TechVision Research Crosstalk Report: Getting Your Identity Data Right

The greatest risk facing most organizations

Abstract

The most complicated challenges facing IT tend to cross traditional IT research and consulting coverage areas. TechVision Research recognizes this challenge and our team is committed to addressing these great challenges with a service offering (enterprise-wide access) that is uniquely structured to address cross-coverage issues. The TechVision Research Crosstalk reports provide a bridge between different overlapping technology areas. This first report captures a discussion between Noreen Kendle, author of Data – The Fundamentals Are Broken and Fixing the Fundamentals – The Business Blueprint and Gary Rowe and Bill Bonney authors of the Future of Identity Management report. In this report we examine the synergy and challenges relating to the architecture and management of enterprise data and enterprise identity management.

Authors:

By Bill Bonney, Principal Consulting Analyst
bill@techvisionresearch.com

Noreen Kendle, Principal Consulting Analyst
noreen@techvisionresearch.com

Gary Rowe, CEO and Principal Consulting Analyst
gary@techvisionresearch.com

Moderated by Ted Ritter, VP Product and Market Development
ted@techvisionreseaerch.com

Table of Contents

Executive Summary & Key Advice

Most organizations have a major challenge getting their identity management correct and in most organizations a big part of this problem is a data problem: *garbage in = garbage out* forms the basis for most enterprise identity mismanagement. As discussed in this report, when we look a bit deeper, we find a plethora of identity data challenges, including multiple authoritative sources of data, inconsistent data, redundant data, old data and misclassification of data.

A key issue is there is a false assumption among IT and business professionals that their data is being managed. It is not being managed. People do not spend the necessary resources in data management and this lack of data management discipline flows through to identity data management.

This report is a synopsis of a discussion between three TechVision Research principal consulting analysts: Bill Bonney, Noreen Kendle and Gary Rowe. In this report, we cover a range of IAM data challenges from the obvious (overloading a field — making assumptions about what is in a field and assumptions about how the field is evaluated) to the less obvious (the lack of usable connectors from the IAM system to the target workforce applications).

The fundamental challenge facing IAM and data is a lack of identity data governance. Based on our experience, most identity teams have little understanding of data architecture, data management and data governance and it's time is that identity management embraces these disciplines. This isn't JUST a data problem, it's a privacy and security problem. As Bill Bonney points out, "the less governance one places on the data, the greater the risk of a compliance and privacy issues arising."

This report covers a lot of ground and raises the need for investing in identity data governance and in addition to this we outline four further steps all organizations must take to begin getting their IAM data under control:

1. All organizations should immediately create / empower the Chief Data Officer (CDO) role.
2. We must consider Virtual Directory Services (VDS)
3. Organizations should develop the construct of an Identity Data Service (IDS)
4. Do not attempt replacing existing IAM before performing a complete data store analysis and normalization

Introduction

Most organizations have a major challenge getting their identity data correct. As Gary Rowe states, "in most organizations a big part of the identity problem is a data problem." The problem often revolves around the source of the data. There is an old IT adage, "garbage in, garbage out" which appropriately applies to the data forms the basis for enterprise identity management.

"The real world data challenges from the identity management perspective include multiple authoritative sources of data, inconsistent data, redundant data, old data and misclassification of data."

-Gary Rowe

As a starting point for the discussion, Gary Rowe describes the lay of the land in enterprise IT: "The real world data challenges from the identity management perspective include multiple authoritative sources of data, inconsistent data, redundant data, old data and misclassification of data."

But are these just identity management issues? We often think of these issues as identity management issues, but they are also issues with the underlying data. As Noreen Kendle states, "when you are protecting identity, you are protecting data." We know that companies have security guards to protect the things that the data represents – the people, buildings, etc. Similarly, In IT we protect the representation of a person's identity — the data. Unfortunately, most companies have at least some level of identity management and very little, if any, data management: typically, data gets addressed reactively when there is an emergency.

Noreen goes on to say "there is a false assumption that data is being managed [in today's enterprise]. People do not spend the necessary resources in data management and they barely spend much in data architecture." In more recent times this has become a symptom of the current AppDev mindset: everything is agile and therefore we don't need design." This lack of data management discipline flows through to identity data management discipline. The bottom-line is that identity data is such an important asset and to manage it you first must identity and inventory it. Gary Rowe goes on to state "I agree with Noreen that with a lack of data management, data gets "managed" reactively. We then try to assemble that non-managed data into an identity management system and we wonder why it is such a nightmare?"

