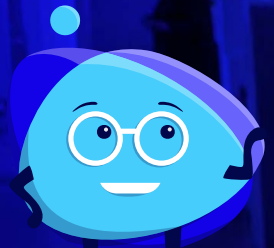
iManage

Making knowledge work



SECURITY CULTURE BEST PRACTICES

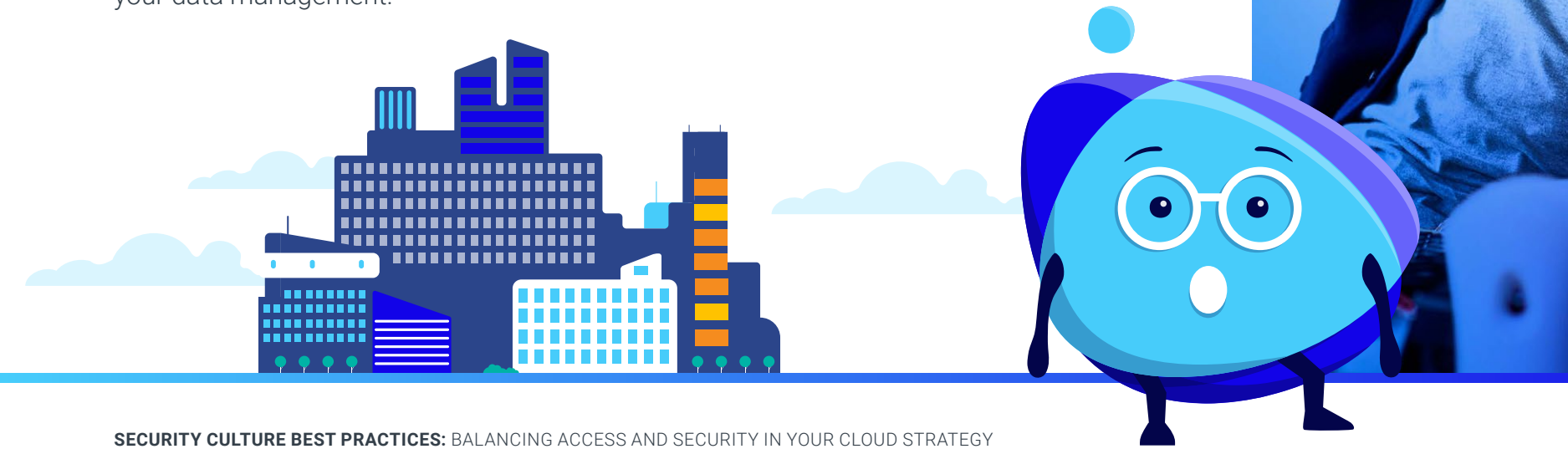
Balancing access and security in your cloud strategy

INTRODUCTION

We live and work in an ever-evolving security threat landscape that impacts how we do business, how we interact with clients, suppliers, and third parties, and how we plan for investments in future growth.

According to the 2022 Thales Data Threat Report only 56% of IT leaders were very confident or had complete knowledge of where their data was being stored, down from 64% the previous year, and only a quarter (25%) stated they were able to classify all their data. Moving to the cloud presents a good opportunity to get your house in order and centralize your data management.

As your organization looks to embark on a cloud strategy that moves your valuable data from the restraints of an on-premises setup to the cloud, it is important to consider that people are the weakest link in any security program. The threat to your data is significant, because negligent employees and credential thieves are the root cause of most insider incidents.



"In a highly digitized and hybrid-friendly workplace, implementing a culture of security calls for cloud-based tools and a knowledge work platform that have advanced security technologies embedded within them. But in the end, how well (or ill) an organization's knowledge assets are protected is wholly dependent on whether these tools are supported, used, and embraced by all employees."

SHAWN MISQUITTA
Vice President of Product Management
iManage

The 2022 Cost of Insider Threats Global Report conducted by the Ponemon Institute revealed that the total average annual cost of insider incidents over a 12-month period was $15.4m. Fifty-seven percent of respondents say the insider incidents involved employee negligence, and 51 percent say a malicious outsider stole data by compromising insider credentials or accounts.

