AODOCS

fourcast.

Document Security: 9 Reasons Why Everything Should Be In The Public Cloud

Whitepaper

Contents

Introduction

For businesses to thrive, they must be able to protect company data and sensitive customer information. Moreover, companies exposed for bad security practices pay a big price, often smeared in the media and slapped with large fines.

Security Scandals Make Headlines

Companies of all sizes fall victim to data leaks and security breaches. In 2017, Huddle, a business collaboration platform, exposed KPMG and BBC files to unauthorized users. Popular hotel chains and Fortune 500 retailers have also fallen victim to hackers. In 2015, Hyatt discovered that an unauthorized person gained access to payment information from debit and credit cards used at their front desks. Retailers, including Target, Whole Foods, Forever 21, Neiman Marcus, and others, have also made headlines for payment information blunders. Even the Internal Revenue Service (IRS) announced that they uncovered a data breach in May 2015. Over 700,000 American taxpayers had their personal information compromised when the agency's "Get Transcript" system was hacked. With the continued rise in cybercrime targeting personal information that is collected and managed by companies, organizations must invest in the right network and document security to stay ahead of the growing threat.

With the continued rise in cybercrime targeting personal information that is collected and managed by companies, organizations must invest in the right network and document security to stay ahead of the growing threat.

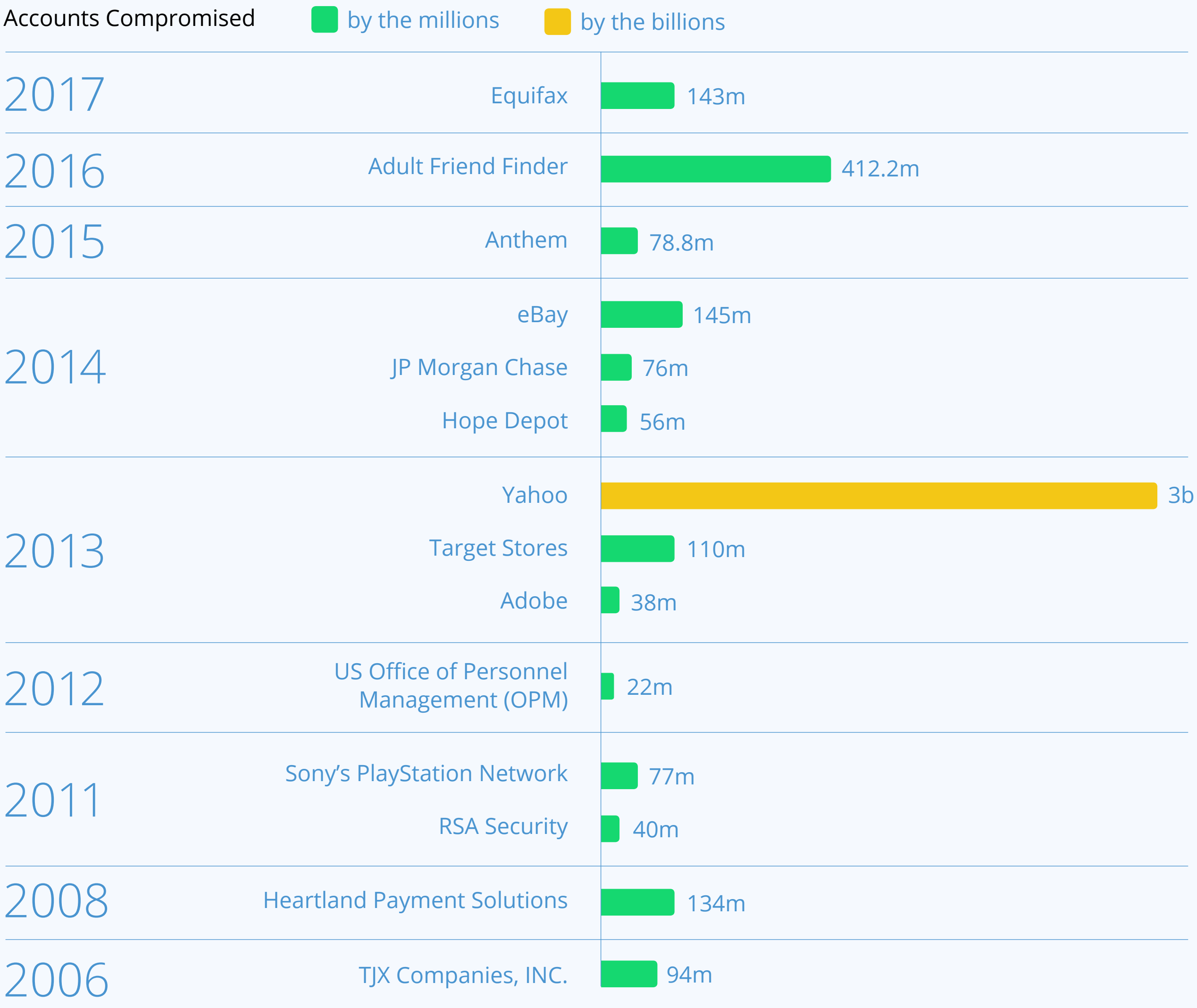
The Cost Of Compromised Data

Research continues to show that these breaches have not only ethical implications but also financial ones. In 2016, Fortune 500 retailer, Target, had millions of holiday shoppers on edge after a massive security breach in which hackers accessed the personal information of as many as 110 million consumers. In August of the following year, Target said that the costs associated with the hack totaled $148 million.

Health insurance company, Anthem, agreed to a $115 million settlement in connection with a 2015 data breach that impacted 80 million of their customers across 10 of their brands including Anthem Blue Cross and Blue Shield, Amerigroup, and Caremore.

The unanticipated costs associated with a security breach can pile up quickly. IBM's report on the costs of a data breach exemplifies how large of a financial impact one can have. Here you'll see some of the largest data breaches over the past two decades.

Biggest Data Breaches of the 21st Century



Source: The 17 biggest data breaches of the 21st century, CSO

Companies Need Cloud Partners

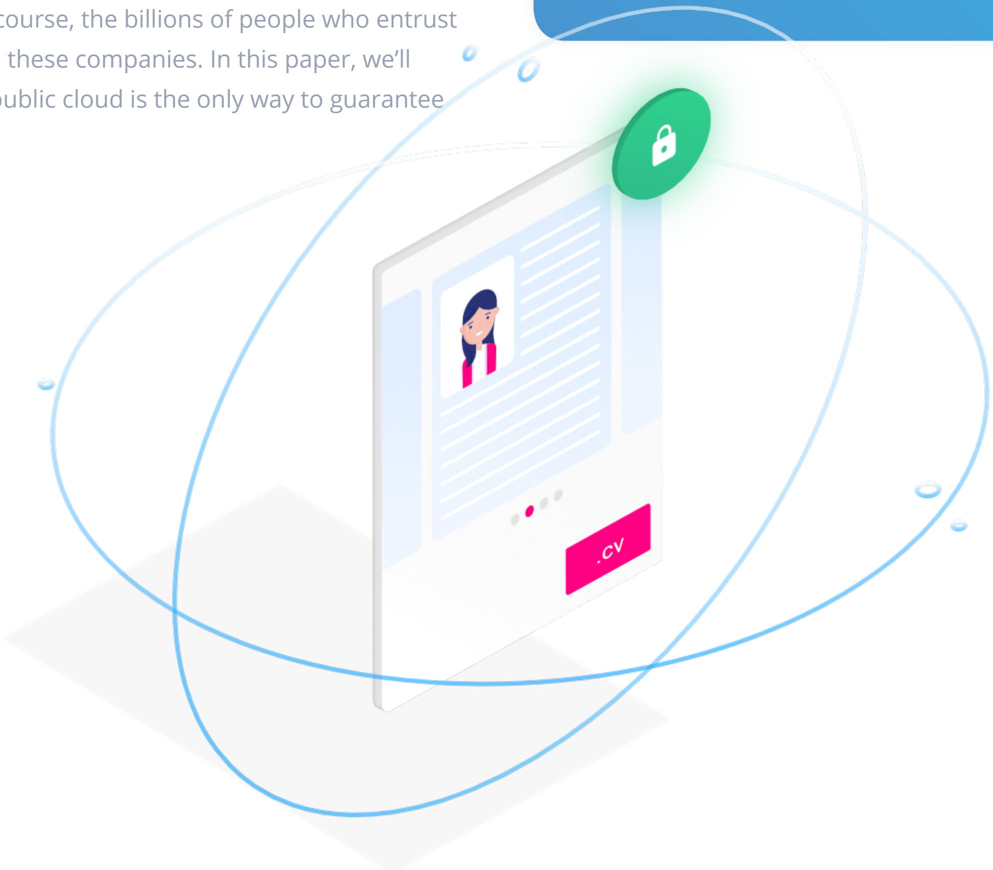
While large companies can pour millions of dollars into their corporate IT security and compliance infrastructures, many organizations don't have the financial resources and specialized human capital to properly combat human error and cybercrime. As illustrated above, the risks associated with getting security wrong are staggering - and growing.

