet of risk management is to apply more resources to protect the assets of greater value. Data is no different. There's no point in spending $100,000 to mitigate a potential $50,000 loss.

How do You Convey a Business-Centric View of Risk?

When it comes to communicating the success or effectiveness of a data risk management program to executive leadership, the CISO is still in the hot seat. Using metrics like block rates and false positive rates is the quickest way to lose buy-in from the CEO and the board of directors. By applying the language of risk and looking at security metrics in the context of the business, CISOs can give those business leaders the insights they need to make better decisions about how to protect their organizations' most sensitive data. Data risk management tools that provide an executive-level dashboard that graphically conveys a business-centric view of risks to critical data, data ownership, and more can help the executives focus on making strategic business decisions based on their understanding of the company's handling of its most critical data. Such dashboards can also help them understand where processes and procedures need to be fortified to reduce the risk of exposure. They can better understand where to apply additional security resources to protect critical data and potentially avert a major breach. The visibility provided by the executive's data risk dashboard can help reduce the time it takes to isolate where unauthorized access occurred and communicate that location to key stakeholders. In turn, that communication can reduce the time it takes to investigate and remediate threats, and potentially avoid or minimize incident management costs and damages.

EMA Perspective

Applying risk management principles to critical data is starting to get traction in the enterprise, spurred along by the success of cyber criminals and the sensational headlines that go along with their exploits. With the GDPR regulations going into effect in late May, the adoption of better data risk management practices is likely to accelerate. Although it's likely to result in some pain before the gain, one early positive outcome is the requirement to create a new C-level position: the Chief Data Officer. The CDO can own all aspects of critical data and facilitate a much-needed conversation between the CISO using security key performance indicators and the Chief Risk Officer, who's focused on credit and market risk.

Applying risk management principles to critical data is starting to get traction in the enterprise.

In the age of data sprawl, highly effective and resourceful cyber adversaries, and the increasing cost of data breaches, it's more important than ever to apply and appropriately disseminate formal risk management processes for evaluating information assets and the vulnerabilities that threaten to compromise them. Without this amount of information being managed and presented to each level of management up to and including the board level, there is no way to determine how much money to apply to make the proper decisions to combat high risks.

Risk management is an invaluable tool for calibrating personal and organizational accountability, prioritizing actions for proactive protection and reactive response, raising and informing awareness about risks, and identifying appropriate or ineffective mitigation measures.

About IBM Security

Traditional security defenses are no match for today's well-funded attackers, while disruptive technologies like Cloud and IoT introduce new vulnerabilities to exploit. IBM Security, with 8,000 professionals in 133 countries delivers an immune system of security technology to detect and prevent threats and respond quickly and completely to breaches. During the past decade, IBM has invested more than $2 billion on security research and development, resulting in 3,700+ security-related patents, and it acquired 20 security companies to build out its portfolio. Today, IBM Security addresses the evolving security landscape and 17,000 clients' most critical needs with AI innovation in the cloud and intelligent orchestration. For more information, visit https://www.ibm.com/security

IBM Data Risk Manager is an integration platform that provides executives and their teams a business-consumable data risk control center, helping to uncover, analyze, and visualize data-related business risks so they can take action to protect their business.

For more information, go to https://www.ibm.com/us-en/marketplace/data-risk-manager

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3716.050818