What's in that Field?

Though this report focuses on the intersection of data management and identity management, at TechVision Research we continually see a lack of data management undermining all aspects of business functions. As Noreen Kendle has experienced "the data mess is equal opportunity across all types of data, including identity data." Noreen goes on to say, "I've seen companies overload their data and use miscellaneous text fields for identity-related information primarily because they don't want to stop and enhance the database schema and structures: this includes credit card numbers, social security numbers, etc." Obviously, this is a huge privacy issue because the fields are not identified as identity fields and the IT staff is unaware of the need to protect the data.

> "The data mess is equal opportunity across all types of data, including identity data."
>
> -Noreen Kendle

Relating to this point, Bill Bonney speaks from experience building an IAM practice at a large online financial services firm. Bill agrees that overloading is an issue but, "It's not just overloading, it's making assumptions about what is in a field and assumptions about how the field is evaluated. Before you know it you have sub-processes built up around a falsely validated field." As discussed below, this establishes a false foundation that eventually causes the entire trust chain to break. As Bill states, "inevitably, someone will also use the data based on how it was first created (the field label of record) and then all hell breaks loose."

In reality, this is a symptom of a far greater problem. There is a huge assumption made by IT staff and the developers of the identity management tools they use that the data fields accurately represent the data stored in those fields. Without real data management, no one should ever assume anything about a data field.

But Identity Data is Special

Typically, when enterprise IT and business teams engage in data discussions, the identity data is off limits. This goes back about 20 years to when organizations first started looking at identity data as special. It was around the same time that meta directories started taking off and the concept of an identity management discipline – separate from the rest of IT – was born. At a conceptual level this distinction makes great sense, but at a practical level we find that identity teams have little understanding of data architecture, data management and data governance. This is a huge problem and a clear outcome of this discussion is it is time that identity management embraces data management and governance.

Building Silos

Identity management is clearly its own discipline and like most IT disciplines it is co-arising with the identity management silo. As Bill Bonney discusses from his experience leading an identity management team, "Identity management (like other areas) becomes a silo in the organization. The IAM team can't expect the central IT team to keep up with IAM project timelines and start creating their own data stores. As the IAM team experiences increasing pressure to keep the IAM project on schedule, they de-emphasize tasks that correct data at the source. Unfortunately, the new data store silo then becomes the defacto "source of truth" for identities. In reality it isn't – and never was - a source of truth, the real source of truth was always in Human Resources." This establishes the entire IAM process on a weak foundation, "using the 'false god' to make subsequent choices" leading to downstream sources quickly diverging from the original source. A related issue is data disparity where each source can change independent of the other, adding to the overall data chaos.

"Identity management (like other areas) becomes a silo in the organization. The IAM team can't expect the central IT team to keep up with IAM project timelines and start creating their own data stores."

-Bill Bonney

The siloization of data and the need to synchronize across silos has become a major focus of IAM. As discussed in the TechVision Research Future of Identity Management report, because enterprise data generally lives in a multitude of disparate silos, data synchronization has been the traditional cornerstone of many solutions. The challenges associated with data synchronization are evident in a multitude of areas, including user account provisioning. We find event triggers, such as changes to authoritative source systems like Human Resource Management Systems (HRMS), result in the automatic creation of user accounts and access privileges on as many downstream target applications and systems as can exist in an organization. While this seems pretty simple, most CISOs and CTOs know how hard (read impossible) the process really is for an organization with hundreds, if not thousands of such workforce applications and services.

This problem typically stems from the lack of usable connectors from the IAM system (normally the provisioning platform) to the target workforce applications. Though IAM vendors have for years touted their dozens if not hundreds of connectors, in actuality we find that they have only a few deployed in any large number, and the rest are derivatives of toolkits for creating connectors that haven't seen the light of day, much less actually worked according to plan.

The reality is that most organizations end up with maybe two or three connected systems typically including Active Directory, and complex enterprise applications from Oracle, SAP and others. This situation often leaves hundreds of applications beyond the realm of provisioning/de-provisioning and outside of the enterprise IAM system. And, it leaves senior management very dissatisfied at having invested millions of dollars on promises made in IAM projects that do not address enough systems to reduce risk or satisfactorily automate administration.