Only public cloud companies have the resources and expertise to build and maintain secure computing, storage, and networking infrastructure as well as reliable user authentication and identity management protocols. They also operate the only IT solutions that are tried and tested by billions of people. By strategically leveraging a solution from a public cloud company that has the resources and technological expertise to build and maintain secure computing, storage, and networking infrastructure, companies can minimize their exposure at a fraction of the cost.

New data breaches and software vulnerabilities are published every day, and they are just the tip of the iceberg. It's no wonder that security and compliance concerns are leading to restless nights for IT professionals, business executives, and, of course, the billions of people who entrust their information to these companies. In this paper, we'll show you why the public cloud is the only way to guarantee document security.

> "Through 2022, at least 95% of cloud security failures will be the customer's fault."
>
> "Is the Cloud Secure?"
> Gartner Research, March 27, 2018

> "93% of organizations use cloud services in some form, with 74% storing some or all of their sensitive data in public clouds."
>
> 2017 report by McAfee



01

Infrastructure & Network Security

The two fundamental building blocks to ensuring that your data is secure are physical infrastructure and network security. Understanding and protecting information from threats and human error require meticulously layered security protocols.

Physical Infrastructure

Last year, British Airways canceled over 400 flights and stranded 75,000 passengers because of an IT outage caused by an engineer who disconnected a power supply at a data center near London's Heathrow airport. When it comes to data centers and networks, even minor human errors can have a major impact on businesses and their customers.

With the exorbitant costs and human resources required to maintain an on-premise system, organizations should be looking to public cloud companies who have the necessary resources to properly manage and secure their data centers.

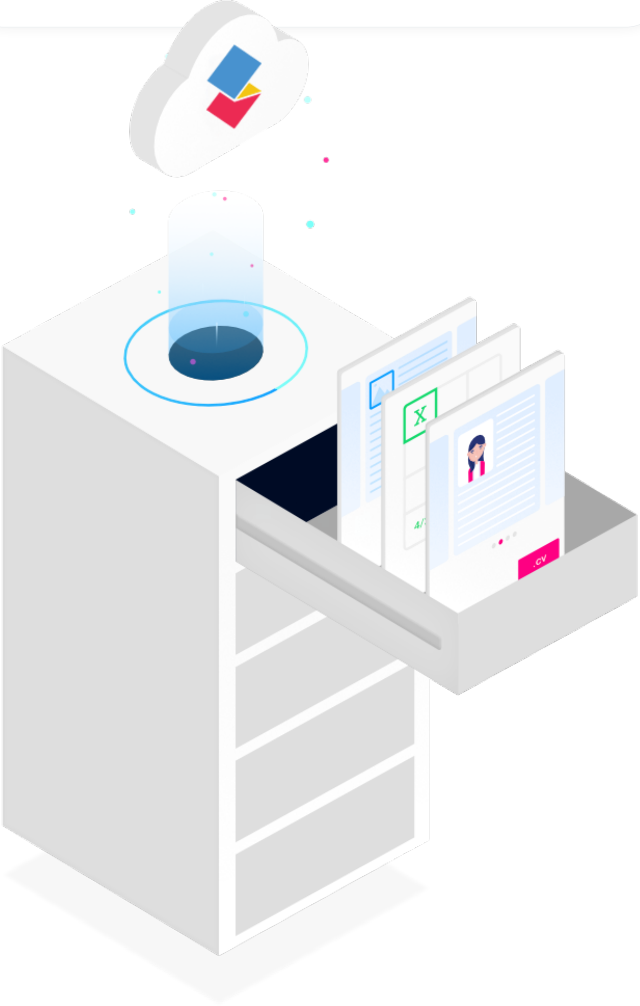
Public cloud companies bring capital and expertise to the table. Their physical infrastructure and data centers are much better protected than what most companies could put in place on their own. For example, Google's focus on security and data protection is ingrained into their company culture and technology solutions. With that in mind, it is the primary design criteria when they are constructing their data centers. Google uses a layered security model that includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and laser beam intrusion detection on the data center floor. The data centers are also monitored 24/7 by high-resolution cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Furthermore, it is only possible to access the data center floor using a security corridor which features multi-factor access control that requires a security badge and biometric confirmation. Only approved employees with specific roles are provided with the credentials necessary to enter.

