4 REASONS WHY IDENTITY AND ACCESS MANAGEMENT SHOULD BE THE CORE OF YOUR SECURITY PROGRAM

IDENTITY AUTOMATION

TABLE OF CONTENTS

As the business world becomes more reliant on technology, your organization's assets—personal data, intellectual property, technology environments, and infrastructure—face a complex and ever-evolving threat landscape. Protecting these critical assets must become a higher priority for IT departments; however, approaching today's hazards with a dated, perimeter-focused approach to security puts a company and its customers at risk.

Organizations are operating in perimeterless, global business environment. Employees no longer solely work in office buildings, behind firewalls and other traditional security technologies. Even when employees are in the office, most are still working from outside a secured perimeter, thanks to the proliferation of mobile devices and more businesses turning to the cloud. Furthermore, workers have more device flexibility than ever as businesses embrace "bring your own device" (BYOD) policies.

These shifts in the workplace have necessitated a change in the way we must view the threat landscape. With end users having so much access from so many different endpoints, threat actors know that the easiest way to steal information isn't to fight through perimeter controls—it's to compromise a user account and walk in right through the front door.

PEOPLE ARE INCREASINGLY WORKING IN A PERIMETERLESS, GLOBAL BUSINESS ENVIRONMENT. THEY NO LONGER SOLELY WORK IN OFFICE BUILDINGS, BEHIND FIREWALLS AND OTHER TRADITIONAL SECURITY TECHNOLOGIES.

This is exactly why you can no longer look at identity and access management (IAM) as being simply a tool or utility that helps your IT staff be more efficient in creating user accounts. Yes, IAM solutions enable IT staff and employees to be more productive, but they also provide a solid security foundation by addressing authentication and rights management. IAM must be the core of *your security program* if the goal is to effectively secure your company's data and systems.

Changing the mindset of a particular organization and its decision-makers isn't always easy. If you're struggling to achieve this shift in your organization, the following four reasons can help you build a persuasive case to make IAM the core of your security program.

REASON ONE: INTRUDERS ARE ALREADY IN YOUR SYSTEMS

It is common for IT to think in terms of spending money on anti-malware solutions, firewalls, and other perimeter security technologies as a way to keep out hackers. However, this way of thinking does not protect a network against today's threat landscape.

While perimeter security is important for protecting data inside the confines of your network, an evolving threat landscape has made it necessary for IT professionals to change their mindset and assume that the attacker is already inside the network. This means putting greater investment and resources toward minimizing what these intruders can access and the damage they can do.

HOW INTRUDERS GET IN

Intruders still get into a network through a system weakness; it's just that the weakness they are looking for has changed. Most likely, an attacker has stolen or acquired someone's legitimate user name and password through a spear-phishing attack or some other method of social engineering. From there, the attacker moves from system to system until he or she finds high-value information, such as customer data, financial information, and intellectual property.

Steps must be taken to limit an intruder's access and movement from one system to the next, but how? By putting an IAM solution in place.

