Integrating Third-Party Risk Management and Identity and Access Management to Safeguard Your Organization from a Third-Party Breach

Introduction

Driven by competition, cost savings, and business efficiency needs, organizations are increasingly relying on third parties – contractors, vendors, suppliers, partners, volunteers, and non-humans (like bots and IoT devices) – to deliver critical labor, service support, products, expertise, and more to meet their business needs.

Third parties have become a workplace norm. According to a recent report by Prevalent, the average organization utilizes nearly 2,400 third parties in various business functions. And although this increased volume and reliance on outside resources has afforded organizations greater diversity, expertise, speed of innovation, and financial success, it has also led to disaster in the form of third-party data breaches.

In fact, according to an Opus and Ponemon study, 59 percent of companies said they have experienced a data breach caused by one of their vendors or third parties. These breaches could happen due to poor security practices of the third-party organization or through any non-employee that was granted access (knowingly or unknowingly) by the organization to their data and systems. Even more alarming, in many cases, these identities have been granted privileged access to sensitive information. The results can be devastating – business downtime, loss of customers' trust, hefty regulatory fines, and lawsuits.

It's obvious that third parties bring with them an inherent level of risk, and much is easily recognized. Yet organizations continue to overlook the dangers third parties pose to their organizations and remain ill equipped to adequately protect themselves.

This white paper examines where most third-party identity risk management approaches struggle; defines a more complete approach; and identifies three use cases where the integration of third-party risk management and IAM can reduce risk and improve operational agility.

Considering the Risks of Third Parties and Non-Employees

Organizations work hard – and spend a large portion of their IT budgets – to secure their networks and data. Gartner reports worldwide spending on information security products and services exceeds $150 billion. Yet Deloitte's 2020 Global Survey on Third Party Governance and Risk Management reports that 85% of organizations do not have processes to effectively manage the risks associated with third parties. Why is this? It's well known that it's less expensive to prevent cyber-attacks than it is to repair the damages resulting from successful breaches.

The answer is not simple. Many organizations have put in place processes and solutions to address third-party risk. Unfortunately, these programs are insufficient for contemporary third-party risk challenges and were typically designed with compliance-driven mindsets. They persist in some organizations solely as spreadsheet questionnaires and in others as monolithic software solutions not designed to manage third-party risk. These third-party risk management programs fall short of including the risk posed to the organization by the employees of third parties who are provided with access to facilities, systems, and data and they almost never take into consideration the non-human worker risk – bots, IoT devices, and robotic process automation (RPA).

The problem is now coming to a head as the sheer volume of third parties with access is overwhelming most organizations' security teams. If an organization exposes its systems and data to any outside third party, the organization is responsible for the risk to its own data and systems as well as any data they are the custodian of.

Yet at most organizations little-to-nothing is done to measure or mitigate the risk that these third parties and their non-employees with access create.

Tracking and managing employees is challenging enough but introducing non-employees into an organization's systems creates unique challenges that most Identity and Access Management (IAM) tools are not designed to accommodate. Organizations try to solve for this problem with manual efforts and customizations to existing systems that are costly, time consuming, and ultimately, have proven to fall short. Organizations that have a modern third-party risk management (TPRM) system in place approach TPRM with a "risk-first" mindset that integrates cybersecurity, compliance, IAM, and risk governance.

Organization Level Risks

In general, to determine risk, organizations assess their possible exposure to identified risk factors and the potential business impact or disruption of these risks. When it comes to TPRM, most organizations focus their strategies at the third-party organization level. Best practices include conducting an assessment to identify gaps between existing and desired practices and controls and then the required remediations to bring the third party into compliance within risk thresholds. However, this approach does not consider the risk posed by third-party non-employees and non-human workers that are granted access. By not assessing the risk of the third-party worker, organizations find themselves out of compliance with their own internal risk threshold and business practices as well as industry and government regulations.

Individual Level Risks

At the individual level, a third party is considered any non-employee of the organization who requires some level of access to the organization's facility, data, or systems. Historically, these individuals' identity lifecycle and access have been managed at the account level and access is "one size fits all". However, this approach has resulted in large numbers of non-employees (who cannot be individually identified and verified) having substantial overprovisioning. This unmanaged approach greatly expands the organization's attack surface and the number of hacker-friendly privileged accounts.

The complex, third-party relationships of today demand that priority be placed on validating the identity status of every non-employee and meticulous management of their entire identity lifecycle, including their risk. To do this accurately and efficiently requires a complete understanding of the third-party relationship at the organization level, the job function of the non-employee, the internal/external people responsible for the non-employee, and the timely termination of access to the organization when appropriate. This comprehensive assessment of identity risk should be performed *prior* to any non-employee being granted access to assets and at intervals throughout their relationship with the organization.

Five Shortcomings of Traditional Third-Party Identity Risk Management Approaches

Many organizations successfully manage employee identity and access through their existing IAM systems. These systems are utilized for both employees and non-employees, however, the absence of a non-employee identity authority severely limits the IAM system's ability to properly govern third-party, non-employee access.

Typically automated, IAM systems and HR systems work together to manage many tasks including onboarding, payroll, and access for direct hires. Unfortunately, the same is not true for their effectiveness in managing the end-to-end lifecycle of non-employee identities without an identity authority.