A strong security culture is therefore a must-have within your organization. The importance of having people on board with what you're trying to achieve, as well as prioritizing the processes and technologies that support the adoption of security best practices, cannot be over-emphasized.

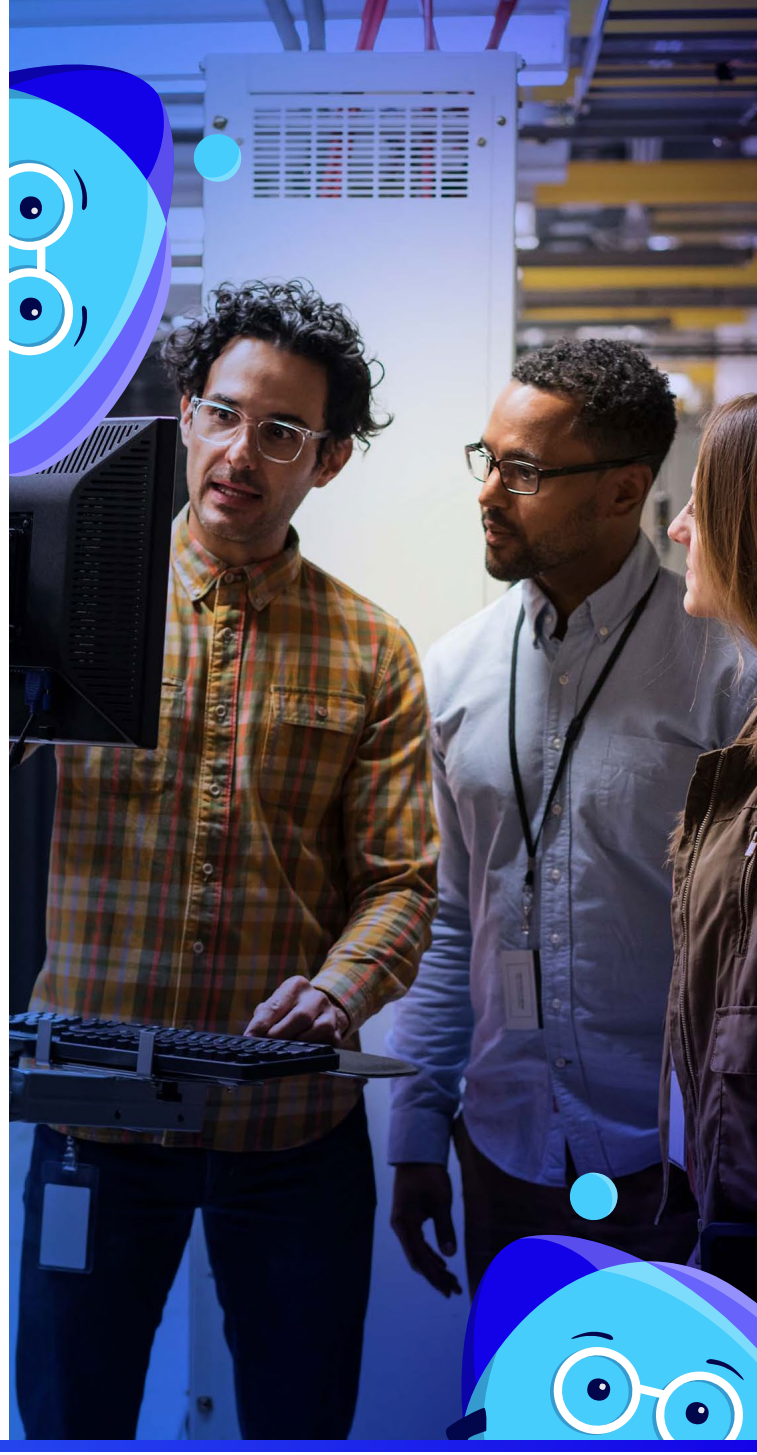
But a culture of security doesn't evolve on its own. It needs to be created, developed, and distributed to achieve 100 percent buy-in, with the role of firm leadership being essential to success. And, although security as a culture manifests differently for each individual according to their role, **the need to take security measures seriously penetrates all layers of an organization, affecting all people at all times.**