HOW TO FIGHT BACK

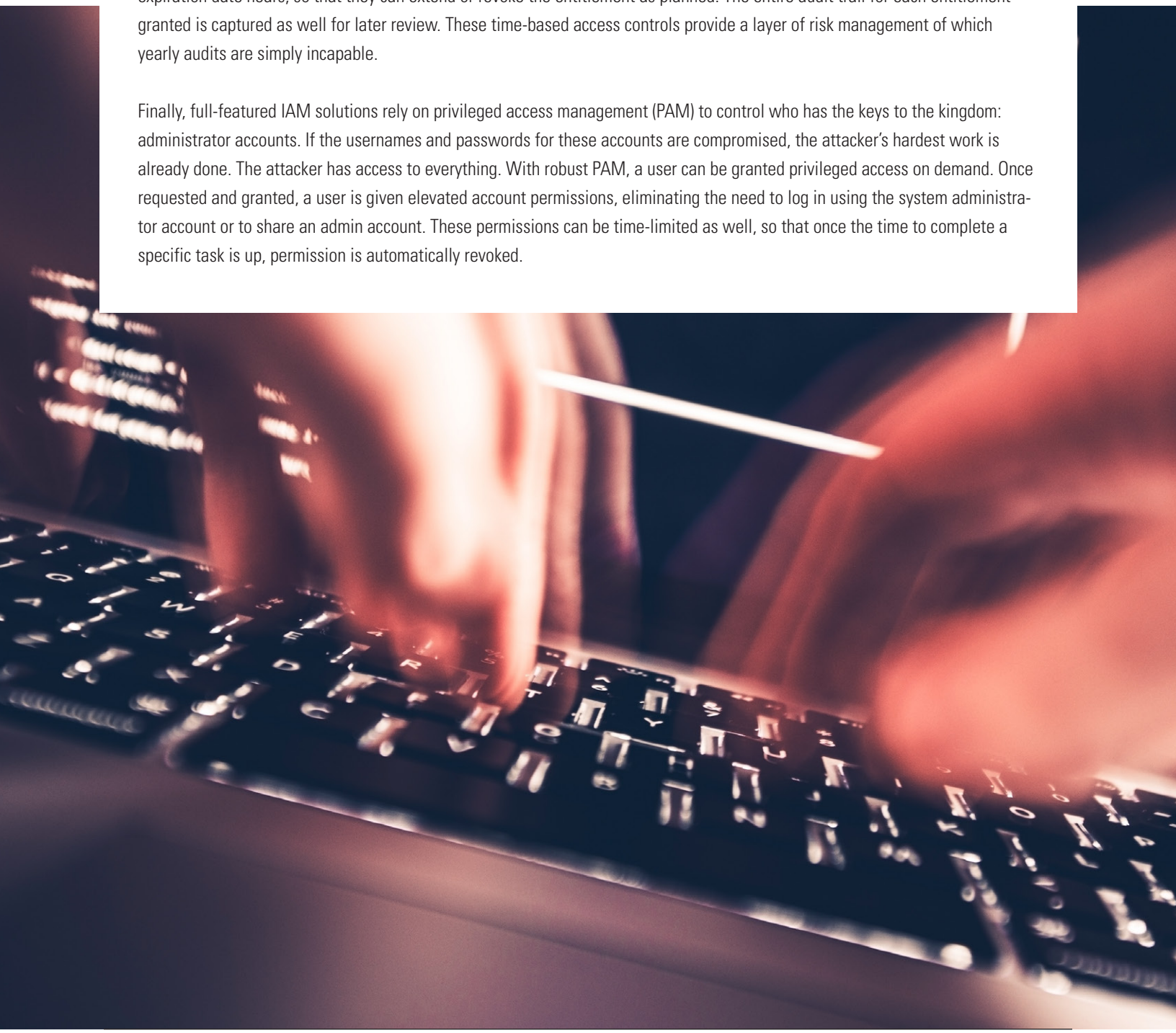
An IAM solution locks down access controls and establishes least-privilege access, so that employees are only given access to the systems and information needed to effectively do their jobs and only for the necessary duration. This way, if a legitimate user account is compromised, the attacker only has access to limited data.

Modern IAM solutions also provide businesses with additional tools to help control user access, especially should a user's credentials become compromised. One such control is automated deprovisioning of accounts. All too often, when it's time to close the books on an engagement, an account remains active until someone in IT manually removes the account from the directory services and revokes the user's access to all applications. When left to a human, this is a time-consuming process that is easily overlooked or even forgotten altogether. When this happens, your company is put at great risk, as these orphaned accounts still maintain access to systems and data, making them extremely attractive to attackers.

Automated deprovisioning eliminates this risk. With a single, automated workflow, all user accounts tied to a person can be deactivated as soon as he or she leaves the organization.