The Top 5 dangers to traditional approaches include:

1. Limited focus on non-human identities

   Traditional IAM processes and systems have been designed for employees of an organization. The process is relatively straightforward and uncomplicated. However, these systems fall short in supporting the needs of non-human third parties due to the lack of contextual data needed to drive well-informed identity, access, and risk decisions.

2. Limited or no validation

   There are virtually no identity checkpoints prior to an organization granting access to non-employees. The non-employee is granted access based solely on the reputation of their third-party employer and with limited or no verification that they are who they say they are, their origin, job function, or the risk they pose. The fact that an organization needs an identity authority to manage these identities before governing access is often realized after a breach has occurred.

3. Manual processes

   With this approach, third-party identity risk is managed manually via spreadsheets or other makeshift processes. This very time-consuming approach is costly, peripheral in nature, and prone to error. Couple this with management tasks typically being dispersed among numerous teams – HR, IT, Compliance, and Legal – with ad hoc or substandard solutions (never intended to manage non-employee identities in the first place), and the threat of a third-party breach grows.

4. Incomplete risk insights

   Organizations entrust third parties to provide accurate risk information, however, this information is seldom verified by the organization. Instead, organizations blindly accept the information the third party is providing with no accountability. A Ponemon Institute study revealed that 63% of organizations did not evaluate their third parties' security practices.

5. Limited governance at every stage of the third-party lifecycle

   The complete view of a non-employee's identity lifecycle– from onboarding to off-boarding – is rarely monitored or audited. As a result, organizations seldom remove access in a timely manner and in many instances do not remove it all once it is no longer required.

Understandably, without a dedicated, purpose-built solution that enables organizations to collect individual, non-employee data collaboratively and continuously and without a means to gauge identity risk before granting them access and throughout the identity lifecycle, most organization's traditional third-party identity risk management approaches will fail to keep their assets safe.

How Identity Management Combined with Third-Party Risk Management Can Reduce Risk at Every Stage of the Third-Party Identity Lifecycle

Broadly speaking, the identity lifecycle of a non-employee consists of three stages: Onboarding, Management (or auditing), and Off-boarding. Each stage presents its own unique risks that can be addressed by expanding the view of the non-employee's risk to the organization.

Stage 1: Onboarding – Know your insiders

The process of onboarding non-employees must start by determining their inherent risk (or the risk they pose prior to granting access.) Once you have a clear picture of the risk they pose, the next step is identity proofing, i.e., verifying their identity and authenticity prior to accessing the organization's system.

Challenges of Onboarding

Organizations face several challenges when onboarding third-party, non-employees. The following is a list of the most common. Not coincidental, these challenges are also the leading causes of third-party breaches.

Using the wrong tools

Using repurposed human resources information systems (HRIS) to identify third parties is ineffective, inefficient, costly, and in most instances a legal liability. These systems were designed strictly to manage employees and are not equipped to manage non-employee data. Additional risks arise with the use of non-humans. In many organizations there are often more bots, IoT devices, and robotic process automations ([RPA] is business process automation technology based on metaphorical software robots or on artificial intelligence/digital workers) granted access to an organization's assets than there are their human counterparts. This access is typically privileged making it much more valuable to a cybercriminal.

Disjointed processes

The onboarding process is disjointed and executed in an ad hoc manner involving multiple internal teams, each with different priorities. As such, the collection of third-party data and risk assessments are often kept in spreadsheets located on a shared drive and lack consistency. Furthermore, most organizations do not appropriately maintain this data, which is essential to proactively governing access and ensuring timely changes or termination of access.

Limited risk visibility

Identifying and organizing third parties at scale is a reactive process that lacks proper security, scrutiny, privacy, and compliance assessments to evaluate risk. Consequently, there is a lack of contextual data about both third-party organizations and their workers, resulting in low visibility at the individual level. This often leads to over-provisioned third-party users. Thus, it becomes impossible to follow a zero-trust security strategy and makes formulating well-informed, timely decisions regarding access unfeasible. In fact, a 2021 Ponemon Institute survey concluded that 74% of respondents attributed their data breaches a result of giving too much privileged access to third parties.

Trusting third parties

The lack of control over third-party, non-employees compels organizations to trust the third parties with its internal vetting processes and appropriate approvals for access. This misplaced trust assumes that each third party is following the same security processes as the host organization and that they are maintaining accurate, updated information on each of their employees, managing the information in a timely manner, and notifying the organization of any changes.

Onboarding Best Practices for Accurate Risk Assessment

Automation

Replacing manual processes with automation reduces cost, time-to-value, and third-party risk. Automation enables consistent application of best practices for third parties and tackles the limitations of existing onboarding tools such as spreadsheets. It also provides an accurate and dynamic record of the third-party landscape and streamlines data collection, identity proofing, risk assessment, and lifecycle management, making it simple to maintain data via reliant systems.

Collaboration

Identity collaboration should include non-employee information from both internal sponsors and external sources (including the third-party's employer) and the non-employee themselves. This effort should include collection of all pertinent non-employee information (role, department, location, skillset, etc.) and be comprehensive in details including verification of credentials, licenses, certifications, etc. A collaborative, comprehensive, and accurate record of the non-employee's identity when onboarding is key in determining a fair risk assessment before granting access.

Visibility

Organizations can reduce third-party risk by gaining visibility into their vendors' inherent risk prior to onboarding them. For example, accessing a library of completed vendor risk assessments with supporting evidence that presents an inherent risk score is a start toward understanding how to right-size ongoing due diligence or determine if their risk profile is acceptable to your organization.