> "Cloud companies and data center providers altogether spent a record $20 billion in 2017."
>
> Recode

Network Security

If you think your firewalls are secure, think again. Physical security is important but protecting your network is just as vital.

> "With sensitive business data stored on local machines, on enterprise databases, and on cloud servers, breaching a company's data has become as simple — or as complex — as gaining access to restricted networks."
>
> Digital Guardian



It's like an arms race between the defense - on-premise firewalls and security systems - and hackers. Almost half (47%) of organizations who suffered a cyber attack identified the root cause of their data breach as a malicious or criminal attack.

"Firewalls are considered a mature technology by most organizations and typically are given minimal thought by security professionals. When it comes to an audit or assessments, a simple check of a box indicating there is a firewall protecting the network is typically all that is done," says Eric Cole in an article for TechTarget.

Not only are internally-built firewalls typically poorly managed and more vulnerable to being hacked, they are also unable to provide the necessary risk alerts. The only companies that truly have enough properly trained staff and dedicated resources to stay on top of network security are public cloud companies.

With so many vulnerabilities out there, from the five backdoors that Cisco discovered this year to the notorious USB Conficker worm, you need the best protection. Without regular maintenance, hackers can and will break through your firewalls and other off-the-shelf security software. Merely having a firewall is not enough to ensure that the data that is housed in your company's network is secure, and the constant testing, maintenance, and upgrades are too rigorous for many businesses trying to go it alone.

On the other hand, Google employs more than 550 full-time security and privacy professionals in their software engineering and operations division. Employees of public cloud companies include some of the world's foremost experts in data, application, and network security - publishing hundreds of research articles on information security and cryptography every year. Their highly specialized teams are broken down into more agile departments that are dedicated to disciplines that include security, privacy, internal audit and compliance, and operational security. This level of specialization ensures that customers' security needs receive even more detailed attention.

02

Software Updates

> “While I am mindful of businesses being slow to migrate, if you are going to use an old operating system, you better be on top of security,” Andy Patrizio from Network World.

Many of the network vulnerabilities described in the previous section were quickly fixed by the vendors after they were found, but this is not enough. Companies also need to update their operating systems, databases, and web servers for the patches to be applied. Many are neglecting this responsibility. When software isn’t properly updated to protect against the latest cyber threats, the entire company is put at risk.

When it comes to software maintenance, there’s more to it than upgrade and installation costs. The ability to keep a company’s software stack updated is also dependant on the capabilities of the corporate IT team and the individual employees who use company-issued or personal devices for work. It's also challenging to update systems and devices without service interruptions. Many IT departments will delay the deployment of critical updates to minimize the impact of interruptions.

> “26% of companies ignore security bugs because they don’t have the time to fix them.”
>
> Catalin Cimpanu, Security News Editor for Bleeping Computer

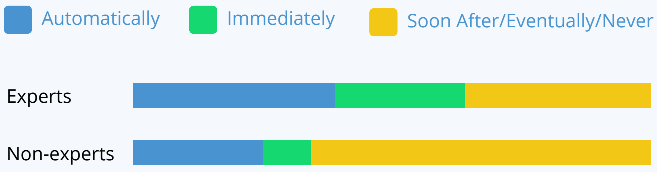
This is a common pitfall of organizations who use more traditional business platforms, like Microsoft Office, where regular updates depend on coordinating the installation processes with multiple departments. In certain instances, as was the case with WannaCry, patches for old software may not even be available.

“Many of the computers affected by WannaCry were running the Windows XP operating system, which couldn’t initially be patched because Microsoft stopped supporting the program in 2014 except for a high fee,” explained USA Today.