Virtual Directories to the Rescue?

Recently, TechVision Research published The Future of Identity Management report and one of the topics with the greatest interest is the potential value of virtual directories. What is the role of virtual directories as an identity data store and as a potential means to address some of these fundamental data issues with identity data? As discussed in the report, Virtual Directory Services (VDS) are a primary means of implementing a consistent view of a multitude of underlying data stores and using that information to make meaningful decisions.

A virtual directory is a service that consolidates data from multiple directories, databases and other sources into a single logical view. When an attribute represented in multiple data sources creates a conflict, a virtual directory can choose the proper attribute value from a particular source based on a resolution policy. Virtual directories can perform data and structural transformations and may enable authentication and federation capabilities. While a virtual directory is not a persistent data store, it may maintain a cache, or working storage, of consolidated information to enhance performance. Virtual directories create a consolidated directory view by tying together several information sources and creating a new directory perspective.

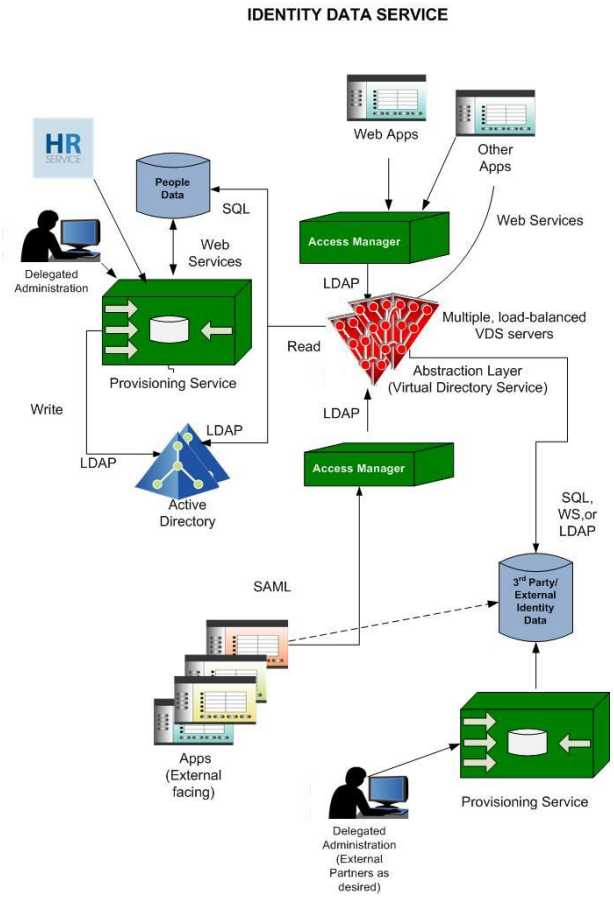

Figure 1 - Identity Data Service (IDS) Architecture

The strength of virtual directories is their ability to retrieve data dynamically in response to an authorization query. In response to authorization requests, a virtual directory attaches to source repositories (which can include other directories, databases, flat files, XML feeds and proprietary data stores) and generates a response by combining information from these sources. Some virtual directory vendors provide synchronization capabilities within their products and we believe this provides substantial potential value for enterprise clients.

Virtual directory products can satisfy many application requirements - both internal and external to the organization. For example, a virtual directory can assemble attributes from multiple disparate sources into a single logical LDAP schema used for security policy enforcement by the company's access management solution. Additionally, a virtual directory administration client can assemble common names, user IDs, phone numbers, email addresses and postal addresses from multiple repositories for delegated administration. Lastly, unlike generic LDAP directories or Active Directory (AD), a virtual directory can have multiple schema definitions, meaning any given set of enterprise applications do not have to conform to a single, monolithic LDAP schema. This greatly enhances the ability to provide finer-grained access control to many disparate applications

- a major step toward adoption of identity data services versus the stovepipe fine grained access control that is currently performed by each application.