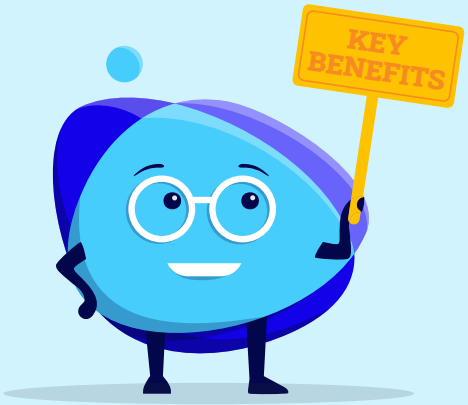
TAKING A UNIFIED APPROACH TO SECURITY

At the highest level, technical and operational teams want the organization to be successful, to empower people to work as effectively as possible, and to do so unhindered by outages or by complex or intrusive security measures. But too often, organizational security is seen only through the lens of the IT team.

While the technology team usually puts security measures in place, oversees vendors, and takes action to mitigate any issues, everyone in an organization is responsible for behaving in a security-conscious manner on the job. This might mean maintaining client confidentiality, following ethical guidelines, or simply appreciating the risks of following a poor approach to security enough to take the appropriate actions in their day-to-day activities.

Business decision makers and leaders at all levels are key to communicating the message that everyone makes choices about security every day — sometimes through formal processes such as financial planning and workload management, sometimes via one-off decisions about when and how to share information with others. In a secure organization, all of these teams must come together to create a unified approach through which a culture of security can emerge.





Developing and sustaining an effective security culture is an essential component of a protective security regime, according to the UK's Centre for the Protection of National Security. It defines the key benefits of an effective security culture as including:

- A workforce that are more likely to be engaged with, and take responsibility for, security issues
- Increased compliance with protective security measures
- Reduced risk of insider incidents
- Awareness of the most relevant security threats
- Employees more likely to think and act in a security-conscious manner

Why security culture matters

Breaches happen for many reasons, including gaps in security infrastructure, willful or accidental actions by individuals, and incursions by external bad actors. To protect itself from a breach, an organization must behave like an organism, with all parts functioning in synergy.

Giving increased relevance to fostering a culture of security, "The Great Resignation" has workers moving between employers or leaving the sector altogether. When employee experience isn't well-documented or easily discovered in the records people leave behind, that experience leaves with them. In an organization with poorly regulated data storage systems, a worker may even be able to take confidential data or files with them. While robust systems and clear processes should prevent this kind of theft, establishing a culture of security may make workers less inclined to take the risk.

A security culture both **embraces** the need for strong security and **enables** the actions required to achieve and maintain it. Every person within the organization must buy into this and act accordingly, day in, day out. A security culture normalizes secure behavior, so that once the seeds are planted the behavior becomes second nature.

Defining the leadership role

The most effective way to secure change adoption throughout the organization is for the senior leadership team to embrace it. They must be well-informed about how an organization's document management systems and data repositories are configured, the security aspects around this infrastructure and the protection provided, and what is required of workers to maintain that protection. They also need to understand, promote, and demonstrate the key behavioral characteristics that a security culture requires.

First, leadership must embed the importance of security in everything that each employee does in the general course of their work. This matters regardless of whether they are using technology for a particular work task, and regardless of their specific role or position in the organizational hierarchy. A culture of security must be embraced by all.

Second, keep security simple, engaging, and transparent. Security that is easy to implement and makes the benefits to the organization tangible helps employees want to be part of the culture of security and is more likely to be successful.

Finally, communicate often, clearly, and in ways that reference the ease of use and the benefits of compliance both to individuals and to the organization as a whole. Understand that not everyone has the same priorities or responds to the same language and craft your message accordingly.

