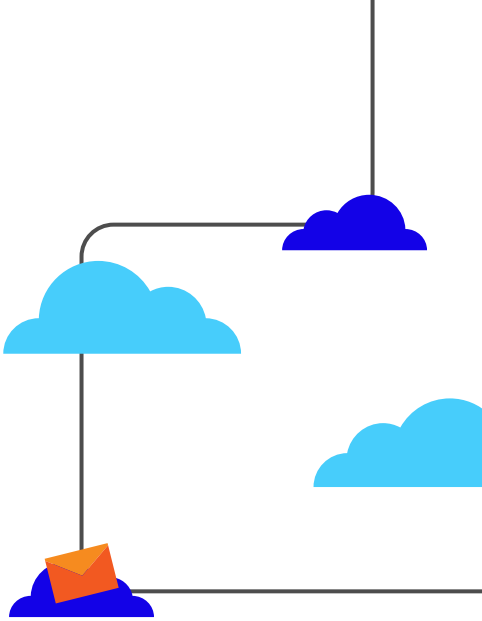
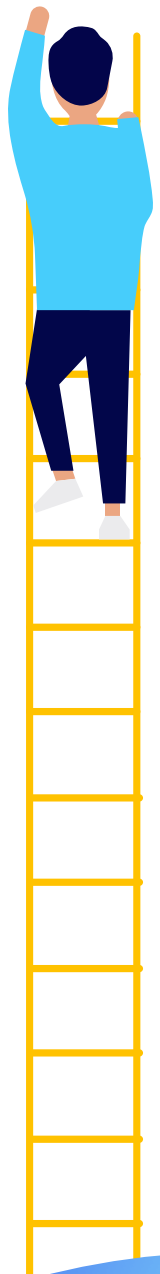
iManage
Making knowledge work

HOW TO CRAFT AND COMMUNICATE **SECURITY POLICY IN YOUR ORGANIZATION**

TABLE OF CONTENTS





EXECUTIVE SUMMARY

Knowledge is power, as the venerable saying goes. But in an increasingly knowledge-driven world, it's also the source of innovation, better business outcomes, and competitive advantage.

That's why protecting that knowledge — whether your own firm's intellectual assets or those of your clients — is critical to your ability to scale growth, ensure client trust, build your reputation among peers, and comply with ever-stricter regulatory oversights worldwide. At the same time, security must be frictionless to allow for accessibility by the right people to the right information when they need it, so they can do their jobs ethically, efficiently, and productively.

In 2020, the global pandemic forced unprecedented change on most of the world's organizations, across private and public sectors. It especially affected knowledge-based enterprises such as professional services firms, which quickly shifted to remote and hybrid work models.

To be sure, it forced us at iManage, where our mission is making knowledge work, to do the same. What didn't change for us or our customers was the rock-solid security foundations built into all our iManage platforms, which helped them move their own operations to remote and hybrid models quickly and securely.

This white paper aims to advise you on how to develop effective security policies and then enlist all of your people in the strategic imperative to build a security culture across your organization. After all, security is no longer IT's job alone. It requires everyone — from leadership to associates to administrative employees — to learn, understand, and respect this bedrock precept: Security is fundamental to the knowledge work we do and, ultimately, to our firm's success.

AUDITING YOUR EXISTING SECURITY CAPABILITIES

Whether you have documented security policies in place or need to draft them, it's important to audit your current security safeguards, so you can identify gaps that could be exploited. With annual cybercrime costs estimated to reach $10.5 trillion worldwide by 2025,[1] you don't want your organization to be among the victims. Not only is a significant intrusion disruptive, but it can also undermine client trust, tarnish your reputation, and violate regulatory mandates.

In today's world of knowledge work, most organizations have deployed some form of a layered, defense-in-depth cybersecurity model, as suggested in the best practices defined by the likes of ISO/IEC 27000 standards. The thinking behind layered cybersecurity has its roots in the design of medieval castles: The more barriers attackers must overcome, the less likely they will succeed in penetrating all of them. And if an initial intrusion is detected, the attack can be contained more easily with limited impact as a result.