Diving further into the discussion of VDS, Bill Bonney raises the point that one of the values of a virtual directory may be the fact that it doesn't substantiate itself outside of the realm in which it is being used. As Bill notes, "it [virtual directory] never actually gets written back." Because of this, a virtual directory does not violate the "sacredness" on which it was built. If the data within the virtual directory doesn't change then sources of truth can be maintained.

> "A virtual directory does not violate the *sacredness* on which it was built. If the data within the virtual directory doesn't change then sources of truth can be maintained."
>
> -Bill Bonney

As discussed in The Future of Identity Management report, an Identity Data Service (IDS) can address these issues by providing people, applications and services sufficient access to identity data to meet operational needs while protecting sensitive identity information. As a result, organizations taking this approach see a reduction in outdated, incomplete or inaccurate data; data that leads to erroneous access privileges. The IDS also provides a better platform to deliver policy-based management and execute a consistent, auditable governance model.

An IDS focuses on the systemization and consistency of delivering identity information to business applications. It starts with a consistent methodology for ensuring the accuracy and maintenance of the data contained in the identity stores.

While many of the core concepts of the IDS (virtual directories, federation, provisioning, etc.) have been in place for many years, IDS's Service Oriented Architecture (SOA) and identity abstraction are core concepts that are critical to enabling IAM that supports the next generation of identity consumers.

Decreasing Resolution over Time

Related to the issue of maintaining "sacredness" of identity data, we find there are significant resolution challenges as data is used and reused throughout the organization. As discussed in Noreen Kendle's Data – The Fundamentals Are Broken report, with technology rapidly advancing, organizations continually upgrade their systems. Noreen finds IT departments strapped with tight budgets and timelines tend to simply *lift and move* the data from the older to the newer technology. This *lift and move* strategy is especially

popular for IAM as we find many organizations are currently embarking on forklift upgrades of their 10+ year-old IAM systems. Even without the forklift upgrade, IAM systems are continually upgraded and tweaked over time, and often this is an *emergency* situation with little or no documentation recording what was actually done to the directory stores.

This is a big challenge for IAM and its data. Time – or the perceived lack of time – is a critical issue here. Staff often shorten or skip documenting business requirements because they believe it will unnecessarily add to system replacement timelines, especially with the conversion processing from the old system to the new system. Any business requirements that are developed are generally used for documentation rather than the design of new data structures. Using the data structures from an existing identity data source appears to be a much quicker method for most organizations. Inherent in this process is the erroneous assumption that the newer IAM technology will fix many of the data issues and limitations of the old system. In reality this method only moves the data disparities—known or unknown—forward.

Without doing a thoughtful analysis of the existing data store against the data requirements of the replacement system — rather than fix previous data issues — the problems may actually become worse as new deficiencies are introduced on top of the previous issues.

Decreasing Data Fidelity over Time

Many organizations are now using packaged IAM solutions to automate common business functions. Each of the packaged software solutions has its own proprietary generic view of data. The organization is forced to distort its business functions to fit into the package's generic view, without adequate business process re-engineering or requisite change management. This results in yet another *version of the truth*. These packaged solutions typically use the data from the replaced systems in a *lift and move* fashion. Despite efforts to clean data during conversion, many of the old systems' data issues are moved forward because most of these issues are unknown or more likely known but undocumented. Each time a new system is implemented (or an existing system is tweaked) using the previous system's data distortions grow exponentially. It's similar to taking a photo of a photo of a photo and on and on until everything becomes gray. Each time the photo is copied we lose resolution and fidelity.