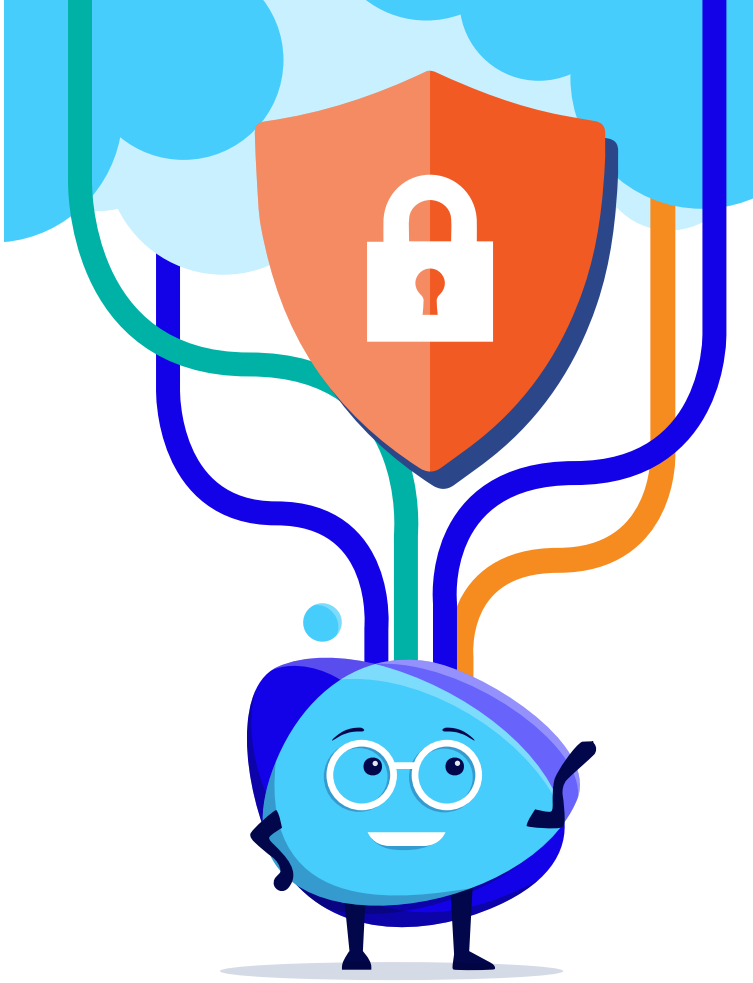
Areas of synergy between decision makers

Commercial decision makers and technical decision makers view the need to protect their organization's systems and data differently, but research commissioned by iManage shows three key areas of synergy. In addition to the leader's role in defining security culture and processes, discussed above, we recognize two more:

- Protecting business-critical data and customer information in the cloud
- Democratizing security knowledge and responsibilities

Creating and maintaining a security culture requires **both.**

Protecting business-critical data and customer information in the cloud means democratizing security knowledge and responsibilities. We de-silo security to enable cross-business knowledge sharing.



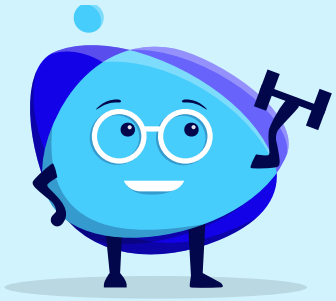
In a **WEAK** security culture

A lack of understanding of the need for strong security across the organization creates an environment where threats may not be recognized or contained.

Work is managed without benefit of a unified approach that classifies documents and emails according to accepted policies and permissions.

Unauthorized cloud-based tools and apps are used throughout the organization to store and transfer files without regard to defined security best practice.

Data is moved between computers or locations using unsecured devices or means.



In a **STRONG** security culture

Secure, authorized tools are used to create and edit new documents because they are the easiest method and using them is second nature.

Confidential materials are saved and stored in a central location, following company best practices that are clear, understood by all, and employ a classification-based approach to prevent data loss.