Furthermore, a proper IAM solution has the ability to provide just-in-time access and set time limits on entitlements for users who only need one-time or short-term elevated privileges. For longer-term entitlements, system owners are notified when the expiration date nears, so that they can extend or revoke the entitlement as planned. The entire audit trail for each entitlement granted is captured as well for later review. These time-based access controls provide a layer of risk management of which yearly audits are simply incapable.

Finally, full-featured IAM solutions rely on privileged access management (PAM) to control who has the keys to the kingdom: administrator accounts. If the usernames and passwords for these accounts are compromised, the attacker's hardest work is already done. The attacker has access to everything. With robust PAM, a user can be granted privileged access on demand. Once requested and granted, a user is given elevated account permissions, eliminating the need to log in using the system administrator account or to share an admin account. These permissions can be time-limited as well, so that once the time to complete a specific task is up, permission is automatically revoked.



REASON TWO: MORE USERS, MORE DEVICES, MORE SYSTEMS, AND LESS IT CONTROL

"We live in a connected world." The biggest cliché of our era provides businesses with the most opportunity for productivity, while simultaneously giving IT the most headaches. Research shows that 74 percent of all businesses are adopting BYOD policies, giving workers the ability to check email, log in to cloud systems, and even access stored network files from anywhere with an access point or a cell signal.[1]

THE RISE OF THE CONTINGENT WORKFORCE

As the need for employees with specialized skills continues to grow, organizations rely more on contractors to take on specific tasks or provide help during the busiest times. Using contracted help enables businesses to quickly fill in workforce gaps at a lower cost, while minimizing the need to lay off full-time equivalent workers. Companies also forge outside partnerships to advance and enhance current products and technologies by connecting systems and data.

74 PERCENT OF ALL BUSINESSES ARE ADOPTING BYOD POLICIES.

AN ANYWHERE, EVERYWHERE WORKPLACE

Even full-time employees have changed the way they work, as many are now electing to work from home. In fact, the number of regular work-at-home employees has grown 103 percent since 2005.[2] Not only are employees being given more flexibility in where they can work, but many also have greater work computer options. Now, instead of IT building out a laptop or desktop from a single image, many employees are simply given a stipend to buy their own workstation. Moreover, notepads have largely been replaced by tablets and smartphones that send information directly to connected systems.

Many businesses are also turning to cloud services to handle everything from data storage to applications and even infrastructure to help save money and put resources into the hands of experienced professionals.

And, while these trends help businesses save money, improve efficiency, and make workers happier, they present organizations with enormous security risks. Because more systems and hardware have moved outside your network, this also puts data outside of IT and perimeter security controls. In some companies, the only control that IT has over an employee's computer is the remote control software that IT uses when users need help.

Unfortunately, businesses and IT departments have no choice but to embrace these trends, so it is more important than ever to have a solution in place that is able to give users access to the data and systems they need, in a manner that is secure enough to keep out attackers. That is why IAM is so crucial.