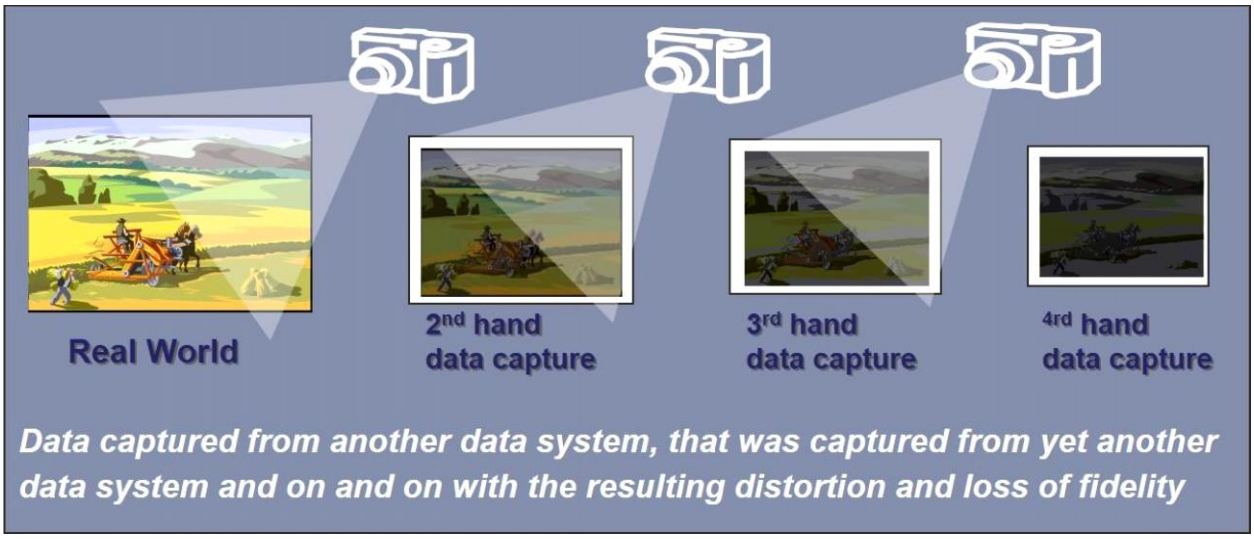

Figure 2 - Example of Loss of Data Fidelity

In terms of data, the "resolution" is the connection between the business and the data. The result is a growing disconnect between the data and the business reality it represents. As data moves further away from the business reality, the organization suffers from a growing number of data problems.

Discussion

Is This a Governance Problem?

So, what is the fundamental problem we're discussing? Is it a lack of discipline? Is it a lack of knowledge? Is it a lack of technology? The TechVision Research team believes the fundamental challenge is a lack of governance for identity — and all enterprise — data. As Bill Bonney states, "Absolutely. A key value of data governance is creating rules around the use of data (what people think). But a key value, often missed, is defining the lifecycle aspect of the data – when it should be deleted/destroyed." This is a critical issue and it has far reaching consequence in privacy, risk and compliance.

We must look at identity data as a multidimensional lifecycle issue. Identity data is created, managed and rarely is it destroyed: most organizations only focus on the creation of identity data, some focus on its management and few focus on its deletion. And, even for those organizations addressing data deletion, it is very difficult to find and eliminate every copy. This is because some stores were replicated for safekeeping and then forgotten and others serve as a formal or informal source of truth for a tangentially related downstream process. As Gary Rowe states, "de-provisioning is often overlooked or not timely and it creates pervasive data, identity management and security problems." Gary has worked with scores of companies that are left with the ghost legacy of former employees that still have access rights – even people they fired for cause! Both Gary and Noreen emphasize the

distinct lack of logic behind this practice: "let's piss off the employee by firing them, kick them to the street and maintain their access to company sensitive resources and then wonder why the security breech occurred."

This takes us back to the importance of the authoritative source of the data. According to Noreen, "no one in the organization manages this." Data governance was a big hot topic a few years back and the groups created at that time still exist. Noreen highlights the logical flow of governance that is missing in most of these organizations: "rules are needed in order to govern anything and we cannot govern anything unless it is managed. And, we can't manage anything unless we identify, define, and inventory it first." In other words, even though organizations may have governance bodies, these bodies are largely ineffective because they cannot develop effective rules when the data is not identified, defined, inventoried, and managed. In reality, our experience working with large organizations is very few data fields are defined and even fewer are what one assumes they are from the field name. For governance to work, we need these building blocks in place. We can't manage data until we define things and we can't define things until we establish the authoritative source. Data (identity or non-identity) governance cannot be effective until the data is managed.

> "Rules are needed in order to govern anything and we cannot govern anything unless it is managed. And, we can't manage anything unless we identify, define, and inventory it first."
>
> -Noreen Kendle

Built on A Foundation of Quicksand

Another axis for the identity lifecycle is one of authenticity decay. Identity data's authenticity decays over time. For example, when created the data is 100% authentic. The first time the data is duplicated, its data authenticity drops to 50%; one more duplication and the authenticity drops to 25%. And, so on. What's quite troubling is there is an inverse relationship between authenticity and risk: the lower the authenticity, the greater the risk. This is most evident when someone thinks that they have "deleted" the data when in fact many copies still remain. Even just one remaining instance of an identity data set that was "supposed to be" deleted significantly increases enterprise risk. Noreen adds that "we're not even considering the countless times employees download identity-laden spreadsheets to their laptops for offline processing."