Data security concerns can be reported quickly and easily, following an established and documented process with an improvement roadmap that everyone can feed back on.

Established two-way communication acknowledges input from employees and keeps them informed of actions taken to maintain a strong security culture.

Employees can see the difference their actions make towards the security of company and client data.

It is important to note in this context that a strong security culture is not an end in itself. Coupled with strong security measures, a security culture enables an organization to meet current and emerging needs for flexible, scalable, and powerful security technology. This continually evolving protection paradigm amplifies return on investment through regular workload activities like increased collaboration, greater productivity, enhanced efficiency, and faster speed to innovation.

Adopting a culture of security not only protects current workloads, it helps the organization build its knowledge base into a strong foundation as time goes on, keeping its collective organizational knowledge assets stored securely and ensuring they can be accessed readily.

BALANCING SECURITY AND ACCESSIBILITY

Striking the right balance between maintaining best-in-class security and giving people access to the documents and materials they need to do their job presents an ongoing challenge.

First, hastening an already strong digital transformation trend, COVID-19 forced organizations to embrace remote working, even when their technology or security measures were not optimally configured to do so. Many organizations moved to the cloud quickly to minimize downtime and provide all-important remote access with the necessary security.

Those wanting to maintain their systems in-house tend to fare worse than those moving to cloud, due to a talent shortage in technical expertise and the difficulty and expense of supporting legacy systems. The 2021 Mainframe Modernization Business Barometer Report found that 89 percent of organizations are concerned about having access to the right IT talent to maintain and manage their legacy systems. That statistic is not likely to improve.

In parallel with these burdens, external threats have grown in number and scope. Ransomware attacks, for example, are no longer always focused on leading companies. The appearance of Ransomware as a Service (RaaS) has allowed threat actors with little to no technical expertise to stage attacks on ever-smaller organizations. This and other forms of malicious activity are a continual source of concern for organizations of every size and stripe.

What are some ways that organizations find the balance between security and accessibility? Well, for a start, they can:

- Choose vendors that are appropriately certified to provide the needed security assurances.
- Choose vendors whose systems and services are easy for people to adopt and use.

These are equal in importance because — while the reliability of the security you implement is crucial — security measures cannot hinder the users. A security system that requires workers to jump through multiple hoops when creating, accessing, saving, or sharing an email or document is likely to be bypassed by the user. This can impede work unnecessarily, curb productivity, and create an attitude of resentment toward the tools that should be helping people.

Balance is achieved between accessibility and security when seamless and easy access to the end user is incorporated with the maximum degree of protection.

How iManage helps organizations achieve the balance

How can organizations ensure that they hit the right balance between great security and optimized, trouble free, seamless accessibility to their data, documents, collaboration tools, and knowledge?

> "In the long-term, it's more cost-effective to be in the cloud versus maintaining our own data center. And the reality is that security in the cloud is more than our security can ever be in our on-premises environment. The cost of ensuring that level of security [on-premises] is simply prohibitive."

SIMON BROWN
IT Partner
MHA Tait Walker

GET THE CASE STUDY ›

iManage solutions, built with security at their core, represent a straightforward answer to providing a multifaceted, employee-centric, and customer-centric platform that solves mission critical short-term needs – but also sets companies up to compete successfully among attractive new entrants and organizations who appear more digitally mature.

> iManage is investing in security that we can't afford."

DAVID MELCZER
Director of IT
Greenbaum, Rowe, Smith & Davis

GET THE CASE STUDY ›

And thanks to our strategic partnership with Microsoft, we have a seamless integration with Microsoft Azure and the 365 platform, including Microsoft Teams. This enables us to extend our security protection across not just our own applications but also those required for collaborative working, document sharing, email and more.

This means that from the initial discussion on requirements to the delivery and support of a customer solution, iManage embeds security best practices across its platform for a comprehensive yet unobtrusive approach. With the whole document lifecycle secured, being safe isn't a barrier to being productive.

