TAG

IMPROVING USER ACCESS AND IDENTITY MANAGEMENT TO ADDRESS MODERN ENTERPRISE RISK

DR. EDWARD AMOROSO, FOUNDER & CEO, TAG
JOHN J. MASSERINI, SENIOR RESEARCH ADVISOR, TAG

BEYOND IDENTITY

IMPROVING USER ACCESS AND IDENTITY MANAGEMENT TO ADDRESS MODERN ENTERPRISE RISK

DR. EDWARD AMOROSO, FOUNDER & CEO, TAG.
JOHN J. MASSERINI, SENIOR RESEARCH ADVISOR, TAG[1]

With the enterprise shift from perimeter security to zero trust, user access and identity management have emerged as essential functional controls, especially in the context of work-from-anywhere initiatives. In this report, we review the evolving role of identity and user access, the positive impact that a strong identity management program can have on the enterprise, and how such a program complements compliance and cyber insurance.

INTRODUCTION

The need to evolve the cybersecurity of enterprise infrastructure was driven, at least in part, by the demands of an increasingly remote workforce. Over the past several years, including during the COVID-19 pandemic, the adoption of zero trust architectures, cloud-first initiatives, work-from-anywhere strategies, and perimeter-less networks have all relied on the presumption that the security controls around user access needed to change.

Unfortunately, user access has been one of the *least managed* security controls within the typical organization. For example, active accounts with owners who have left the company, executives who refuse to change passwords, service accounts being reused by countless applications, and cloud environments with undocumented trust relationships, all illustrate the poor identity management practices in use across many organizations.

[1] *This technical report was developed by the TAG Analyst team led by Dr. Edward Amoroso. Much of the report was developed and written by longtime industry expert, Mr. John J. Masserini, during his tenure supporting research and advisory project work within TAG.*

We explain in this report how modern approaches to user access and identity management are required to ensure that proper control is in place for the modern enterprise. Commercial vendor **Beyond Identity** is used to illustrate our points since their platform effectively implements the concepts being shown here. Specifically, we focus on how improved user access and identity management can streamline compliance, security, and even insurance.

EVOLUTION FROM PASSWORDS

The first time a password was used on a computer system was six decades ago. It's thus surprising that despite the advances of modern technology experienced since, our private information, critical infrastructure, and use of applications continue to rely on passwords for security. It is clearly time now for organizations to fundamentally rethink how user access and identity management can evolve to meet the needs of the modern organization.

The urgency of making such a change is evident in publicly available data. For example, a recent report from the Identity Defined Security Alliance reflects that 84% of organizations had an identity-related breach in 2021. Additionally, the 2023 IBM Cost of a Data Breach report shows that phishing and stolen credentials continue to remain the top two attack vectors. These are fixable problems, but they require rethinking user access and identity management.

The challenge of driving such evolution is complicated by the depth of technology debt that most organizations carry. While modern IT infrastructure has moved to adopt new technologies such as Kubernetes, DevOps, and SaaS, many are still heavily dependent on mainframes, legacy software, and countless other older systems. The one security thread that weaves these modern and legacy systems technology together is the user credential.

THREAT VECTORS

When we look at the disparate technologies across the enterprise, they all have different threat and attack vectors. Missing patches, misconfigured services, and network dependencies all play a role in how attackers approach targeted systems. The one common vector that is technology independent – and that is successful against any device, any network, any application, or any infrastructure involves *targeting the user*.

As suggested above, the password remains the most often attacked because it is invariably the weakest link. While the security community has tried to educate users on the use of stronger passwords, multi-factor authentication (MFA), and biometrics, the abuse of user credentials is still the primary attack vector across all platforms. This is unfortunate since there are so many excellent commercial options – including vendors such as Beyond Identity.[2]

Sadly, the reason for such slow progress is fundamentally human. Most users simply have too many passwords, and these are required to be complex and changed too frequently to remember. According to a recent study, the average person has over 100 passwords they have to remember at any given time.[3] It has been obvious for some time now that a better approach to managing user access is required.

LEVERAGING REGULATORY FRAMEWORKS

Depending on the industry, most organizations will have a range of different government, sector-specific, or customer-demanded requirements that need to be satisfied as part of assessments and

[2] Technical discussions with the team from Beyond Identity helped immeasurably during the production of this report. Useful information on their passwordless multifactor and zero trust authentication solutions can be found at https://www.beyondidentity.com/.
*[3] See **https://tech.co/password-managers/how-many-passwords-average-person**.*

audits. This was previously only applicable to larger companies, but more recently, this has expanded to include mid-sized and even smaller companies. The major frameworks that apply in most cases include the following:

- **CCPA (California Consumer Privacy Act):** CCPA primarily focuses on the privacy of personal information. While it doesn't specifically address user access and authentication, it mandates that organizations must implement reasonable security measures to protect personal data. This indirectly emphasizes the importance of robust user authentication and access control to prevent unauthorized data access.
- **HIPAA (Health Insurance Portability and Accountability Act):** HIPAA is a healthcare-specific regulation. It requires healthcare organizations to establish stringent access controls and authentication mechanisms for electronic protected health information (ePHI). HIPAA enforces user authentication through unique user IDs, strong passwords, and access logs to ensure only authorized personnel access patient data.
- **GDPR (General Data Protection Regulation):** GDPR doesn't prescribe specific authentication methods but emphasizes the principle of data protection by design and default. Organizations must implement adequate measures, which often include secure authentication, to safeguard personal data. GDPR also mandates notifying authorities of data breaches promptly, highlighting the need for robust access controls.
- **PCI DSS (Payment Card Industry Data Security Standard):** PCI DSS addresses authentication and access control in the context of payment card data. It requires organizations to implement MFA for access to cardholder data systems. Additionally, PCI DSS mandates role-based access control (RBAC) to limit access based on job functions and needs.
- **NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection):** NERC CIP focuses on the security of critical infrastructure, particularly in the energy sector. It includes requirements for user authentication and access control for systems and devices that impact the reliability of the power grid. NERC CIP emphasizes the use of strong authentication methods and access controls to protect critical assets.
- **NIST Cybersecurity Framework:** The NIST Cybersecurity Framework doesn't focus on a specific regulation but provides guidance on managing and mitigating cybersecurity risk. It promotes the implementation of robust identity and access management (IAM) practices, including continuous monitoring, access reviews, and strong authentication methods, to secure systems and data against modern threats.
- **ISO 27001 (Information Security Management System):** ISO 27001 is a global standard for information security management. It requires organizations to establish an effective access control policy that includes user authentication, authorization, and audit logging. It promotes a risk-based approach to managing user access to protect sensitive information.
- **CIS Controls (Center for Internet Security Critical Security Controls):** The CIS Controls are a set of best practices for cybersecurity. Control 5 specifically addresses the security of user access and identity. It recommends implementing strong authentication, password policies, and regular access reviews to enhance security and reduce the risk of unauthorized access.

These well-known cybersecurity frameworks provide guidelines and requirements to help organizations address the challenges of modern user access and identity authentication, ensuring the protection of sensitive data and critical systems. Organizations must tailor their security practices to meet the specific requirements of the applicable frameworks relevant to their industry and data handling practices.

FOCUSING ON CONTROLS

If we look at one set of cybersecurity controls, in this instance the MITRE ATTACK framework,[4] we see dozens of attack techniques which focus solely on access controls. For example, default accounts, trust relationships, and valid accounts with weak passwords are all examples of areas in which significant effort has been spent identifying potential attack vectors that poor access control can introduce.

From an enterprise perspective, access control attacks take on many different flavors. For instance, protecting against a credential phishing attack, whether targeted or not, is different than managing trust relationships within an AWS cloud infrastructure. As such, understanding exactly which solution sets covers which part of an attack chain is of utmost importance. Understanding how local controls translate between frameworks is equally important.

Another framework that should be considered is the **CISA Zero Trust Maturity Model (ZTMM)**. While not a regulatory standard, it is becoming a widely adopted model by which zero trust can be achieved within the enterprise. Many of the key components of the ZTMM go directly towards addressing the identity-centric controls of the NIST CSF and ISO 27001, making it a useful foundation for future-proofing an identity management strategy.

Many regulators and auditors look to the NIST CSF or ISO 27001 as the main standards by which one measures the maturity of an enterprise's cyber risk management program. By being able to evaluate the various tiers of access control solutions against any or all of these frameworks, an enterprise will be able to quickly discern its security posture for MITRE ATT&CK, NIST CSF, or against industry standards such as PCI DSS.

STEPPING UP THE CYBER INSURANCE GAME

There has been a profound shift recently by the insurance companies to mandate detailed explanations as to the types and levels of controls that are in place as part of acquiring cyber insurance. Gone are the days of yes or no answers to MFA, privileged access, and provisioning controls. Now, insurance companies are demanding to see evidence of alignment with applicable frameworks to ensure they have clarity around the risks they are insuring.

When considering the substantial uptick in malware and ransomware attacks since 2020, it is not surprising that the insurance industry would be taking a serious look at how and when it writes policies to cover cyberattacks. The bellwether $1.4 billion lawsuit filed by Merck[5] when its cyber insurer refused to pay caused a tectonic shift in how insurance companies write such policies.

The trend in cyber insurance has thus shifted from proper control being a means to reduce premiums to one where proper control is a prerequisite to buying any policy. Long gone are the days when any company could check the box and purchase a cyber insurance policy virtually over the phone with no evidence of functioning controls or audit history. Today, the biggest challenge is qualifying for a policy, not the cost.