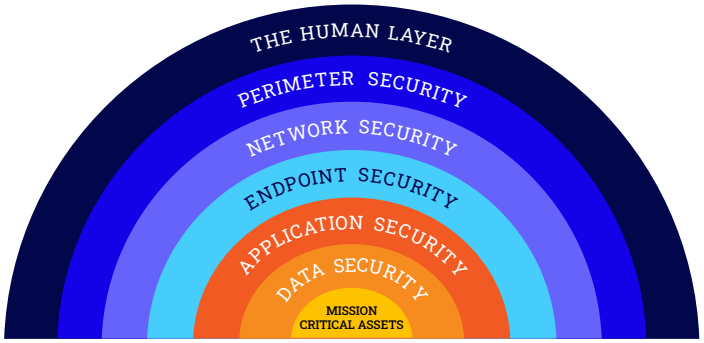
Identifying security weakness and vulnerabilities

As all IT professionals know, the days are long gone when sufficient cybersecurity meant simply installing firewalls to guard your networks, antivirus software to protect user endpoints, and an identity and access management (IAM) system to control an individual's access to networks, applications, and data.

Of course, all that is still important, but both IT and organizational complexities have grown in recent years. New technologies, especially cloud computing, web-based applications, and diverse devices, are now common.

In addition to pandemic-driven hybrid work models making remote access an ever-bigger security concern, the importance of business ecosystems has led to third-party partners seeking access to either physical assets for monitoring or knowledge assets for collaborative endeavors.

To effectively evaluate every point of vulnerability in your organization, many security experts find it helps to use the Open Systems Interconnection (OSI) model as your navigation map with the following seven layers as reference points:



The human layer, the weakest point in almost all organizations. This vulnerability can be due to employee turnover, user errors, inappropriate behaviors, lack of awareness, and so on. It's why email phishing attacks that can unleash disruptive and costly ransomware are so prevalent — and, too often, successful. It's also why periodic security awareness training and a security culture are so critical.

Perimeter security, guarding your outer network edge where devices connect. This level of security includes routers and wireless access points, as well as virtual private network (VPN) accessibility for remote workers. You should catalog every connected device — including PCs, laptops, tablets, smartphones, smart TVs, and printers — whether it is continuously connected or only occasionally so.

Network security, protecting the digital backbone of your organization. Your network should be segmented (functionally, geographically, or some other logical way), so that an attack can't spread horizontally across the entire network to access servers and endpoints at will. If your business involves industrial operations, your operational technology (OT) networks should be separated from your IT ones. Access credentials must be monitored and restricted to need-to-know resources and ethical walls must isolate conflicted users or opposing teams in legal matters.

[1]Steve Morgan, Cybercrime to Cost the World $10.5 Trillion Annually by 2025, Cybercrime Magazine, November 13, 2020.

Endpoint security, defending the devices connected to your network. The number of devices can be daunting, even in small organizations, as can their diversity, considering the "bring your own device" (BYOD) latitude that most companies have given their employees for years now. Fortunately, available software can help manage them all, including patches and upgrades that need to be done regularly; otherwise, attackers can exploit them in many ways. It's also important to have an IAM system that can automatically cut off access when employee terminations occur.

Application security, supporting the software tools your employees use to do their work. These tools also need regular updates to patch security holes and to provide new features and capabilities. Unauthorized application downloads should be restricted.

Data security, shielding the most frequent target of attacks. Data comes in two basic forms: structured, such as Social Security numbers and credit card information in databases; and unstructured, such as text (e.g., documents, email), video, and graphics. Data encryption can prevent attackers from using this information. Automated and continuous backups and recovery procedures should be in place.

Mission-critical assets. It is vital to safeguard your business essentials, such as core intellectual property that belongs to you, your customers, or your clients. Not all data requires equal protection, but this type of data should have the highest levels of security.

Determining and prioritizing new technology needs

If done right, the discovery involved in auditing your security safeguards will take significant time and well-qualified expertise to complete. If your IT team lacks either or both, outside consultants can conduct the audit for you.

In addition to taking a detailed inventory of all the devices, applications, network components, existing security controls, and other elements, you need to document the findings in a version-controlled file, such as a spreadsheet, that itself is protected and backed up.

The next step is to prioritize the gaps and vulnerabilities that are most critical as well as the technology needed to address them. In many cases, those issues won't need to be resolved with technology but rather with a new or revised process or protocol.