TAKING BACK CONTROL

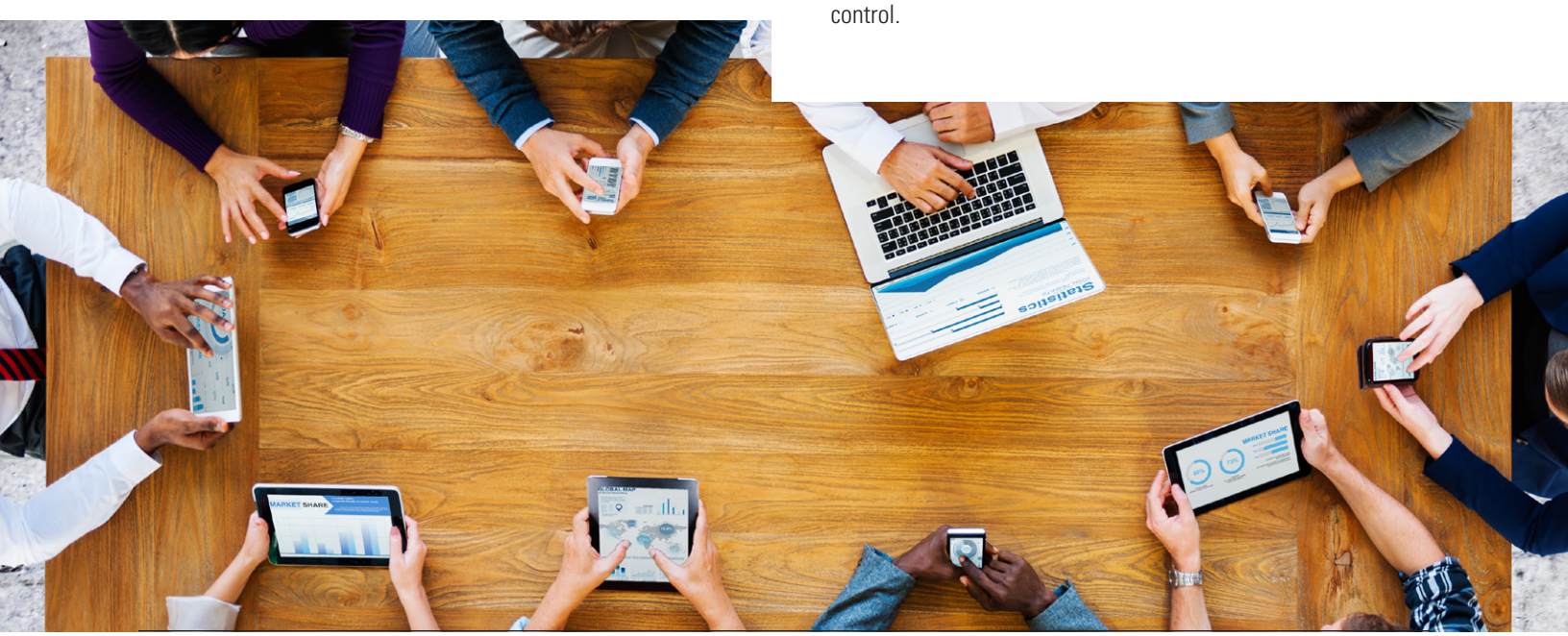
The right IAM solution provides secure, full identity lifecycle management. Not only will the solution take care of the provisioning and deprovisioning of user accounts, but it will also manage resource access for all of an organization's users. By providing a database of roles determined by location, manager, department, or other variables, IT administrators can easily assign users the proper entitlements. Some of these solutions even make this process as easy as dragging and dropping a user into a group. So, from day one of an individual's employment, only the resources to which the user has privileges can be accessed and nothing more. As those needs change, the IAM solution's full lifecycle management capabilities help by adding or removing necessary entitlements.

With users having access to so many devices and systems, password management becomes a challenge as well. IAM solutions address this challenge by enabling strong authentication across the different systems to which a user has access. This goes beyond a simple, strong-password policy by adding extra layers of security through adaptive or risk-based authentication. For example, user credentials may be used from an unusual location or at a time that falls outside of the employee's normal hours or working patterns. This is sometimes referred to as "contextual authentication" because it looks at not only the username and password, but the context surrounding the log-in.

There is also a need to control the access of contractors, partners, and contingent workers. Because these people don't work directly for the company, they are not typically entered into the authoritative employee system by HR. As a result, IT has to manually create accounts in the systems these users need to access, provide necessary entitlements, and remove people once access is no longer needed.

As a manual process, organizations not only spend a great deal of time managing these accounts, but they are more apt to make a mistake if there is a lack of communication. User accounts may be given greater access than they actually need, or users may accumulate access over time. There is also the chance that these accounts won't be deprovisioned when they are no longer needed, leaving unattended accounts available for a disgruntled employee or even an outside threat to leverage in an attack against you.