When evaluating common questions and requests from insurers, having the ability to demonstrate functional, modern controls around user access will make the insurance application process more straightforward. Insurance carriers are experts in probability, so the more an organization can show that they have mitigated the most frequently attacked vector's risk to a satisfactory level, the lower the probability of an attack occurring.

[4] MITRE ATT&CK provides a detailed taxonomy of security attack vectors that helps developers, practitioners, researchers, and vendors design security solutions that address that actual methods that are included in modern breach campaigns by the most capable malicious actors. See ***https://attack.mitre.org/*** *for more information.*
[5] Information on this case can be found at: ***https://www.fiercepharma.com/pharma/merck-entitled-14b-payout-cyberattack-case-after-judge-refutes-insurers-warlike-action-claim.***

Thus, by having the ability to articulate risk reduction through the mitigation of access control attack vectors, carriers can quantify the potential risk using industry-acceptable frameworks, allowing them to develop statistically valid risk models. It is the key component the industry actuaries have been missing when it comes to cyber insurance and is sure to become standardized in the future.

THE BEYOND IDENTITY PLATFORM OVERVIEW

The Beyond Identity solution addresses both the workforce and customer needs in a single platform. With Beyond Identity, an enterprise can provide phishing-resistant multifactor authentication and zero trust capabilities to end users, developers, and customers, all in a single cloud-based platform.

Beyond Identity's platform is FIDO2-certified, providing the highest level of assurance available on the market.[6] The solution provides a password less user experience with the highest level of device trust available, delivering continuous authentication for each user session in the background.

SECURING THE WORKFORCE

The Beyond Identity platform provides a robust password less solution that cryptographically binds identities to authorized devices. Beyond Identity can query over 200 different risk indicators on the trusted device and determine if the device is trustworthy. Through the use of a risk-based policy engine, the organization can customize these risk indicators to determine if the factor is important to them and empower Beyond Identity to make decisions such as step-up authentication for providing an additional level of user identification.

A key benefit of continual device validation is the ability to disconnect sessions or require additional authentication should the risk profile of the device change. This real-time capability empowers organizations to begin adopting zero-trust initiatives in the way they were meant to be implemented.

SECURING THE DEVOPS PIPELINE

As we have seen in the last few years, attackers who can gain access to code repositories can have their illegitimate code bundled up with formal, vendor updates and installed by unsuspecting customers under the guise of product updates. Understanding who is committing code to the repository and having an irrefutable audit trail is a basic step in ensuring application integrity and mitigating supply chain risk.

Beyond Identity maintains all CI/CD user access in a central repository, controlling which devices can create signing keys and being able to revoke keys across the entire enterprise. This capability is accomplished by associating the developers' signing keys with the trusted corporate identity, thus creating a distinct relationship between committed code and enterprise users. Beyond Identity's tight integration with all of the leading code repositories enables these tasks to be performed seamlessly and automatically during the commit process, avoiding error-prone, manual developer processes.

SECURING CUSTOMERS

Modern biometrics technology has emerged as the de facto standard for modern mobile device access. It should be familiar, for example, that common everyday tasks such as reading emails, paying for groceries with your mobile wallet, or performing banking transactions, now involve fingerprint or facial ID access providing the initial authorization on our devices.

[6] *See* ***https://fidoalliance.org/fido2/*** *for more information on FIDO certification.*

However, building that functionality into web applications is not always straightforward. With Beyond Identity's authentication APIs or software development kit (SDK), developers can quickly integrate password less authentication into their applications, which leverages the effortless aspect of biometric based authentication while maintaining a very high level of trust in the credentials.

With the Beyond Identity approach, the private keys of the trusted credential are stored within the Trusted Platform Module (TPM) and are never transferred back to the host application. Not only does this simplify the process of access management, but it also empowers users to leverage their credentials across all of their devices, eliminating the impact of different user experiences across platforms. Finally, enterprises benefit from ensuring that login credentials are never stored eliminating the threat of a large-scale data breach.

DEVELOPING AN ENTERPRISE ACTION PLAN

It is recommended that organizations review their approach to user access and identity management to ensure that they are leveraging all possible new technologies including the types discussed above. Obviously, we endorse and recommend that a review of the Beyond Identity platform be included in such review, given the many benefits offered for securing workforce, DevOps, and customer environments.

Justification for the time spent putting an action plan in place to review and optimize this aspect of the enterprise security ecosystem comes from the benefits suggested above in the areas of improved regulatory coverage, better threat coverage during development, and the potential to make the cyber insurance process a more straightforward and successful engagement.

The resources listed above, including the various frameworks and recommended methodologies such as from CISA will complement and enhance the process of reviewing and improving user access and identity management. As suggested throughout this report, Beyond Identity is well-positioned as a commercial platform for these tasks. TAG Analysts are always available to readers for additional assistance in source selection.

Find out more about **Beyond Identity.**

ABOUT TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science/sustainability.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Dr. Edward Amoroso, John J. Masserini

Publisher: TAG Cyber, a division of TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.