Stage 2: Identity Management (Auditing)

Auditing third-party access ensures communication between the organization and the third party and proactive identity lifecycle management of a non-employee. It is also essential that third parties conduct their own internal audits at the employee level to mitigate risk even further.

Third-Party Auditing Challenges

Poor audit trails

Many organizations fail during an audit because they cannot produce third-party identity access information. One of the more common reasons for failure is that even if the organization manages to collect the access data (which requires significant manual effort and time), they have no justification for the continued access some third parties have beyond their lifecycles. More than half the respondents of a recent Ponemon

Institute study did not have an inventory of the third parties that had access to their systems.

One and done

Once "onboarded," third party, non-employees are all but forgotten, thereby opening avenues for security breaches resulting from "orphaned accounts" that retain access to the organization long after the non-employee has left the third party. Equally as ineffective is auditing third-party access on an annual basis which simply isn't frequent enough, considering the dynamic nature of third-party usage and access to an organization's assets in today's high-threat environment.

Best Practices for Third-Party Audits and Continuous Risk Assessments

Ensuring that regulatory and legal requirements are optimized for compliance requires visibility into third-party access at the organization and identity-level. This is achieved through a comprehensive understanding of the organization's culture, risk appetite, trustworthiness, job function, best practices, accreditations and certifications, and the type of training put in context. The insights derived from validation exercises allow for proactive third-party identity and access maintenance and management.

Consistency

It is also necessary to have consistent, updated risk assessments over the lifecycle of the third-party relationship as risk is organic and numerous factors impact risk scores – resulting in risk scores moving up or down. Identity proofing, the process of collecting, validating, and verifying information about a person is correct, at regular intervals in the lifecycle ensures that if access needs have changed that they have been adjusted in a timely fashion. Often, the non-employee may still require access, but not as much access as they may have acquired over time.

Context and Continuity

Given the natural changes to business that occur over time, each third party's structure should be periodically re-evaluated. These periodic evaluations should be in the same likeness as the original assessment to ensure continuity in rating/scoring. Yet, it must also be contextual; accounting for changes in the services and processes of the third-party organization.

Behavioral Analytics

Being vigilant for anomalous, third-party behavior, such as access from unexpected locations or odd times of the day increases awareness and the ability to respond quickly when threats arise. Frequent re-validation of identity and access status is paramount to proactively managing the third-party lifecycle.

Stacked verification

For many organizations, account inactivity and access removal are a cause-and-effect relationship. However, a layered procedure for off-boarding third parties allows for proactive maintenance of third-party, non-employees. Regular access validation also helps organizations gauge identity-level risk. There are three layers of verification to consider:

- Layer 1 (inactivity reports): In the event a non-employee has not accessed the organization for a certain amount of time, access would be deactivated. This level of verification should be considered the last resort for access removal because it leaves an account vulnerable during the inactive period.

- Layer 2 (risk-dependent validation): Contingent upon the third party's risk level, validation can be set to automatically occur on a weekly or monthly basis. This includes finding out who the third party's sponsor, hiring manager, or external vendor manager is and distributing the responsibility of maintaining the non-employee's records.
- Layer 3 (self-attestation): Emailing the third party on a weekly/monthly basis to confirm the non-employee's job status is self-attestation confirmation. Attestation email notification may go to the non-employee's third-party email address, so responding via this process serves to verify their employment status with the third-party vendor (since the non-employee would still have access to their email account.)

Continuous Monitoring

A lot can happen between annual control-based vendor risk assessments, and that vendor activity can impact your compliance posture too. That's why it's important to continuously monitor third parties for:

- Cybersecurity vulnerabilities such as exposed credentials for sale on the Dark Web
- Adverse media and negative news such as regulatory and legal sanctions, missed earnings, or executive changes that can signal a shift in strategy or impact their ability to deliver
- Financial performance to evaluate the health of third parties
- Breach events that may not have been reported, providing additional context into cybersecurity practices

Critical to third-party risk management is incorporating these continuous monitoring insights into regular decision making, and correlating findings with regular controls-based assessments and mapping the results to compliance frameworks to prove to auditors that you have a process in place.

Stage 3: Off-Boarding

Off-boarding third parties or terminating a non-employee's access is equally as important as onboarding. Timely removal of access may be the **single best practice** (and is also the most overlooked) an organization can follow to reduce the threat of a breach from an orphaned account.

Offboarding Challenges

Accurate and timely communication

Receiving clear and accurate information from third-party vendors on a timely basis can be difficult. Often an organization will receive information regarding a termination of a non-employee too late or never at all.

Best Practices for Off-Boarding

Automation

Automation can be deployed in various ways during off-boarding:

- Setting end dates can be used to deactivate the authoritative records of a third party, triggering account disablement to a granular level. End dates can also be used for revoking access if the self-validation process is not completed by a predetermined deadline.

- Automation can be applied to revoke access based on a change in risk score.
- Lastly, automation can prevent orphaned accounts by automatically disabling access when the identity is deactivated.
- In highly regulated industries like healthcare, manufacturing, insurance, and financial services, a well-defined off-boarding business process must be in place and inclusive of an automated, authoritative identity source in order to effectively and efficiently meet industry regulations.