Modern IAM solutions meet these challenges by delegating to non-IT employees within the company, such as hiring managers, to manage the account lifecycles of outside individuals whom they sponsor. Sponsorship gives a hiring manager more control over a user account and the ability to better communicate any access or system needs associated with that particular user. The access granted to these sponsored individuals falls within preset security and privacy policies and carries an expiration date that can be extended at the request of the sponsor. So, while IT does not have to spend time on account set-up and removal for these users, the IAM solution still enables IT to maintain control.



REASON THREE: ROBUST IAM SECURITY DELIVERS COMPLIANCE

Controlling user accounts, especially those with privileged access, has always been an important part of regulatory compliance. Take the Payment Card Industry Data Security Standard (PCI-DSS), for example. One of the goals of PCI compliance is to implement strong access control measures that require a business to:

Restrict access to cardholder (sensitive) data to a need-to-know basis

Assign a unique ID to each person with computer access

Track and monitor all access to network resources and cardholder data

Substitute just about any other compliance standard, be it HIPAA, SOX, or the EU Data Protection Directive, and somewhere in the language, it will mention privileged access, unique user IDs, and the monitoring and logging of access to sensitive data.

Years ago, IAM systems were sold as a way to help companies manage compliance audits. Over time, however, this mindset has changed, as analysts, vendors, and other industry influencers have pushed the point that even if companies are meeting all compliance check boxes, this doesn't mean their digital environments are actually secure. User accounts are still being compromised, and attackers are still able to move laterally throughout corporate digital ecosystems looking for sensitive data—the very data that being compliant is supposed to protect.

Modern IAM solutions are designed with a security-first mindset that addresses these concerns with features, such as continuous access certification and PAM:

CONTINUOUS ACCESS CERTIFICATION

Enables IT to set time limits on accounts, so that access is reviewed in an ongoing process, rather than only once a year. To be compliant, many regulatory standards require a company to audit access on an annual basis. Yet, certifying access only once a year simply won't cut it for companies that are taking security seriously because this leaves room for gaps. For example, a person could transfer to a different department with different responsibilities months before an audit comes around. Not to mention that many annual audits are simply rubber-stamped due to the volume of accounts.

PRIVILEGED ACCESS MANAGEMENT

Enables IT to grant automatically expiring time-based administrative access, shared access to an administrative account, and more. Compliance regulations often require the restriction of administrative accounts or at least a record of who has access to what. However, security-focused organizations recognize the true risk that poorly managed administrative accounts present and opt for IAM solutions that address compliance by providing greater security.

Companies focused on achieving compliance, simply aren't doing enough to address today's security threats. Modern IAM solutions, with features like continuous access certification and PAM, provide an additional layer of security that enable you to lock down your organization's most valuable assets, keeping your network resources, your intellectual property, and your customers' data safe.

REASON FOUR: THE COST OF A BREACH CAN CRIPPLE YOUR BUSINESS.

Research shows that 43 percent of data loss comes from insider threats, both intentional and accidental.[3] To show just how serious this is, more than 666,000 internal security breaches occurred in 2014, which averages out to 2,560 incidents per day.[4] These are the very threats that an IAM solution is put in place to minimize the risk of should a breach occur.

Part of this cost comes from penalties that a business has to pay for non-compliance. Take PCI-DSS, for example. Potential charges range from $5,000 to $100,000 a month, depending on the payment card and the type of business.[6]

Then there is the loss of customer trust. The IBM/Ponemon study suggests that businesses that suffer from a data breach can expect customer churn rates to increase by 2.9 percent following a breach.

There are also detection and escalation costs that average out to $417,700, notification costs that usually total in excess of $500,000, and remediation costs that can run up a bill of about $1.6 million.

Of course, one would also have to consider the dollars lost if intellectual property is stolen. All of the research and development dollars that a company has spent would be in vain.