This decay function completely undermines the IAM structure. This is similar to building on a foundation of quicksand. This has far-reaching implications throughout the enterprise. As Gary Rowe adds, "in most organizations a big part of the identity problem is a data

problem. If there are 30 systems that have different versions of 'Gary Rowe' (name spelled differently, different titles, different address, etc.) it becomes impossible to identify the authoritative source." Things can even get worse if one's attributes change (e.g. move from employee to contractor).

To emphasize the need to build a strong foundation, Gary points out "we can pull it together physically through federation, consolidation, and synchronization. These are table stakes capabilities of IAM programs." Unfortunately, we do find that many organizations are skipping the foundation and are attempting to use VDS to solve the problem of multiple authoritative sources and data silos dispersed across the organization.
Noreen sums this up by saying "addressing the fundamentals of data is most critical for identity management and information protection. We know organizations have great staff, great processes, and really cool tools, but they are building on quicksand because they assume there are magic fairies keeping the data right."

"We can pull it together physically through federation, consolidation, and synchronization. These are table stakes capabilities of IAM programs."

-Gary Rowe

Identity Data Context and Granularity

All data comes with specific attributes with regard to security and privacy. Security and risk revolves around the data classification of these attributes. We've seen a real evolution of data classification over the years. We see organizations go through cycles and pendulum swings from all data considered sensitive to very little data being classified as sensitive. We've seen similar patterns with data retention. Many organizations have evolved from only keeping "necessary" data to keeping everything. As discussed below, this is a major challenge of all IAM operations.

Who You Gonna Call?

So far we've been focusing on the challenges of identity data, its governance, and its authenticity. Though many people in the organization recognize there are problems, it is difficult to determine who actually owns the problem, who cares about these problems and who will want to do something about these problems?

As Noreen points out, "data governance is rarely in anyone's job description and it's never in a job description related to identity management." Noreen has great empathy for the IAM folks since they know they have big problems but they have to work with what they've got. They are the biggest victims in all of this! The IAM guys shouldn't have to be cleaning

up the data.

Bill chimes in "the ultimate owners of the data source create these problems. If we think of the average accounting department with their Oracle/SAP system. They usually can't represent the *entire* world in the reports they have available, so they do massaging of data and then keep track of what they do on a regular basis. They store the rules for massaging the data on spreadsheets on their computers." Once they do this, there is no real ability for these departments to send this info upstream to recombine with the authoritative source. This is a major flaw in data management and If the reintegration of locally produced data with its authoritative source was better supported, there would be fewer silos of data.

To add to what Bill is saying, there are structural road blocks to data ownership and management. From Noreen's perspective, the data was created for one function in one department and that department is judged by how well it does that one function. There is almost never a concept of someone owning the data. No one is incentivized to care about the entire lifecycle of the data, especially once the data leaves the department's purview.

The good news is organizations are finally starting to address this problem. A trend that Noreen Kendle is seeing is the rise of the Chief Data Officer (CDO). According to Noreen, data has never had a seat of authority at the table with the IT and senior business management. Even when the organization is enlightened enough to establish a CDO, they still rarely have much authority. Gary Rowe adds "The CDO role needs to be a priority for every global 5000 organization—data is the most important asset most organizations have and the lack of an empowered data leader in most organizations is a mistake."

"The CDO role needs to be a priority for every global 5000 organization—data is the most important asset most organizations have and the lack of an empowered data leader in most organizations is a mistake."

-Gary Rowe

So, we're back to *who are you gonna call?* If even CDOs do not have any authority how can we address these issues? All three principal consulting analysts agree that it's time we turn things on their head and look to people in security and privacy to drive governance of corporate data. As Bill Bonney points out, "the less governance one places on the data, the greater the risk of a compliance and privacy issues arising. In IT, we don't have data officers, but we do have enterprise architects and CIOs."