A third-party relationship may eventually come to an end, but your risk exposure doesn't disappear when the contract is terminated. There are final obligations to meet, data destruction procedures to follow, ongoing service agreements to consider, vendor access and credentials to remove, and final payment terms to confirm. Consider implementing the following as part of your third-party offboarding process:

- Conduct contract assessments and reviews: Schedule tasks to review contracts to ensure all obligations have been met. Issue customizable contract assessments to evaluate status.
- Issue offboarding surveys: Leverage customizable surveys and workflows to report on system access, data destruction, access management, compliance with all relevant laws, final payments, and more.
- Implement workflow: Increase efficiency with automation and rules that automatically suggests actions based on answers to offboarding assessments and routes tasks to additional reviewers.
- Centrally manage documents: Centrally store and manage documents and certifications, such as NDAs, SLAs, SOWs and contracts.
- Remediate risks immediately: Take actionable steps to reduce vendor risk remediation recommendations and guidance.
- Produce risk reporting: Identify, alert, and communicate exceptions to common behavior.
- Report against compliance requirements: Visualize and address compliance requirements by automatically mapping assessment results to any regulation or framework.

Leveraging SecZetta and Prevalent to Improve Third-Party Identity Risk Management

Prevalent and SecZetta have partnered to close the critical gaps threatening the assets of organizations by eliminating the challenges associated with the management of third-party relationships. Prevalent, a recognized leader in third-party risk management (TPRM), provides visibility into third-party risk by assessing and engaging with third parties at scale while SecZetta provides rich, user-level identity data insights that an organization would otherwise be unable to obtain.

This powerhouse duo offers an integrated third-party identity and risk management solution that empowers an organization's IT security team with contextual, risk-based access control for its third-party, non-employees.

SecZetta's Third-Party Identity Risk solution can be set to automatically adjust a non-employee's status based on security incidents, exposed credentials, compliance violations, and other company-level risks identified by the Prevalent Third-Party Risk Management Platform.

Key benefits include:

- The ability for an organization to make informed access decisions by correlating risk scores between third-party companies and non-employees.
- Quick incident response to external threats with continuous vendor risk intelligence.
- A simplified, unified approach to third-party identity, lifecycle, and risk management.
- Substantial reduction in risks associated with third-party breaches.

Organizations utilize Prevalent's software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers and other third parties. Prevalent's flexible, hybrid approach to TPRM is tailored to each organization's unique needs and is well known for delivering a rapid return on investment. Regardless of where an organization starts, Prevalent can stop the pain associated with TPRM by removing the complexity of making informed decisions and accelerating adoption and maturity of an organizations TPRM program.

SecZetta's Third-Party Identity Management solution enables organizations to execute risk-based identity and access lifecycle strategies for diverse non-employee populations. Because the solution suite is purpose built, it's uniquely able to manage the complex relationships organizations have with non-employees in a single, easy-to-use application that simultaneously helps facilitate commercial initiatives, support regulatory compliance, and reduce third-party risk.

How SecZetta and Prevalent Work Together

Secure Third-Party Non-Employee Onboarding

A third party onboards their employees in the SecZetta solution, where administrators can access company-level risk scores from Prevalent. All third-party employees inherit the same baseline score, which can be adjusted for each individual based on their role or other attributes. SecZetta then passes this data to an IAM solution for further action.

Build a Comprehensive Vendor Profile

Prevalent provides comprehensive third-party intelligence to build authoritative company profiles, including industry and business insights, beneficial ownership, 4th-party relationships, and more.

Risk Scoring & Analysis

The combined solution enables customers to quickly gauge vendor risk impact with straightforward A (high risk) to E (low risk) domain-level ratings.

Dynamically Adjust Access Based on Organizational Risk

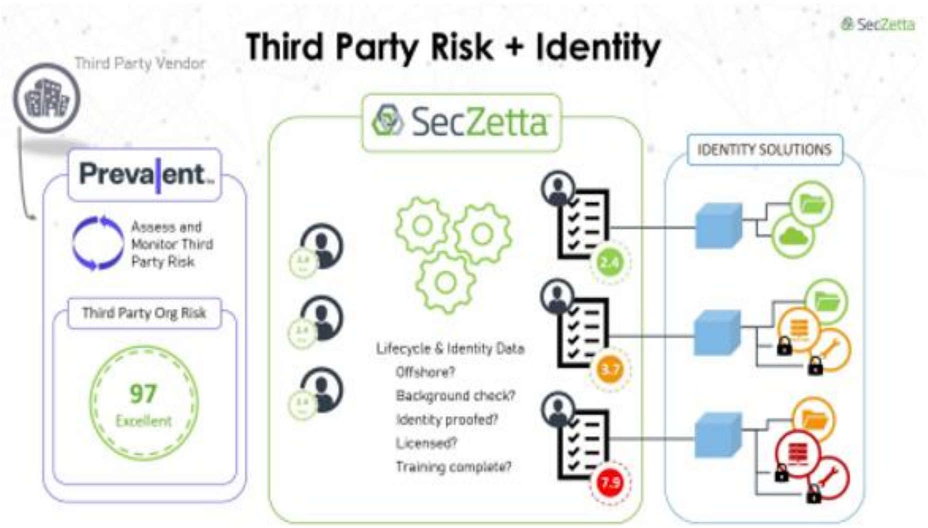
SecZetta can adjust risk scores in concert with Prevalent's risk assessment results and continuous threat monitoring data, enabling IT security teams to fine-tune third-party employee access as their companies' risk levels change.