The implications of a software vulnerability can be as severe as any other IT security breach. IHG released data showing that cash registers at more than 1,000 of its properties were compromised by malicious software that was designed to siphon customer debit and credit card data.

Employing dedicated vulnerability management, malware prevention, and monitoring teams, Google provides companies with a secure business platform. Google’s malware strategy uses manual and automated scanners to scour their search index for domains that may be vehicles for malware or phishing schemes. Google also utilizes multiple antivirus engines in Gmail and Drive as well as on their servers and workstations to help identify malware that may have been missed by other antivirus programs.

How soon do you install updates?



The Conversion, CC-BY-ND
Source: Google Research

03

User Authentication

Getting document permissions and user authentication right goes a long way to ensuring proper organizational security. It's important to make sure that the people who are accessing your data are who they say they are. This can be achieved with strong passwords, multi-factor authentication, and physical security keys; all things in which public cloud companies are investing heavily.

For example, Google's Titan Security Key uses multi-factor authentication to protect Google users from attacks. Hackers may be able to steal your password in the digital world but they will have a much harder time stealing a physical security key. With multi-layered authentication practices, organizations reduce the risk of unauthorized persons being able to pose as approved users.

Just look what happened back in 2017 when Deloitte, once named "the best cybersecurity consultant in the world" by Gartner, failed to use two-factor authentication. Hackers were able to access Deloitte's network after cracking the password of an administrator account that didn't require two-factor authentication. This gave the cybercriminals unrestricted access to the company's emails and email attachments. Had Deloitte been using two-factor authentication, the hackers would not have had the secondary identifier that they needed to log in and the account owner would have been alerted about the unauthorized use of their account - things that would have likely prevented the breach.

Hacked passwords cause 81% of data breaches.

2017 Verizon Data Breach Investigations Report

Still, it's not just about passwords. It's also about having the right policies and procedures in place. A public cloud solution provides customizable permissions and integrated workflows that help improve security and increase productivity. Organizations can monitor who is trying to access their network and proactively block unknown devices from connecting.

04

File Access Permissions

Having a system that lets you set the proper permissions and prevent unauthorized people from accessing files is important. However, you shouldn't think that human error won't lead to unwanted vulnerabilities. Expecting your users to manually set permissions on each file without ever making a mistake is unrealistic and simply bad for security and compliance.

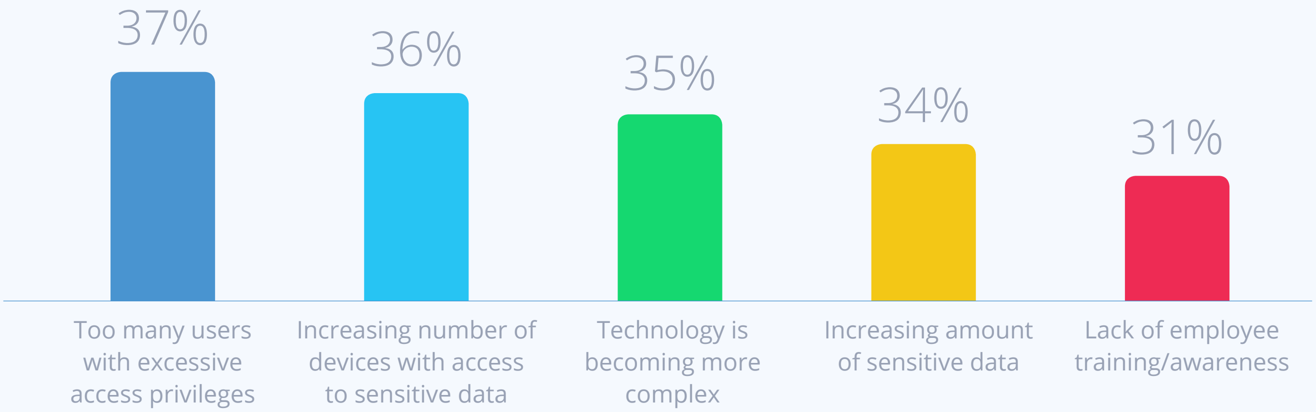
The key to getting file access permissions right is automation. By automating your file access permissions, you'll reduce the manual work, and in turn, the risk.

