eBook

CALIAN®

Are you making it easy for cyber criminals to attack your business?

www.calian.com
1.877.225.4264 | 770 Palladium Drive, Ottawa, ON, K2V 1C8

CALIAN®

If your policies are inadequate, your processes inefficient, and your controls almost non-existent, then you'll be unable to manage the security of the ever-increasing volume of highly sensitive data. It's a frightening scenario when you consider the growing trend of Bring Your Own Device (BYOD), Internet of Things (IoT), mobility and remote employees—all generating data and all heightening the vulnerability of the company to being breached.

Because of these factors, the need for Identity and Access Management (IAM) has exploded. Consider the 2018 Verizon Data Breach Investigations Report finding that hacking (93% of breaches) was the most common threat action reported as one of the causes of data breaches, and that within the hacking category 81% of the attacks used stolen credentials. For instance, the massive eBay breach in May 2014 compromised 145 million users—all because hackers gained access into the company network for 229 days using the credentials of three corporate employees.

What also adds pressure and reinforces the need for identity security and governance measures are compliance regulations such as the new European Union (EU) GDPR (General Data Protection Regulation) and Canada's PIPEDA (Personal Information Protection and Electronic Documents Act). The foundation of IAM principles are Authentication and Authorization. With these programs and technical controls in place, you can prevent attacks like the eBay breach mentioned above.

It's critical, therefore, that you implement a sound IAM approach to manage the complexity and volume of data and to bolster your company's ability to protect intellectual property and individual privacy from both internal and external threats. IAM protects your company through password-

CALIAN®

Fallout when you fail to manage identity and access

In today's environment ubiquitous access to information and data is expected. So, when you have many employees, contractors, consultants, and others, coming and going without their access to data being revoked, then the vulnerability of your company to data loss or a breach greatly increases. When you don't know who has access to your network, when you don't know what they can access, and when you don't even know who they are, your company is teetering on the brink of non-compliance and is exposing it to the high risk of a cyber attack that can potentially put you out of business—the repercussions of cleaning up after a breach can be considerable.

The ability to manage and control access to your ever-increasing volume of highly sensitive data is the primary action that you can take to prevent a costly attack. Breaches don't occur because cyber criminals are attempting to penetrate your super secure firewalls and perimeter protection, they occur primarily because you've made it ridiculously easy for them to rob your employees of their credentials. Then they can walk right in—even though you have

Deny unauthorized users access

One of the most effective ways to close the door to cyber criminals is to follow the basics of IAM, which is a system that secures, stores, and manages user identities and access privileges. First, it protects your company by ensuring that users are who they say they are and, second, grants access only to those who have permission to access application resources.

The most common IAM practices are single sign-on (SSO), multi-factor authentication (MFA), and privileged access management—you can deploy these on-premise or in the cloud. Meanwhile, unauthorized users do not have access to sensitive corporate data which helps to safeguard the privacy and security of the organization and the individual.

www.calian.com
1.877.225.4264 | 770 Palladium Drive, Ottawa, ON, K2V 1C8

CALIAN®

Boost security

Improve data security

When you implement an identity management system it forces your company to review and clarify user identity and access policies. Traditional approaches to authorization tend to be task based. As employees and contractors change projects and move throughout the organization, this approach proves to be difficult to manage and often leaves users with authorization to access material that they no longer have a need for. A shift to "Role-Based Access Control" helps to simplify access management and ultimately improves your security posture.

One of the single most effective measures organizations can take to reduce unauthorized access is to implement MFA. The simple act of adding a swipe card, 1-time password, or external confirmation on your mobile device makes it virtually impossible for a hacker to take advantage of stolen credentials.

With identities and access managed, there is greater control of user access. This results in reducing the risks associated with unmanaged access such as internal and external breaches. When you reduce these risks through an identity management system, you enhance security.

With a secure, centralized IAM approach to managing user identities and access permissions, your employees are more productive by using SSO technology. This reduces how many interactions they have with security systems and increases the possibility of successfully accessing the resources they need to do their job.

Track behavior

In a recent ESG research survey, security professionals were asked to identify their weakest area of security monitoring. More than one-quarter, 28%, pointed to "user behavior activity monitoring/visibility"—the highest percentage of all categories.

This brings us to one of the most important benefits of identity access management technology: the ability to track your user's behavior throughout the system. Seeing where your users are gives you more insight into what applications and data they are accessing and alerts you to any sudden changes in behavior.

Prevent breaches and reduce IT costs

Implementing an IAM system reduces your IT costs. Most organizations increase their security budgets to protect the business from the threat of cyber attacks. While investing most of their security budget in network perimeter protections, organizations are spending millions while cyber criminals continue regardless.

With the average IAM spend about 5% of the security budget, and with compromised identity and access the cause of over 80% of breaches, it makes sense to prevent these breaches with a simple IAM solution: multi-factor authentication. This solution reduces the number of breaches and, therefore, decreases IT costs. In other words, reduce the money spent on network perimeter protections into fully implementing IAM technology.

Furthermore, organizations must pay special attention to the credentials with the most access: privileged accounts. These administrator accounts are highly coveted and targeted by attackers due to their ability to access and modify most systems. Privileged Access Management (PAM) is the combination of policies, procedures and technology around the management and control of these special accounts. Implementing a PAM solution enables you to reduce the risk of breaches due to the hijacking of these special credentials.

Avoid non-compliance

With IAM, you'll no longer be teetering on the brink of non compliance which can cost millions of dollars in regulatory fines. With systems such as IAM and PAM to help secure, manage, and control access to critical business assets, you'll be in full compliance; for instance, by automating user administration processes; by providing centralized administration for assigning and controlling user access rights; by adjusting access rights when an employee's job function changes; and by revoking user access upon termination—to name just a few IAM solutions that ensure your business is fully

CALIAN®

Ensure your data remains secure

The penalties for failing to protect the personal information in your care include customer churn, class actions, damage to brand, and claims from customers, financial institutions, shareholders, and others.

Furthermore, global data breach notification requirements present critical issues for your company: the current environment is increasingly challenging—escalating global security threats, expanding vulnerabilities, and increasing data breach notification requirements. Then, of course, your company is facing prospective new legislation such as GDPR, as well as current legislation such as PIPEDA, which now includes mandatory reporting of breaches of security safeguards.

IAM and PAM systems should be a critical part of your organization's security framework. If they aren't, then your company is a lucrative target for cyber criminals.