Last — and certainly not least — you should assess and test the backup and recovery capabilities for your current data and applications, for both on-premises and cloud environments. These capabilities must be available to facilitate a documented incident response plan that has specific roles and responsibilities assigned to relevant and qualified personnel by name.

Over time, technology advances and people change positions or leave the organization. For these reasons, you should conduct both a security audit and practice the incident response plan's procedures at least once a year.

SETTING A DOCUMENTED SECURITY POLICY FOR YOUR ENTIRE ORGANIZATION

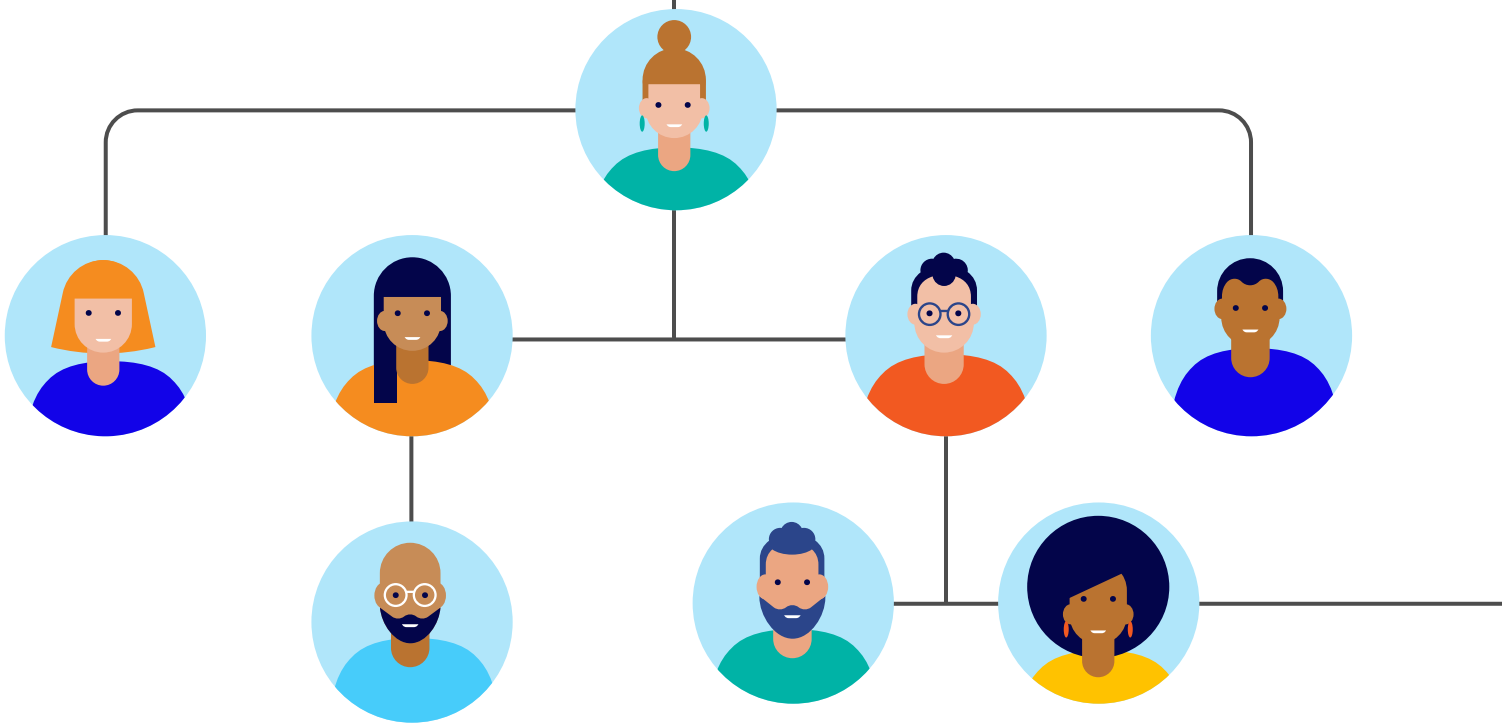
A security policy establishes guidelines and standard procedures to protect an organization, its operations, and its knowledge and intellectual assets from cyberthreats, both internal and external. While the latter gets the headlines, the former deserves serious concern.