When these costs are totaled up, there is a chance that the business will fail as a result. For a small business, the chance is significantly higher, with 60 percent of small businesses closing their doors within six months of a data breach.[7]

RESEARCH SHOWS THAT 43 PERCENT OF DATA LOSS COMES FROM INSIDER THREATS, BOTH INTENTIONAL AND ACCIDENTAL.[3]

Finally, a data breach can cost a person his or her job. Target's CIO Beth Jacob resigned after the company's breach, with CEO Gregg Steinhafel leaving shortly after her. Amy Pascal, the head of Sony Pictures, also submitted her resignation after Sony was hacked. The 2012 breach of Utah's Department of Technology Services cost Executive Director Stephen Fletcher his job after an error at the password-authentication level was found to be the cause of 280,000 Social Security numbers being exposed. And who could forget the U.S. Office of Personnel Management (OPM) breach that cost Director Katherine Archuleta her job in 2015 after being warned that the OPM's systems were vulnerable?[8]

To see just how devastating a data breach can be to a business, take a look at the annual Cost of a Data Breach Study conducted by IBM and the Ponemon Institute:[5]

The average total cost of a breach is $4 million, which is up 29 percent since 2013.

The average cost per record breached is $158.

Two of the highest averages came from the healthcare industry, at $355 per record and retail, at $172 per record.

NOW IS THE TIME TO PUT IAM AT THE CORE OF YOUR SECURITY PROGRAM

Your legacy IAM solution was built to address the business needs of yesterday, helping your IT staff to more efficiently create user accounts and manage compliance audits. However, it can't keep up with challenges you are facing now—a growing number of users, devices, systems—all under less IT control.

The threat landscape has changed. Attackers are targeting your users because they know if they can gain control of their accounts, they can eventually find confidential data. This reason alone is exactly why your organization needs to put as much effort into managing and controlling user accounts and their entitlements as you do with firewalls and intrusion prevention technologies.

If your organization intends to go beyond compliance and into defense, IAM must be at the core of your security program. This means implementing a solution that goes well-beyond the utility-like functionality of a legacy IAM system by addressing authentication and rights management and managing the full lifecycle of all users, even those that are not traditional, full-time employees.

Now is the time to implement a full-featured IAM solution that was purpose-built to address your business's evolving security needs both today and tomorrow.

SOURCES

1. Maddox, T. ZDNet. (January 2015) Research: 74 percent using or adopting BYOD. http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/

2.Grevstad, E. PC Magazine. (December 2015) 2.5% of U.S. Employees Work from Home. http://www.pcmag.com/article2/0,2817,2496850,00.asp

3. Seals, T. Infosecurity. (September 2015) Insider Threats Responsible for 43% of Data Breaches. http://www.infosecurity-magazine.com/news/insider-threats-reponsible-for-43/

4. InformationWeek Dark Reading. (February 2014) Over 2,560 Internal Security Breaches Occurred In US Businesses Every Day. http://www.darkreading.com/attacks-breaches/over-2560-internal-security-breaches-occurred-in-us-businesses-every-day/d/d-id/1141325

5. IBM and Ponemon Institute. (2016) Cost of Data Breach Study. http://www-03.ibm.com/security/data-breach/

6. Fritsche, D. and Sasne, B. Hytrust. (September 2014) Whitepaper: The Costs of Failing a PCI-DSS Audit. https://www.hytrust.com/wp-content/uploads/2015/08/HyTrust_Cost_of_Failed_Audit.pdf

7. PRO OnCall Technologies. (November 2014) 3 Companies that Went Out of Business Due to a Security Breach. https://prooncall.com/3-companies-went-business-due-security-breach/

8. InformationWeek. (June 2015) 14 Security Fails That Cost Executives Their Jobs. http://www.informationweek.com/government/cybersecurity/14-security-fails-that-cost-executives-their-jobs/d/d-id/1321279?image_number=1

Contact Sales: sales@identityautomation.com
Contact Support: support@identityautomation.com
Other information: info@identityautomation.com

Toll Free: 877-221-8401
Voice: 281-220-0021

Corporate Headquarters:
8833 N. Sam Houston Pkwy. W.
Houston, TX 77064