Automated Workflow for Updating Scores

SecZetta pulls recent, company-level risk data from Prevalent, automatically applies a risk rating to all employees, and then dynamically adjusts each non-employee's risk score as needed.

Incident Response

Should an organization be breached, the incident can be immediately communicated to SecZetta so that all relevant profiles can be terminated, resulting in timely removal of access. If terminating all access is not a viable option, SecZetta offers the flexibility to terminate access based on a number of factors including system access, location, and risk score. Once security controls are re-established in compliance with the organization's risk threshold, access can be immediately re-instated in entirety or through phases based on the organization's needs.



Prevalent and SecZetta provide a complete solution for third-party identity and risk management.

Take the Next Step to Reduce Third-Party Identity Risk

Many organizations today rely heavily on third parties to operate, which generally means granting third-party non-employees with access to systems and networks. However, non-employees often receive access without consideration for the individual risks they pose to the organization. This disconnect between third-party identity management and company-level risk opens the front door wide to data breaches, compliance violations, and other business disruptions.

Together, SecZetta and Prevalent have a solution that provides visibility, automation, and scale in reducing third-party identity risks. Take the next step by contacting us today.

Prevalent

WEBSITE: www.prevalent.net
FREE DEMO: http://www.prevalent.net/demo
☎ 877-773-8253
📍 1181 N. Tatum Boulevard, Phoenix, AZ 85028

SecZetta

WEBSITE: www.seczetta.com
FREE DEMO: www.seczetta.com/demo
☎ 781-832-0767
📍 1082 Davol St., Fall River, MA 02720

About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers and other third parties across the vendor risk management lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time. For more, visit www.prevalent.net.

About SecZetta

SecZetta is the leading provider of third-party identity management solutions. Our solutions enable organizations to execute risk-based identity access and lifecycle strategies for diverse non-employee populations. Because the solution suite is purpose-built, it’s uniquely able to manage the complex relationships organizations have with non-employees in a single, easy-to-use application that simultaneously helps facilitate commercial initiatives, support regulatory compliance, and reduce third-party risk. For more information visit, https://seczetta.com/

SecZetta

THE FIRST STEP TO ZERO TRUST: ACCURATELY IDENTIFY AND MANAGE WHO HAS ACCESS

Introduction

A decade ago, a strong perimeter strategy was considered the best security practice for keeping an organization's facility, network, and data secure. The premise was simple; successfully guard your network perimeter, and your assets remained safe.

Today's digital transformation has dramatically changed the security landscape from the perimeter defense standard that afforded access strictly to an organization's employees to one in the cloud where security best practices must be incorporated far beyond the walls of an organization. Gone with the perimeter is also the notion that access is provided to employees alone. In fact, many organizations have such a substantial operational reliance on third parties that they actually have more "outsiders" who are provided with "insider" access than employees.

According to a recent report by Ponemon Institute, **51% of businesses have suffered a data breach caused by a third party.** This could be an individual in the organization's supply chain, an IT service provider, volunteer, consultant, partner, or even a non-human service granted access to the organization's data and systems. In short, despite strong defenses, most organizations are still only locking their front door and unknowingly leaving their windows and interior doors to their assets wide open to a breach from a third-party, non-employee.

The results of these breaches have been devastating. The 2021 Cost of a Data Breach Report detailed the average cost of a third-party breach to be **$4.29 million** – $370,000 more than a non-third-party data breach. So it's no surprise that in May 2021, the White House stepped in, delivering an Executive Order that mandates changes directed towards modernizing cybersecurity strategies to limit the number of breaches at U.S. government and related organizations.

At the core of the federal government's mandate is the advancement and implementation of zero trust architecture. Zero trust means that absolutely no one is entrusted (from inside or outside the network) to an organization's assets and that verification is required for everyone trying to gain access to an organization's resources. While the term "zero trust" may appear new, the idea of enhancing "perimeter-less security" or enforcement of "least privilege" is not. In fact, cybersecurity professionals have been touting the importance of "zero trust security" for years – just in different terms.

A large number of high-profile breaches in the news, combined with the federal mandate, have left organizations scrambling to understand what zero trust means for their organization and how to integrate their own zero trust strategies as quickly and cost-effectively as possible.

But where to start? Identity. Identity. Identity.