> When you know that you can have your data, your workloads in the cloud — our two most important are Exchange and our documents — I don't have to worry. I can sleep. I trust that Microsoft and iManage are ensuring that our security is strong and they're watching 24/7. They're both large companies, they have reputations to protect, and they can bring more to the table than we ever could as a midsized firm"

PATRICIA MANSUY
Interim CIO
Cole Schotz

GET THE CASE STUDY ›

Taking advantage of Zero Trust architecture

A key advantage of moving your document management to iManage in the Cloud is to take advantage of Zero Trust architecture. Zero Trust is exactly as it sounds: security based on the need to verify every interaction – and nothing that isn't verified can be trusted. An individual's ability to access specific data, move around within the system, and view or modify data with differing permission levels relies on the ability of Zero Trust security checkpoints to validate that the specific user and the device they are using have the appropriate credentials to proceed.

The Zero Trust model is widely recognized as an effective approach to prevent data breaches and mitigate the risk of attacks by threat actors. Your sensitive data is protected anytime, anywhere.

Importantly, Zero Trust is a journey. What was considered secured yesterday may not be secure today. To be effective, the model must always evolve and adapt so that it can protect your sensitive data anytime, anywhere. By assuming no user can be trusted by default, our Zero Trust approach and our integration with Microsoft Azure work to ensure state-of-the art security for our customers that is continually updated to meet the changing threat landscape in modern office and hybrid environments.

But a security system that requests verification every time a document is acted upon is too intrusive for a modern work environment. Whether text-based, audio, or video-based, documents or emails, people must be able to seamlessly access materials from across the organization as they go about their day-to-day work. As the work requires, they must be able to edit, copy, and share files with relevant parties whether internal to the organization or outside it.

In the course of their work people might easily touch hundreds of documents and other files each day. Technologies underpinning our Zero Trust approach allow us to monitor how individual files and data are used, who is accessing them, how they are edited, whether and where they are copied or moved to, when they are deleted, and so on. All of this helps build a picture not only of the use and movement of data and files, but also of how individuals are behaving. Patterns can be identified and measures taken to minimize the risk of data loss.

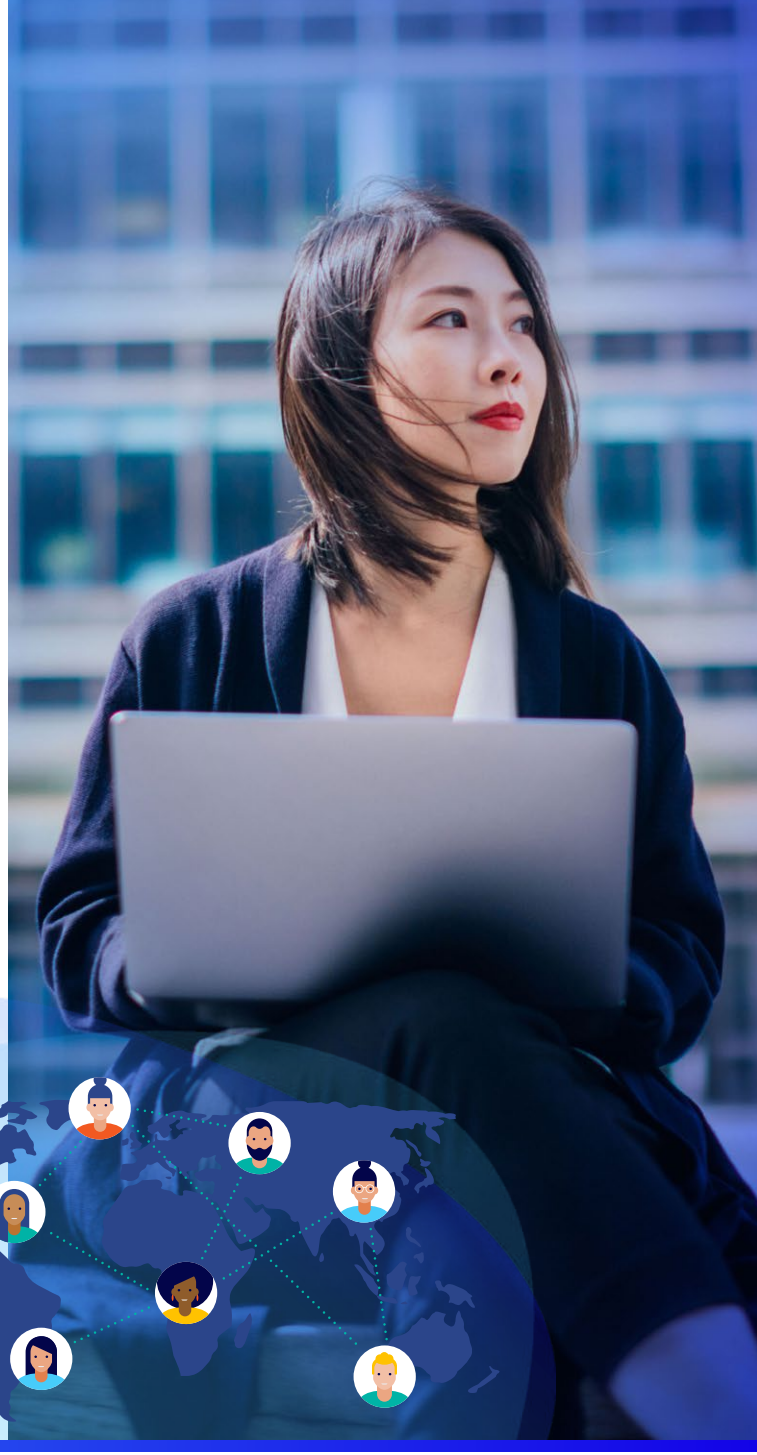
Recognizing both internal and external threats, iManage secures knowledge at its source with enterprise-level security policies and controls that are practical to manage and seamless to operate within.