According to one of the most respected annual cyberthreat reports, 18 percent of data breaches in 2021 were internal and 39 percent involved third-party partners.[2] For professional services firms experiencing lateral turnover by job-hopping associates and employees, terminating employees may want to secretly take with them confidential information, which can include intellectual property. This type of theft is common. The large frequency of partner data breaches suggests that a security policy should also cover any members of your business ecosystem with network access.

Generally, a security policy has two parts: technical and organizational. The first, for example, would include network diagrams that show segmentation, the locations of routers and wireless access points, and the names of personnel with administrative and configuration privileges. It could include the firm's incident response plan, too.

The organizational part of a security policy provides rules governing employee access and use of information, data, and intellectual property that belongs to the firm or to its clients. Typical topics would include: acceptable use of IT infrastructure, applications, and data; access control, including remote access; how to handle sensitive data; proper email protocols; and the use of social media.

To be effective, a security policy must apply to everyone, from leadership and partners to associates to administrative employees. It should explicitly state consequences or penalties for inappropriate use of IT and knowledge assets, either intentionally or inadvertently. But to apply to everyone, the policy must be supported by periodic training and ongoing communication, which will be discussed later in this paper.



[2]Gabriel Bassett et al., Data Breach Investigations Report, p. 11, Verizon, May 25, 2022.

Balancing security and accessibility

One important consideration that organizations must evaluate, especially law firms and other providers of professional services, is how to balance security and accessibility. These two factors are essential to making knowledge work and, based on our experience with thousands of customers worldwide, they underpin the pain points and successes that iManage customers share.

As illustrated in Figure 1, iManage Security Policy Manager can help enact effective knowledge and intellectual property safeguards while supporting appropriate accessibility for relevant stakeholders. Although designed for law firms and corporate legal departments, its features and capabilities can benefit many other professional service providers as well as organizations in a wide range of industries.

Ensuring secure, cross-business knowledge sharing

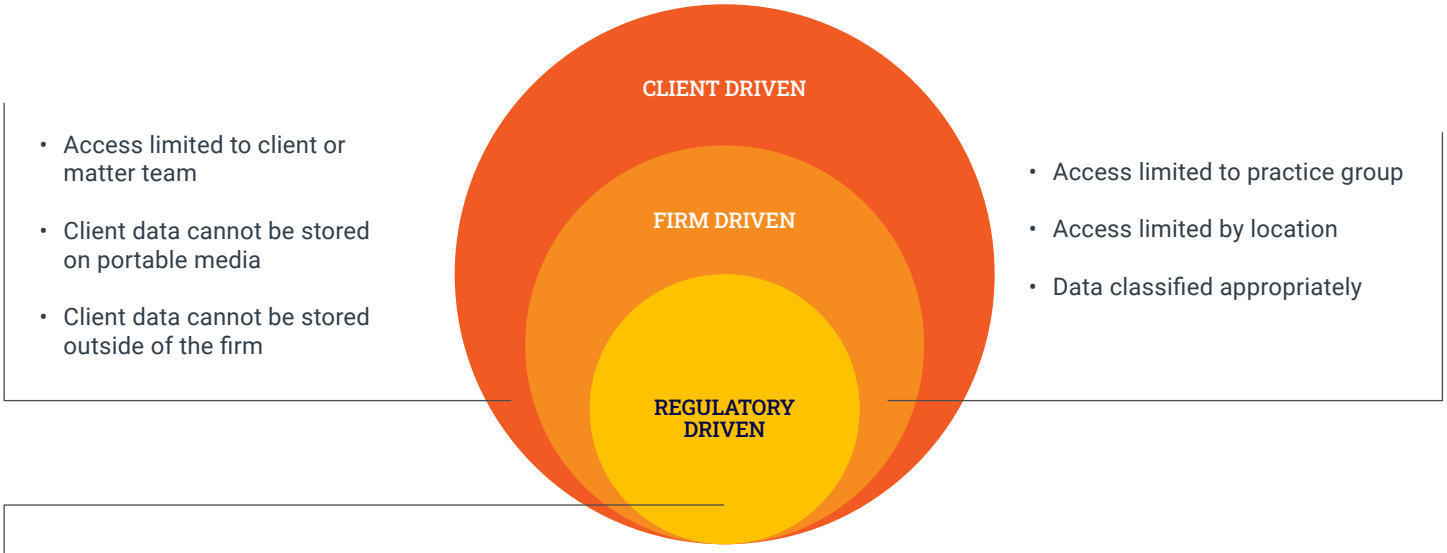
Sharing knowledge easily yet securely across your organization can break down silos and facilitate greater collaboration, which can lead to better business outcomes. For law firms, security must support the entire legal document lifecycle, too, including creation, management, legal hold, records retention, and disposition.