Bill is definitely seeing data governance becoming a discipline as part of privacy and compliance, particularly in financial services organization. Of course, the challenge we see

for all organizations is how one builds a business case for this data governance? Certainly, Home Depot recently paying out $19.5M to US Consumers harmed by its 2014 breach is a data point for any business case.

Thinking Global While Acting Local

There is another axis on our identity lifecycle representing the progressive atomization of enterprise IT. We see increasing interest in micro services and containerization — particularly when moving to the cloud — breaking down enterprise applications into molecular components. In the case of identity, these movements can heavily leverage what is happening on the data side. The disambiguation of applications and breaking down of application silos puts great pressure on the identity data and in particular, tracking the authoritative source. Applications, as we knew them with a capital "A", are morphing into apps with their scope crumbling as they become localized. As apps become more local, identity must become more global: a massive enterprise-wide concept. Identity must become all-encompassing, touching everything. And, "everything" is continually growing as the quantizing of applications results in significantly increased surface area. As Gary states, "we need to reinforce the correlation – good data with authoritative sources supports an identity program and it mitigates the opportunities for breach."

Putting This in Context

> "Identity context is critical."
>
> -Bill Bonney

We can't discuss identity and data without discussing context. As Bill notes, "identity context is critical." In fact, we might be able to stop developing an identity silo to begin with. If we switch to context-based identity, we open the door to never having to alter the authoritative source or even create a virtual directory. Context-based identity correlates relevant data, such as attributes about a person or device, to understand relationships, environmental factors, temporal state, and roles and can also be used to assess anomalies and support security programs. The more data points an organization has to work with, the stronger the intelligence and the resulting ability to discern between normal and anomalous behaviors.

How much context-based identity information is enough? Where do we reach the point of diminishing returns and what line should be drawn in terms of collecting external personal data? By successfully answering these questions and externalizing the context data to the greatest extent possible, we can make rich authentication decisions while decreasing the creation and maintenance of internal identity data silos.

We also need to address departmental ownership around data and context. For IDM to work, HR must be involved to create the authoritative source. HR often declines to do this

or places restrictions around the use of HR systems when non-employee worker data is concerned, and that creates the first silo.

Recommendations and Conclusion

Five Step Program

If we shift the focus on data governance to the privacy/compliance side of the house, we need to develop a clear roadmap for these people to take this on. After all, data governance is not a standard part of the training, or even the job description for privacy, security or compliance people. In Data – The Fundamentals Are Broken, Noreen Kendle defines five steps organizations must take for effective data governance. These steps have direct analogues on the identity side of the house.

Data is an important business asset and technology is its enabler. We need to spend as much or even more time, effort, and resources on our data as we do on our technology or we will never gain the benefits promised by the technology. We must start by fixing the fundamentals of data.

There are five basic steps an organization can take to address the broken data fundamentals:

1. Establish the Business to Data Connection using a Business Blueprint - The Business Blueprint is a proven method to understanding and documenting a Business-to-Data connection that serves as a foundation for connecting the data to the real world business organization: the organization the data is intended to represent. The Blueprint is a holistic informational diagram of the real world business organization defining the important things and events that the data must represent. To understand and plan what data is needed to optimally and effectively represent the business, the holistic blueprint of the business must be created independent of any data models or designs. The blueprint is not a model of the data, rather it is a model of the business the data will represent.
2. Create a Data Oversight Framework - The second step to fixing the fundamentals is building a Data Oversight Framework (DOF) to establish a "playbook" (the strategy, principles, policies, and rules for the information-data assets) along with the functions to implement and support it. The framework covers all of the data strategy components necessary to establish and orchestrate the data assets' well-being. The DOF is foundational for all other data strategy components (e.g. data governance and ownership, data security, data asset management, etc.). Developing the framework gets everyone on the same page and in agreement as to the direction, value, importance, and priority of the information-data assets.
3. Establish an Enterprise Data Construction Practice - The third step to fixing the fundamentals is establishing an Enterprise Data Construction (EDC) Practice for the development of data systems and structures to house the data. A holistic (i.e. city

plan) approach is used to properly support data as a representation of the real-world business organization. The EDC Practice covers the identification, architecture, design, and deployment of data structures and systems across the organization including the organizations meta-information. The practice uses the Business Blueprint as the foundation for all of the organization's data and data structures. This forms a holistic data infrastructure that ties all of the organization's data systems together.