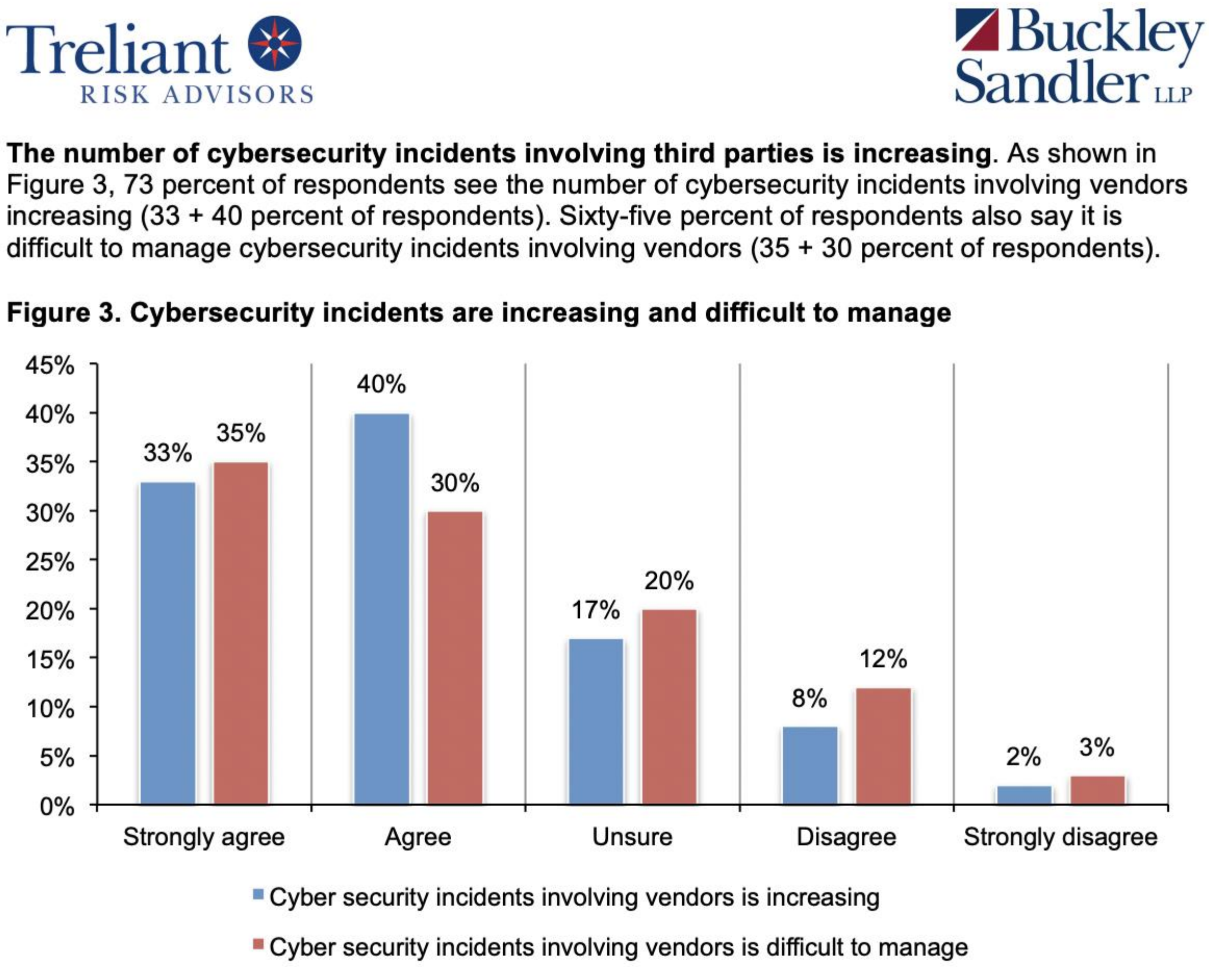
The answer is simple. Start at the beginning. **Identify who has access to your organization's assets and manage their identities** accurately, effectively, and efficiently so access to assets can be governed wisely. If you can't identify who has access to your assets, how can you manage their identity and gauge their risk to your organization?

Many organizations' identity programs are still primarily designed to manage **employee identity**. Some of these programs may even be based on zero trust principles but all lack the contextual third-party data that is needed to make well-informed decisions about non-employee, third-party access. And while most IGA systems are designed to manage both employee and non-employee access, the absence of non-employee contextual information severely limits an IGA system's ability to properly govern their access.

However tempting, it is not practical to use a HRIS to create an authoritative source of information for third-party non-employee users. This is mainly because these users are fundamentally different than employees. They have unique, non-linear relationships with the organizations, require collaborative onboarding and identity lifecycle management, and in some countries, may create legal liability for the organization if housed in a HRIS.

Why Third-Party Identity Risks are Crushing Zero Trust Strategies

Cost savings, on-demand access to sought after skillsets, business efficiencies, and even the COVID-19 pandemic are just a few forces driving organizations to provide network, data, and facility access to a diverse population of third-party partners, individual contractors, supply chains, volunteers, and non-humans (like bots and IoT devices.) A Ponemon Institute study found that the average organization utilizes nearly **6000 third parties** in various business functions. This increased volume has pushed manual identity practices, proprietary solutions, and customized IGA systems beyond their limits, rendering them inadequate to keep assets safe.



Treliant RISK ADVISORS

Buckley Sandler LLP

The number of cybersecurity incidents involving third parties is increasing. As shown in Figure 3, 73 percent of respondents see the number of cybersecurity incidents involving vendors increasing (33 + 40 percent of respondents). Sixty-five percent of respondents also say it is difficult to manage cybersecurity incidents involving vendors (35 + 30 percent of respondents).

Figure 3. Cybersecurity incidents are increasing and difficult to manage

45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
33%
35%
40%
30%
17%
20%
8%
12%
2%
3%
Strongly agree
Agree
Unsure
Disagree
Strongly disagree
Cyber security incidents involving vendors is increasing
Cyber security incidents involving vendors is difficult to manage

Full report: Data Risk in the Third-Party Ecosystem

Customized IGA Systems

A well-planned and executed zero trust strategy can not be accomplished by trying to customize IGA systems to manage the full identity lifecycle of non-employees. IGA solutions are not designed to provide contextual third-party non-employee information or to adequately weigh the identity risks necessary to govern access. They are incapable of meeting the zero trust principles to "identify, measure, and mitigate threats" when used alone.