ADOPTING A MODERN SECURITY CULTURE

Supporting a modern workforce that is often widely distributed – even across continents —organizations must be equipped to fight off threats from ever-smarter threat actors. Security practices need to be robust, able to respond to the changing threat landscape at pace, and able to track data as it moves around the system. Each individual must receive the right level of access, while unwanted and suspicious activity is blocked or flagged for further review.

It must achieve all this in the background, so that workers can go about their day-to-day business with ease, while understanding that the security measures are not barriers to be overcome, but rather like sentries whose sole function is to protect the organization.

A well-implemented security system is not just a technology solution, then, it is also a cultural one in which workers understand, endorse, and embrace the ways that employees access, use, store, and share company data.



PEOPLE • PROCESS • TECHNOLOGY

As you embark on your digital transformation journey, remember that "people" come first in the enduring model for organizational change management, People • Process • Technology, and that no cloud strategy will be successful without them.

A culture of security must be embraced by all. Instructing people on why a culture of security is good and necessary, or reminding people that poor data security is bad for an organization's reputation, won't necessarily result in secure behaviors being followed. What will impact those behaviors is when you make the right action the easy option. Everyone wants to do the right thing, but at the end of the day, the easy button wins.

Make it personal, not abstract. Humans respond to stories. Tell the stories that illustrate what is at stake when an organization's data is breached. Lost clients, lost jobs, even criminal action. Make it personal. Make it real.

Leaders build and maintain a security culture. A security culture does not appear of its own volition, nor does it remain in place without being nurtured. Rather, a security culture, like any other aspect of an organization's culture and practice, relies on strong leadership and support from senior leaders and individual managers.

In sum, to ensure that good security practice is second nature, embed convenient, efficient practices within everyday workloads, make good practice as simple as possible, and make bad practice difficult or impossible.This is how a security culture becomes interwoven in the fabric of the organization.

iManage

Making knowledge work

Learn how iManage can help your organization take a best practices approach to developing and maintaining a culture of security that balances safety and access in your cloud strategy.

Contact us:
www.imanage.com/contact-us/

Visit our website:
www.imanage.com

twitter.com/imanageinc

youtube.com/imanage

linkedin.com/company/imanage