4. Build the Data Asset Management Infrastructure - The forth step to fixing the fundamentals is creating a Data Asset Management (DAM) Framework by building the infrastructure necessary to manage the data as an asset. The Framework includes the methods, processes, procedures, and tools required to manage data as an asset and it utilizes the data infrastructure developed through the Business Blueprint and EDC Practice.
5. Establish a Data Asset Management Practice focused on Enterprise Foundational Data - The fifth step to fixing the fundamentals is establishing a Data Asset Management (DAM) practice with an initial focus on Enterprise Foundational data. This practice applies proper asset management principles and methods to the business organization's most critical type of data assets: the enterprise foundational data asset.

The big concern with this is as Noreen points out, "they really need to incorporate the data skills. Doing this without data fundamentals skills will be a nonstarter." Gary Rowe adds, "If the above steps are consistently followed, the identity management program will be a huge beneficiary".

This engaging and interactive discussion covered much ground and the following are key take-away points to consider in conjunction with the above five step program:

1. All organizations should immediately create / empower the Chief Data Officer (CDO) role. Addressing the fundamentals of data is most critical for identity management and information protection. We know organizations have great staff, great processes, and really cool tools, but they are building on quicksand because they assume there are magic fairies keeping the data right. Good data with authoritative sources supports an identity program and it mitigates the opportunities for breach.
2. We need to turn things on their head and look to people in security and privacy to drive governance of corporate data because the fundamental challenge we're facing is a lack of governance for identity — and all enterprise — data. Data (identity or non-identity) governance cannot be effective until the data is managed.
3. It's time that identity management embraces data management and governance.
4. We must consider virtual directory services (VDS) since one of the values of VDS may be the fact that it doesn't substantiate itself outside of the realm in which it is being used. Because of this, a virtual directory does not violate the "sacredness" on which it was built. If the data within the virtual directory doesn't change then

sources of truth can be maintained.

5. Organizations should develop the construct of an Identity Data Service (IDS) focusing on the systemization and consistency of delivering identity information to business applications. IDS development starts with a consistent methodology for ensuring the accuracy and maintenance of the data contained in the identity stores.
6. For organizations considering replacing their IAM system, without doing a thoughtful analysis of the existing data stores against the data requirements of the replacement system — rather than fix previous data issues — the problems may actually become worse as new deficiencies are introduced on top of the previous issues. This is because each time a new system is implemented (or an existing system is tweaked) using the previous system's data distortions grow exponentially.
7. Ensure the data governance team has the proper data skills and get the team moving on our five step program to address the broken data fundamentals.

For Additional Information

For additional reading on these topics, please see the following TechVision Research reports:

Data: The Fundamentals Are Broken by Noreen Kendle
https://techvisionresearch.com/project/data-fundamentals-broken/

The Future of Identity Management by Bill Bonney, David Goodman, Gary Rowe and Doug Simmons
https://techvisionresearch.com/project/the-future-of-identity-management/

Fixing the Fundamentals: The Business Blueprint by Noreen Kendle
https://techvisionresearch.com/project/fixing-the-fundamentals-the-business-blueprint/

About TechVision

World-class research requires world-class consulting analysts and our team is just that. Gaining value from research also means having access to research. All **TechVision Research** licenses are "enterprise licenses"; this means everyone that needs access to content can have access to content. We know major technology initiatives involve many different skill sets across an organization and limiting content to a few can compromise the effectiveness of the team and the success of the initiative. Our research leverages our team's in-depth knowledge, as well as their real world consulting experience. We combine great analyst skills with real world client experiences to provide a deep and balanced perspective.

TechVision Consulting builds off our research with specific projects to help organizations better understand, architect, select, build, and deploy infrastructure technologies. Our well-rounded experience and strong analytical skills help us separate the "hype" from the reality. This expertise provides organizations with a deeper understanding of the full scope of vendor capabilities, product life cycles, and provides a basis for more informed decisions. We also support vendors in areas such as product or strategy reviews and assessments, requirement analysis, target market assessment, technology trend analysis, go-to-market plan assessment, and gap analysis.

TechVision Updates will provide regular updates on the latest developments with respect to the issues addressed in this report.