IGA solutions are designed to manage access – not identity – and while one might be able to support a small number of external users through a form-based method, it is not a scalable approach for supporting diverse external population types or high volumes of users.

Human Error

According to global cybersecurity education experts, Cybint Solutions, **95%** of cybersecurity breaches result from human error. The predominantly manual processes that enable most third-party identity management programs plus the sheer volume of non-employee identities within an organization creates increased vulnerability. Couple this with identity lifecycle management of non-employees dispersed among numerous teams; HR, IT, Compliance, and Legal with ad hoc or substandard programs (never intended to manage non-employee identities in the first place), and the threat of a third-party breach appears to grow exponentially.

The large number of team members necessary to manually onboard non-employees is an extremely inefficient use of resources. Oftentimes this is a costly, time-consuming approach that typically results in copying credentials from one non-employee to another with limited thought given to the processes surrounding deprovisioning access when it is no longer needed.

Zero Trust Begins with SecZetta's Third-Party Identity Risk Solution

Understandably, without a dedicated, purpose-built solution that allows organizations to collect each individual third-party non-employee's data collaboratively and continuously and without a means to **gauge identity risk before granting them access**, most organization's zero trust strategies will fall short.

SecZetta provides a robust third-party identity risk solution that is easy to use, integrates swiftly with peripheral systems through an open API, and allows organizations to execute risk-based identity access and lifecycle strategies for *all* third-party non-employee populations.

This centralized, automated, and **authoritative solution to non-employee, third-party identity risk management is rooted in zero trust**. SecZetta's flexibility via no-code system configuration allows organizations to gather the non-employee data most pertinent to them for complete identity accuracy in governing access.

From day one, SecZetta can begin working with a multitude of HR, VMS, TPRM, or IAM platforms to:

- Support your zero trust strategy
- Improve operational efficiency
- Streamline compliance audits
- Assess risk
- Provide identity verification
- Deprovision access at termination

SecZetta's Third-Party Identity Risk Management solution is rooted in zero trust and works to help harden systems against third-party attacks while solving the numerous challenges surrounding third-party, non-employee identity and risk management. For more information or to schedule a demo, visit https://www.seczetta.com/request-a-demo/ or call us at (781) 832-0767.

WHY AN IDENTITY MASTER REPOSITORY IS CRUCIAL TO AN ORGANIZATION’S SECURITY

Consolidating Records into a Single Source for Workforce Identity Should be Part of Every IAM Strategy

Introduction

Organizations have realized that properly managing user identities is a critical component of their digital security strategies. However, traditional methods of creating a Master Identity Repository have proven tremendously labor intensive and error prone. The evolution of digital technologies and the growing number and wide range of users has created a new set of challenges. From identity sprawl caused by users' identities being managed by multiple disconnected systems to trying to create order after a merger or acquisition, the need for a master identity repository has never been greater.

This paper details the complexities organizations encounter as they manage digital identities. It will also explain how to consolidate the data from multiple identity sources to create a single true identity that can be added to a Master Identity Repository and used for downstream systems.

Challenges of Managing Digital Identities

Organizations attempting to manage their digital identities struggle with excessive complexity. They may have multiple systems of record for managing identities, which can result in duplicate databases or separate identities stored as vendor records, human resources records, and student records.

Employees and rapidly growing numbers of third-party users can have increasingly fluctuating relationships with organizations. Oftentimes, new identities are needed to align with the access required for each new role. These changing, varied relationships may then result in a duplicate directory or other application accounts.

The result can create inaccurate, outdated, or multiple active identities for the same person which can leave the organization out of compliance and more vulnerable to security breaches. When organizations undergo a merger or acquisition, tracking down this disparate digital identity information for employees and third-party users that work with the acquired/merged company and incorporating them into the parent organization's system of record becomes a tedious, time-consuming, and error-prone task.

Multiple systems of record

Many organizations store information about individuals in multiple systems of record. For example, a single healthcare worker may have their record managed in a hospital records system, an employee HR information system (HRIS), and also a student records repository. When a person's record exists within these multiple systems, duplicate accounts are often created for the same person in downstream systems. This results in either very frustrated and confused end-users as well as a massive reconciliation effort to remove and consolidate duplicative accounts. Further, if accounts do not get cleaned up, it exposes more avenues to potential breaches as well as issues with compliance, payroll, taxes, and audits.

Identity sprawl

An individual's affiliation and relationship with the organization can change over time. A freelancer might be hired full-time. A student at a university could become an employee or research assistant and ultimately an alumnus. An individual might start a relationship with an organization as a volunteer, and then become a medical student, a hospital employee, join a practice as an affiliate, or open their practice.

As relationships change, the organization usually creates a new record for each role. Resulting identities created from that record come with specific permissions and access to data sources necessary to fulfill that role. When an individual has multiple authoritative records, the organization can easily end up with inaccurate data or multiple active identities for the same person. This can potentially:

- Provide additional access points to sensitive data if a bad actor discovers open accounts.
- Leave an organization out of compliance and vulnerable to security breaches.
- Be problematic for HR teams and Identity/Security teams that assign and track user privileges.
- Make it impossible to apply policies and/or audit populations properly. For example, an employee terminated for cause could be allowed to return through a third party.

