ITGlue
A Kaseya COMPANY

Securing Your Documentation and Passwords: The Complete Guide

The power of information is unparalleled in this digital age. Organizations of all sizes are embracing digital transformation to unlock new possibilities, enhance efficiency and stay competitive in an increasingly connected world. However, with these technological advancements come a multitude of challenges, foremost among them being the security of your most valuable assets — your documentation and passwords.

In this eBook, we shall explore the cybersecurity risks that result from digital transformation and the strategies needed to safeguard your critical documentation and passwords.

Digital transformation and cybersecurity risks

The ongoing digital transformation has revolutionized the business world by facilitating increased productivity, higher customer satisfaction, data-driven insights, improved analytics, better innovation and more. However, it has also created new opportunities for cyber actors to breach the defenses of businesses. Here are some critical security risks companies face when they undergo digital transformation.

Growing threat surface

One of the major side effects of digital transformation is the overall increase in threat surface for cybercriminals to exploit. Since organizations are digitizing every part of their operations, there is a steep increase in vulnerable endpoints. With hackers now having more ground to cover, an unexpected compromise in any of these endpoints could risk the security posture of the entire IT infrastructure.

Also, maintaining a large infrastructure comes with many challenges. From securing every endpoint to incorporating the right preventive measures, the tasks are endless. Cybercriminals continually devise innovative tactics to circumvent organizations' proactive security efforts, resulting in potentially costly breaches, especially for those handling sensitive data.

Increasing attacks on the cloud

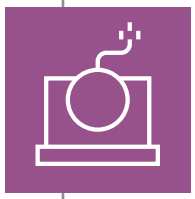
As IT infrastructures rapidly expand, so does the data produced. As a result, organizations are compelled to migrate vast data volumes to the cloud. Consequently, cyberattacks on cloud-based networks surged by approximately 48% in 2022, as reported by Check Point Research. Furthermore, 70% of organizations hosting data in public clouds experienced security incidents.

Various factors such as misconfigurations, compromised user accounts, API vulnerabilities and insider threats contribute to the growing prevalence of cloud-based attacks. Even top-tier companies sometimes neglect cloud security, leading to misconfigured servers and weak password practices. Implementing stringent security measures, including access controls and role-based access restrictions, can mitigate most cloud-based threats.

Security measures not keeping up with digital transformation

Modern organization's inability to implement cybersecurity measures that can keep pace with rapid digital transformation is a critical concern. Limited workforce resources and security tools compel many organizations to rely on basic cybersecurity measures. Also, investing in advanced security solutions is often a significant business decision that most companies are hesitant to make.

In some instances, organizations overlook simple security measures for convenience. Consider the adoption of multifactor authentication (MFA) for cloud-based accounts as an example. Despite its effectiveness in preventing attacks, MFA adoption among Microsoft users reached only 28% as of December 2022, leaving cloud networks susceptible to exploitation.



Pressure to adopt new technology

Global businesses face immense pressure to adopt new technology and gain a competitive edge. Digital transformation is a pivotal decision that can fundamentally alter established business practices. Despite initial challenges such as high upfront costs and technical complexity, organizations must navigate this transformative process to remain relevant.

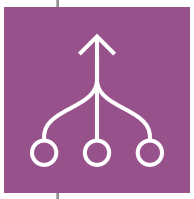
While this pressure can stimulate creativity and innovation, it necessitates deployment of the appropriate technological infrastructure. Inadequate understanding of complex solutions or failure to select the right technology can introduce vulnerabilities that hackers may exploit.

MFA adoption among Microsoft users reached only 28% as of December 2022, leaving cloud networks susceptible to exploitation.

How to incorporate effective cybersecurity measures

Amid the challenges caused by digital transformation and the rapidly changing threat landscape, many organizations are struggling to secure their vast IT infrastructure. A one-size-fits-all approach is not the ideal way to go. Since every company has its own priorities and security requirements, organizations must incorporate a strategic approach to boost their cyber resilience.

