The exposure of data for up to 14 million of Verizon’s customers in July 2017 was an enormous embarrassment, particularly for an organization that presents itself as a premium cybersecurity consultancy. After all, Verizon produces its Data Breach Investigations Report (DBIR) annually, which documents the largest cyberthreats its customers could face in the upcoming year and how to avoid them. The irony is that Verizon itself has now become a data point for its future reports.

As has happened in other breaches, an external vendor was responsible for the incorrect settings that allowed open access to Verizon user information. This incident reinforces the concern regarding how security professionals can stay on top of all the data and all the different configurations extant in departments across the enterprise. The good news is that, in recent years, many IT organizations have initiated master data management (MDM) projects to help rectify this situation.

Having standard configurations that are documented and staff that is trained to follow these standards helps. But it is well known that one of the biggest risk factors is people—and people make mistakes. Whether intentional or not, mistakes introduce the opportunity for breaches. One of those mistakes can occur when an organization’s cybersecurity team is not involved as a stakeholder in IT projects such as MDM.

**What Is MDM?**

MDM is an effort to rationalize disparate and overlapping databases to ensure the accuracy, integrity and consistency of corporate data. Multiple databases with multiple versions of data that might not be consistent across an organization’s database landscape can be caused by silos within the organization, mergers and acquisitions, and other issues.

The most common example of why this is a problem is when a customer’s information is not accurate across all databases. This can cause damaging miscommunications with customers that can, ultimately, harm the organization’s reputation.

There are two methods for collating data in an MDM environment: consolidated and federated. In a consolidated system, the data are collated and distributed from a centralized source. In a federated system, there is a virtual view of the data, which are collated and distributed from multiple sources.

**Why MDM Is a Cybersecurity Concern**

In a time when MDM and business intelligence (BI) are common terms in the business world, organizations are still trying to figure out how to keep data fresh across multiple systems and, of greater challenge, how to report on the data. The larger concern for any security professional is the fact that data hold significant corporate risk.

With personally identifiable information (PII), the US Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), the US Sarbanes-Oxley Act (SOX), and the EU General Data Protection Regulation (GDPR), to mention just a few overarching laws and regulations that govern how to protect data, the difficulty comes with knowing where all the data are...
The Initial MDM Project
The cybersecurity team clearly should be involved as a stakeholder at the beginning of any MDM initiative to help define and apply the relevant cybersecurity standards and policies.

The cybersecurity team’s relationship with the enterprise’s IT organization and users should be good enough that the team is informed of data-involved projects during the planning/initial stages. That being stated, the team must be constantly watchful for MDM projects (or any data-involving projects, for that matter) as the business and IT organizations may not always understand the need for the team’s requisite involvement.

At a minimum, cybersecurity should be a participant in the architectural committee that reviews every project during the planning and kickoff phases.
Securing MDM Tools
Securing the firm’s MDM tools is no different from applying cybersecurity standards and processes to other IT applications. It is important to be absolutely certain that the tools’ security settings are optioned correctly and the organization’s identity and access management (IAM) policies and procedures for accessing the tools are firmly in place and regularly reviewed for compliance. In addition, care should be taken to ensure that the cybersecurity standards for security patching are followed.

Securing MDM Processes
Depending on the organization and how the cybersecurity team is involved in IT projects and implementations, MDM can be reviewed as a part of the software development life cycle (SDLC) process, another consideration for the architectural review board or an item for the change control process. The key is to have the requisite opportunities to assess the data, their sensitivity and how they are being protected. One review is not sufficient, as many times over the life of an application the data will be manipulated, which can change the data’s security requirements.

Recent data breaches and data exposure incidents indicate that third parties represent one of the greatest vulnerabilities today. With this in mind, it is important that the cybersecurity team tackles

Standards and Policies Regarding MDM
Basic processes need to include good data access control designed around job roles and a need-to-know basis. Also, the data should be protected during both storage and transmission. Thus, encryption should be a standard requirement for anything sensitive or proprietary.

Data retention needs to be defined with highly detailed backup schedules, expiration dates and destruction methods. Special attention needs to be paid when data and reports are downloaded to desktops/laptops for manipulation by business analysts.

With the basics in place, the MDM team should be required to maintain a current data map (tutorials on creating data maps can be found on the Internet), which should be updated as part of every MDM project and/or data change. At a minimum, the data map should be reviewed quarterly to ensure that it reflects the true data landscape.

As part of managing the data map, the cybersecurity team needs to ensure there is a clear vision of when and for what reason data leave the organization’s network. It is extremely important, no matter the type, that the data be identified, documented, classified and tracked, along with the identity of the recipient. Classification includes the type of data and the data’s sensitivity level. Tracking is important to ensure the firm knows what information is sent where. All this information becomes part of the data map and needs to be updated as part of any associated change control event.
the role of reviewing contracts with third parties and ensuring ongoing compliance with them. This is necessary to assure strong data protection requirements, define acceptable protection methodologies, define responsibility in the event of a data breach, mandate cyberinsurance levels and outline the appropriate media response if there is a breach.

Getting Started

If the organization's cybersecurity team is not already involved with the MDM efforts, it either should be or soon will be, as the enterprise and IT organizations take advantage of MDM's benefits. Hopefully, the roles and responsibilities for each team are well defined, which will make the cybersecurity team's involvement in these new efforts more productive.

The conversation with the MDM team can begin with the fact that data are powerful assets that warrant five-star security and the cybersecurity team wants to help the MDM team protect its data. Demonstrating respect for the value of both the data and the MDM team will help build a relationship based on common interests. It is critical to avoid being heavy-handed, as this will quickly sour the relationship between the teams.

As rapport is established, the project's documentation can be requested. After in-depth study, it is advisable to start with the basics of encrypting the MDM data both while at rest and during transit, with a focus on sensitive, valuable information. After encryption is addressed, it is possible to begin applying the rest of the cybersecurity organization's standards and policies to the new project, including IAM, patch management and data retention. This will allow the MDM team to continue to own data responsibility while incorporating a cybersecurity view.

Any new technologies or processes that will be required by the project must be analyzed and, if required, new cybersecurity standards and/or policies developed to cover them. Also, it is important to identify any tools that will be used so the cybersecurity team can ensure they are secured. On an ongoing basis, the strength of the security of any access tools that may be used by the firm's data analysts should be evaluated.

To properly secure the MDM data in the future, detailed data maps must be developed and maintained over the life cycle of the data. After the initial MDM implementation, the security of its data and procedures must be included in the organization's standard review processes.

Ultimately, the most important thing is that there should be trust, mutual respect and strong working relationships among IT, the business organization and the cybersecurity team. Not having those relationships in place can expose the organization to cyberrisk.

Endnotes