To overcome organizational resistance to adoption, security must be unobtrusive and as transparent as possible. Security must ensure ease of use, mobile and remote access on any device, and compliance with broad, quickly evolving regulatory changes.

Modern organizations need systems that provide high security but give more granular access controls and flexibility than the open or closed options that can either risk too much or inhibit workflow.

SECURITY POLICY MANAGER — KEY DRIVERS

Figure 1. Key accessibility and data protection drivers supported by iManage Security Policy Manager



INTEGRATING MULTIPLE VIEWPOINTS WHEN CRAFTING SECURITY POLICIES

Security is everyone's responsibility, so security policies should reflect the needs and interests of an organization's many different functions and stakeholders.

Getting cross-functional input and buy-in

Principal among those other functions and stakeholders are the corporate legal team, finance, human resources, procurement, production, and administration. Of course, IT supports all of them in their secure access and use of technology, applications, and data.

As part of crafting an organizational security policy, it is important to clearly explain the goals of developing such a policy, answer any questions to clarify misunderstandings, and solicit their input and support. Keep stakeholders informed of the policy's development and let them know that you value their advice. Doing so will help ensure that when the policy is ready for organizational adoption, they will already have bought into it, given that their input helped draft it.

In addition, consideration must be given to a company's executive leadership, which typically consists of the heads of these functions as well as the CEO, president, and COO. Many professional services firms — such as law firms, accounting practices, and business consultants — are organized as partnerships with a managing partner or director heading all administration. In any case, many if not all of these other functions exist, too.

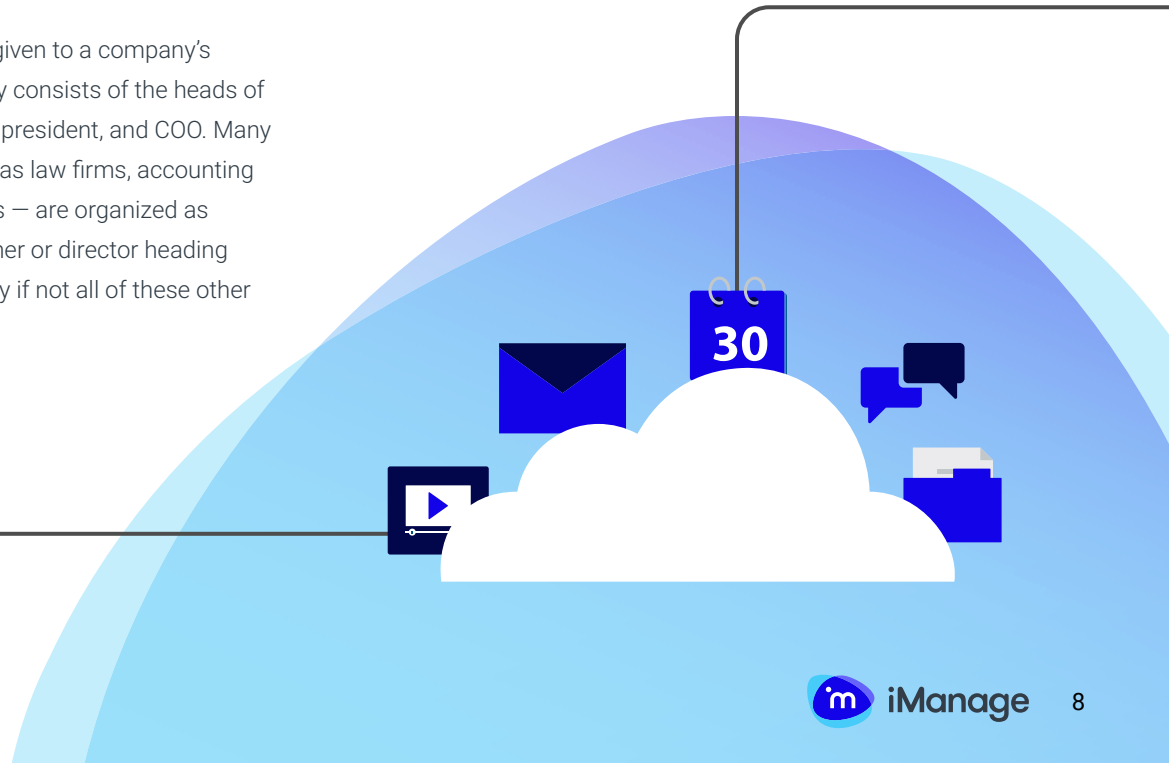
Understanding different security concerns across teams and departments