To establish effective cybersecurity measures, organizations must focus on modernizing their IT infrastructure, consolidating their IT operations, securing their data and information, integrating various IT tools and incorporating a process- and human-centric approach. Let's discuss the significance of these measures.



Consolidate your IT operations

Most IT administrators struggle with cybersecurity since they don't have full visibility into their entire IT environment. With IT infrastructure rapidly expanding in organizations worldwide, IT administrators need the right solutions that can provide a unified view of their IT environment. For instance, a network management solution with built-in network discovery and diagramming can provide a comprehensive overview of your network.

Similarly, a robust documentation solution that integrates with all your IT management tools can compile all the data and present it to you in a unified way. You need information about your software licenses, hardware assets, expirations, passwords, how-tos and user permissions for your daily operations. Imagine all these details scattered across multiple disparate tools. Besides making it difficult to retrieve information, this can also affect your security posture.

By leveraging consolidation, you can modernize your IT environment and make information management a breeze.

Secure all data and information

Data is the most valuable commodity in today's world. With huge volumes of data generated daily, companies typically spend a fortune to keep all this data secure. Data privacy laws legally require organizations that handle customer or employee information to invest in robust security solutions. Since cloud adoption is vital in digital transformation, companies must proactively secure their cloud storage infrastructure.

Here's a list of things you must do to secure your valuable data:

- **Back up your data regularly:** Modern backup solutions have powerful automation capabilities to automate your entire backup process. Use a robust tool that has powerful encryption systems to lock your data in a secure system.
- **Use strong passwords and MFA:** You can enforce strong password policies among your workforce to ensure your information is well-protected. Based on the importance of the information, you can use one or more additional layers of security (MFA) to secure the critical information in your infrastructure.
- **Create awareness:** Effective data security requires the participation of your workforce as well since they are the first line of defense in your network. Create training materials to educate your workforce periodically and train them on spotting suspicious emails that require them to click malicious links.
- **Limit access to critical data:** Access control is a great way to prevent the wrong people from accessing critical data in your IT network. You can define user roles and assign permissions on who can access the data in your IT infrastructure. This ensures that only the right people have access to the right information.

Data privacy laws legally require organizations that handle customer or employee information to invest in robust security solutions.

Follow a process- and human-centric approach

A process-driven approach can help you overcome the limitations of resource constraints in cybersecurity management. Processes help you define how your security solutions must function, your people's roles and the documentation required to ensure seamless information flow. With the right processes, you can easily identify security risks and incorporate the right strategies to overcome them.

While processes are significant to ensure seamless operations, they become ineffective if people don't follow them correctly. When cybercriminals use social engineering attacks like phishing to target organizations, they are counting on the vulnerability of human behavior to gain access to an IT infrastructure.

By focusing on a people-centric approach, you can prevent social engineering attacks targeting your network. You can provide awareness training periodically and empower your employees to actively participate in your cybersecurity strategy. You must also regularly test your employees' ability to identify threats by simulating various phishing attacks. This simulation test will help identify the weak links in your workforce so you can provide specialized training for them.

When cybercriminals use social engineering attacks like phishing to target organizations, they are counting on the vulnerability of human behavior to gain access to an IT infrastructure.

A multilayered approach to security

A multilayered approach leverages various security controls to protect different vulnerable areas in your IT infrastructure. The idea behind this approach is to incorporate security measures where hackers will face multiple barriers when accessing your IT network. Since hackers mostly target networks with easy access, this approach discourages them from breaking into your IT infrastructure.

Under the multilayered approach, companies incorporate robust strategies for various components, including devices, networks, infrastructure and applications. Cybercriminals could target any of these components to gain control over the entire IT environment. For instance, a successful attack on an individual computer can lead to the breach of an entire network.

Each layer in a multilayered approach provides a protective barrier against a specific attack type, making it more challenging for hackers to gain access. Let's see how a multilayered approach incorporating a robust IT documentation solution would work in today's threat scenario.