Increasing numbers of third parties with credentials

According to a recent Ponemon Institute survey, 59% of global companies said they have experienced a data breach caused by one of their vendors or third parties. In the US, the percentage is 61%. For example, in March of 2020, one of an American multinational conglomerate's third-party service providers experienced a data-leak due to unauthorized access to an employee email account that exposed data such as passports, birth certificates, marriage certificates, death certificates, and other data. Another breach which targeted a third-party email vendor impacted more than 1 million mobile phone customers and employees by stealing customer data such as names, addresses, phone numbers, account numbers, rate plans, and billing information. In yet another example, over 8 million retail customer sales records in multiple countries were exposed due to a security vulnerability in a third-party app.

Still organizations often do not have a system of record for third-party users, including contractors, vendors, affiliates, freelancers, partners (i.e., supply chain), and others who have access to their systems and proprietary information. Organizations often use a hodgepodge of manual communications, tools, and spreadsheets to gather information needed about the third-party user to make access decisions. This is a very manual process that is time-consuming, subject to human error, and not easily auditable. These inefficient processes result in:

- Incomplete inventory of third-party workers, customers, and service accounts.
- Multiple identities for each employee and non-employee.
- Accumulation of access to sensitive data or areas during the relationship.
- Unclear understanding of the network, data, systems, and personally identifiable information (PII) those identities can access.
- Inability to identify users who no longer need access.
- Lack of support for rapid onboarding.
- Use of costly home-grown or customized systems for third-party identity management.

Mergers and acquisitions

During a merger or acquisition, thousands of employees and third-party users may need to be added to the parent company's digital identity management system. Without automation, it can take hundreds of hours to determine which of these employees and third-party users are valid, how many duplications there are, and to consolidate authoritative records to create a master identity. This timeline is not only cumbersome but unacceptable for workers who may need access to systems and data to perform critical job functions.

What's Necessary in a Solution

Simplifying digital identity management for enterprises requires an automated solution that can efficiently merge data about employees and third-party users from many different sources to establish a master identity in one centralized repository. To manage this Identity Master appropriately, organizations should look for a solution that delivers:

- Authoritative record consolidation
- Identity master repository
- Record matching capabilities
- Manual escalation verification
- Automation
- Ease of use

Authoritative record consolidation

The solution should merge and organize authoritative record data from many different sources such as HR systems or other repositories into a single system of record to create a master identity in a centralized repository. To do so, it should easily integrate with the industry standard vendor management, HRIS, and identity management solutions as well as be able to upload data from homegrown databases or flat files. It should also support data clean-up in directories and applications or create a unique identifier (UID) that can be used across downstream systems, directories, and applications.

Identity master repository

Identity consolidation allows the organization to understand who is out there and what their status is so well-informed decisions about the global workforce and non-employees can be made. The result is an identity master repository that helps an organization manage all aspects of a user's relationship and their entire lifecycle with the organization to reduce cost, meet compliance regulations, and most importantly, mitigate risk.

Record matching capabilities

To create the master record, the solution should be able to pull attributes from existing systems of record and use these to build a single master identity, even without a common unique identifier (such as SS number) across sources. Organizations should be able to define what criteria in each data source are most critical for producing a high confidence match and use a configurable scoring system to ensure that the most important data/records are given priority in the master record. Organizations should be able to set these priorities per attribute and within a specific time frame. If desired, organizations should be able to avoid using PII for identifiers to minimize the risk of exposing PII and of running afoul of regulations such as CCPA and GDPR.

Manual verification

The automated process should include a separate holding repository for uncertain matches so they can be escalated and reviewed manually. This holding area allows a human to make fact-based decisions when a judgment call is necessary.

Automation

The solution should automate the process of creating master identities for thousands of people at the same time. Thus, if the organization undergoes a merger or acquisition and needs to onboard thousands of employees and third-party users they can do so with less cost, time, errors, and risk than they could using manual processes.

Ease of use

The solution should provide a clean and modern point-and-click user (no code) interface to make it quicker and easier for administrators to configure and manage identities without expensive customizations or specialized IT resource assistance.

Integration

The solution must be able to integrate with vendor management, HRIS, and other downstream applications like identity access and management systems.

Conclusion

With digital identity foundational to data privacy and security, organizations must accurately manage the identities for any user accessing their IT systems. Today's siloed, manual systems and processes are simply not up to the task. Multiple systems of record that are not consolidated into a single identity master can result in identity sprawl, inaccuracies, the duplication of identities, and an expanded attack surface. These challenges are compounded by the increasing prevalence of third parties accessing internal IT systems and the need to incorporate large numbers of new identities in the wake of a merger or acquisition.

Fortunately, identity master solutions are now available that automate the process of record consolidation providing a single identity master as a source for identity management solutions. Using these solutions together, organizations can speed and simplify the management of all aspects of a person's relationship with the organization across their entire lifecycle, reducing cost, improving security, and easing regulatory compliance.

[1] Major Third-Party Data Breaches Revealed in March

About SecZetta

SecZetta is the leading provider of third-party identity management solutions. Our solutions enable organizations to execute risk-based identity access and lifecycle strategies for diverse non-employee populations. Because the solution suite is purpose-built, it's uniquely able to manage the complex relationships organizations have with non-employees in a single, easy-to-use application that simultaneously helps facilitate commercial initiatives, support regulatory compliance, and reduce third-party risk.