As you gather input from different functions, you'll discover their security concerns will vary, depending on their working contexts.

For example, legal has ethical and regulatory requirements for the intellectual and knowledge assets they must handle. Finance and accounting need ready access to financial data for planning and reporting but must be careful about leaks, especially if the company is publicly traded. Human resources staff needs employee data secured, often in compliance with various privacy regulations, and must be able to conduct easy onboarding of new hires and to terminate access privileges immediately whenever an employee leaves the firm.

Nevertheless, these and all other teams and departments share a common desire in the overall organization's security: They want it to be frictionless, so they can quickly and easily access the data, information, and knowledge assets they need from wherever they're working.

iManage Work 10 and iManage Cloud, along with our iManage security-related offerings, can help organizations achieve the balance between security and accessibility that's right for their particular requirements. In addition, these solutions provide flexibility and scalability to adapt to a company's changes — mergers, acquisitions, or divestitures — and growth over time.



RESPECTING AUDIENCE MOTIVATIONS WHEN COMMUNICATING SECURITY POLICIES

If layered, defense-in-depth cybersecurity models are reduced to their most basic elements, three would emerge: technology, processes, and people. Of those, people are the most exploited vulnerability.

Speaking the language your audience speaks

Given this situation, the goal of all organizations must be to build a security culture in which all their people — everyone from leadership on down — respect and support the need for security without any reservations. Core to this goal is for them to understand that security is everyone's responsibility.

Each person must know their relevant responsibility in securing data, information, and knowledge while safeguarding intellectual property. Communications and training around the topic and organizational policy are required and should be conducted periodically, at least annually.

To be most effective, communications and training should use the language of a particular audience. If legal, then use terminology such as "ethical walls" and "need-to-know." If production, use manufacturing or logistics terms, such as "output" and "just-in-time."

Whoever developed the security policy should be part of the team developing the communications and training, or at least actively advise them to ensure clarity and accuracy for the entire organization. Next, reach out to the various functional stakeholders who provided input to the security policy's development.

Having earlier enlisted the support of these stakeholders — actual group leaders or individual contributors respected by their teams — the security policy project team can ask for their help. They can ensure that both communications and training speak directly to their respective groups and are not over the heads of these audiences.

Adapting messaging as needed for different audiences

What's more, a true security culture will be integrated into a firm's organizational fabric of values. For security to become a part of day-to-day work, employees must know and apply the security policy in its entirety, no matter where they are.

Communications and training professionals know the acronym WIIFM — "What's in it for me?" — as the key to capturing an audience's attention as well as their support for what's being said and taught. Frankly, security in general and security policy in particular can put people to sleep or set their minds wandering to other priorities in their work or personal lives.

To avoid such passivity or, worse, indifference, individual audiences need messaging that answers WIIFM directly and does so in engaging and compelling ways. Good storytelling, role-playing, short pop quizzes, good graphics, and other techniques can help. But be careful about using humor because security is serious, especially the consequences of breaches.

MAINTAINING CONSISTENCY IN COMMUNICATION WHILE SCALING SECURITY POLICIES

If your organization is just implementing its first security policy, or if you've updated an existing policy and decided it's time to build a security culture around it, the following tips will help you achieve your goals. At the same time, the full implementation of a comprehensive security policy can take months, during which time employees will need periodic updates relevant to them and the work they do.

Communication should be ongoing

Although most people prefer convenient "one and done" and "set and forget" methodologies for getting their work done, cultivating a security culture takes purposeful, ongoing communications after initial training happens.