Build a good foundation

Your foundation starts with looking at your entire network and building a framework for security management. This ensures that all aspects of your security program can be easily maintained and scaled as operations grow and change. Your security foundation will likely be a broad program with different processes for different components. You can either base this on any existing compliance regulations in your industry or build an entirely new security foundation based on your requirements.

Data security

There are various security controls you can incorporate for data security. In modern-day IT networks, the following measures are crucial and provide a foundational layer of protection:

- **Multifactor authentication (MFA):** This feature adds an extra layer of protection when accessing your IT documentation by requiring an authentication code from a secondary device in addition to your username and password, enhancing security.
- **Single sign-on (SSO):** Make your authentication process easier and more secure during login by unifying the credentials of multiple solutions.
- **IP access control:** This feature allows you to restrict access only to a predetermined list of IP addresses, keeping potential bad actors out of your network.
- **Roles and security permissions:** You can select different access permission levels based on a user's role in your network, ensuring only the appropriate personnel have access to different parts of your IT information.

Password security

Since passwords are the first line of defense against unauthorized access, your multilayered security approach should also focus on strengthening your passwords. Besides implementing strong password policies, you can incorporate features like host-proof hosting and password rotation to ensure robust password management.

Host-proof hosting guarantees that your IT documentation solution never accesses passwords in their unencrypted state. All passwords undergo encryption and decryption exclusively on the end-user device, and decryption is only possible with the user-specific passphrase.

Passwords serve as the initial defense in safeguarding your data and sensitive information. Failing to change or renew them regularly exposes your organization to risks. Manually rotating passwords one by one is a tedious and time-consuming task, contributing to this common challenge. To prevent passwords from becoming stale and jeopardizing your data, opt for automated password rotation to ensure they stay fresh and secure.

With an OTP generator, you can easily access shared passwords without compromising security. This streamlines the login process when, for example, multiple technicians are given administrator access to an application. The OTP Generator ensures they will all be able to access the OTP code to successfully complete the MFA login.

Knowledge security

Knowledge security is a critical part of any cybersecurity strategy since it protects all the organizational and shared knowledge in your organization. It starts with incorporating the right measures to ensure the quality of your documentation, from completeness to version control and finally to continuous maintenance.

Once you've compiled essential knowledge within your IT infrastructure, the next step is to review and approve it with the relevant stakeholders. To enhance knowledge security, it's crucial to assess your documentation for outdated information and archive it as needed. This process becomes seamless with features like workflows and flags. These tools enable timely alerts to the relevant team members, ensuring documents undergo regular reviews or updates, preventing information from becoming stale and inaccurate.

To enhance knowledge security, it's crucial to assess your documentation for outdated information and archive it as needed. This process becomes seamless with features like workflows and flags.

Building a resilient and secure digital future

As we witness the expanding threat landscape, increased cloud vulnerabilities and security measures struggling to keep pace, a multifaceted approach is essential to fortify your defenses. With a focus on consolidation, data protection, processes and people, organizations must equip themselves with the right tools and insights to safeguard their invaluable documentation and passwords. In an age where data is king, organizations must focus on building a more resilient and secure digital future.

Secure, Mature and Integrated Documentation

Make documentation easy

Create and store KB, checklists and SOP articles effortlessly, embed rich network diagrams or import Word documents so your team is empowered to train and help themselves.

Secure your critical information

Sleep better with next-level password management featuring access control, host-proof hosting, at-risk password report and audit trail.

See the complete picture

Link related items together, so that all the information you need is at your fingertips. Rapidly define and understand relationships between various elements of your documentation.

Build a documentation culture

Edit and collaborate directly within the platform. Automatically save and sync to ensure your documents are always up to date for all team members.

Trusted by More than 13,000 Partners in 70+ Countries

Safeguard Your IT Operations with Secure Documentation

Request a Demo

When it comes to data security, IT Glue is second to none. We have achieved a SOC 2 Type-2 attestation, a set of data security and service controls that can only be maintained through ongoing, company-wide commitment.