Similar to building a safety culture inside a factory, security awareness needs to be frequently referred to by leadership to show their support. It should also be promoted by posters in office environments, such as break rooms, hallways, and bulletin boards, and by consistent mentions in company communications.

Those mentions can explain in short form, preferably using graphics, the security technologies being used (e.g., "What's a firewall and how does it work?"). They can also show the latest example of a phishing email that made it through the firm's spam filters.

People learn by repetition, so keep in mind the "7x rule" when communicating. Research has consistently shown that people must see or hear a message at least seven times before they get it. The message can come via different media and channels, but clarity and consistency are key.

Updating your users in multiple formats

To keep employees informed of security news, whether related to policy, implementation activities, or new threats, use all the company communications media that are available to you, such as email and Slack.

Front-line supervisors are also important communication channels, perhaps the most important. That's because research has shown teams look to their supervisors first, not only for company information but also for guidance on how that information should be used. So be sure to enlist their support in amplifying security's importance and sharing security news in positive, constructive, and actionable ways.

Communicating in advance of changes whenever possible

Surprises, especially ones that can disrupt someone's work, are never welcome. Too often, for example, operating system or application upgrades can abruptly lock up a user's device or needed application for several minutes or longer, especially if their device must reboot.

Another example: Periodic password changes — considered a best practice — can be annoying or even disruptive, if your PC or other device suddenly demands you select a new password during a client or customer web conference.

For these reasons, if changes to your organization's security operations or policy require some action by employees or different behaviors, it's best to inform them well in advance. The bigger and potentially more disruptive the change, the more advance notice should be given.

YOUR BEST DEFENSE AGAINST THREATS: A STRONG SECURITY CULTURE

Secure technology and best practices are essential. Knowing your documentation, communications, contracts, and chats are being secured at their source enables you to open and share your knowledge resources seamlessly with others who need access — and enables them to enrich it further with their own content, context, and experience.

But investment in the world's best security technology is useless if the people in your organization believe it is IT's job to protect the company from cyberattacks, and don't take security seriously. External forces, hacks and attacks, inconsistent approaches to security, poor file-saving habits — all these and more are threats to preserving institutional knowledge.

Attacks are a given — and although a strong security culture won't prevent them happening, it dramatically reduces the odds that the attackers can be successful by exploiting employee ignorance or negligence.

The fundamentals of fail-safe security must be observed — and the protection parameters followed — before you can confidently make the meaningful connections from one document or subject-matter expert to another that grow and activate your knowledge assets. Protecting the components and curators of knowledge that you have within your organization secure your foundation for a better future.

Protect your knowledge and secure your vision with iManage today. For more information, we invite you to visit: https://imanage.com/making-knowledge-work/protect.

iMANAGE SECURITY PRODUCTS

Security Policy Manager

Easily manage complex security policies at scale, including need-to-know access, ethical walls, or information barriers and data segregation to minimize the impact of a security breach. Secure critical content across multiple repositories with need-to-know security access, without affecting productivity or performance.

LEARN MORE ›

Threat Manager

AI-based threat detection with alerts, reporting, metrics, and information governance controls can help manage sensitive information with greater levels of visibility and control. Protect sensitive content with sophisticated real-time threat detection, intervention to prevent data loss, analytics, and data governance.

LEARN MORE ›

Records Manager

Manage both physical and electronic records without slowing down employees by using integrated governance policies that monitor and enforce compliance. A single, intuitive interface for physical and electronic records management can keep your business compliant and productive.

LEARN MORE ›

About iManage

iManage is the company dedicated to Making Knowledge Work™. Its intelligent, cloud-enabled, secure knowledge work platform enables organizations to uncover and activate the knowledge that exists inside their business content and communications. Advanced Artificial Intelligence and powerful document and email management create connections across data, systems, and people while leveraging the context of organizational content to fuel deep insights, informed business decisions, and collaboration. Underpinned by best-of-breed security and sophisticated workflows and governance approaches, iManage has earned its place as the industry standard by continually innovating to solve complex professional challenges and enabling better business outcomes for over one million professionals across 65+ countries.

Visit https://imanage.com to learn more.

© iManage LLC 2022. All rights reserved.

iManage
Making knowledge work