AODocs is a good example of a platform that lets you completely automate file access permissions. To prevent data exposure, you can automate your sharing permissions with workflows while monitoring tools will alert you if a file with sensitive content is shared with people that are not supposed to have access to it.

> "I sleep better knowing that all of our files and folders are viewed only by the persons intended to see them, and that the security and retention of those files is taken care of."
>
> AODocs customer, Peter Vorhees

When companies don't leverage automated document controls and permissions, their data is at risk. GoDaddy, Verizon, and DowJones, for example, exposed documents containing sensitive information because of improperly managed Amazon Web Services (AWS) S3 cloud storage bucket settings. Companies can easily avoid accidental human errors like this by using automation tools like AODocs.

What do you believe are the main enablers of insider attacks?



Source: Insider Threat 2018 Report, Cybersecurity Insiders

05

Centralized Information

Information is far more secure and easier to control when everything is stored in one central location. The more locations where files can be stored, the more likely that at least one of these locations will be accessed by unauthorized users.

To enhance productivity, the public cloud provides a suite of business tools with centralized access and real-time collaboration capabilities. This is an inherent advantage over the traditional workflow: save, drag, drop, email, download, edit, and repeat. Whereas many of the steps in the old-school process expose documents to security vulnerabilities, public cloud platforms allow you to keep your documents centralized and accessible.

Companies who leverage G Suite can also securely share documents like contracts, terms and conditions, and job opportunities with people who don't have Google accounts using a new technology called AOBox. The original document remains in a controlled, centralized location while a link can be easily shared with external users so they can securely collaborate on the document.

Sharing files with tools like AOBox is much safer than using email attachments. Beyond being a version control nightmare, email attachments open your information up to unauthorized modifications and expose it to any software or network vulnerabilities found on the recipient's device. By controlling access to documents, companies can effectively negate the risk of a file being shared with someone without their knowledge.

Centralizing information also means that no information should be stored on local devices. USB keys are one of the biggest offenders. These devices are often lost or stolen. In late 2017, a USB stick with highly confidential Heathrow Airport security data was found on the street. The drive's files included detailed airport security and anti-terror measures. Moreover, people tend to use USB keys that they got for free from conferences. It's possible that these devices were intentionally infected with viruses. A security event in Taiwan recently awarded quiz winners USB sticks that contained malware designed to steal personal information. That's not all, the list of USB drive-related incidents goes on.

There is also the possibility that your phone or laptop will be lost or stolen. Those odds become even greater when you're traveling or running between meetings, events, and other appointments. If you have all of your files saved directly on your physical laptop or phone, you're presented with an obvious problem. If you lose it, those files are gone and, if it gets stolen, you're in even bigger trouble.

With cloud technology, personal computers and phones are disposable. You can misplace or wipe these devices at any time without losing any sensitive work-related data. Even better, you can be up and running on a new device in only a few minutes.

As many public cloud providers, like Google, have advanced security features, you're able to revoke the access of a lost or stolen device as soon as it goes missing. In addition, these providers use cutting-edge security to ensure that all your corporate data is safe and sound in the cloud.

06

Audit Monitoring

Black hat hackers who repeatedly probe and attack whatever IT protocols a company has put in place will return time and again with new skills and approaches. When your documents are in the public cloud, the provider is in charge of the network security. That means that their security team is monitoring the network audit logs for you.

When your documents are all in the public cloud, it's also much easier to centralize aggregated audit data. Audits won’t be hidden within clunky firewall administration interfaces and other closed proprietary systems. This is important for maintaining and improving your security protocols.

When the audit information is readily available, your company is better equipped to conduct thorough security analyses. Data analysis systems such as Google BigQuery make it easier, faster, and cheaper to load and analyze your audit log data. These systems can ingest vast amounts of data and allow you to quickly identify and investigate suspicious events. Automated alerts also allow for an immediate response in the event of a security breach.

Through real-time monitoring, companies can secure and manage their systems and files. When combined with an accurate audit log, from which your IT teams can pinpoint what information was exposed, companies can dramatically reduce the impact of security incidents.

When the audit information is readily available, your company is better equipped to conduct thorough security analyses.

07

Backups

If there are secure backups in place, your company will not have to worry about compliance or experiencing a loss of business productivity in the event of a security breach.

In a world of ransomware attacks, companies are preparing for the worst-case scenario by having smart backup strategies in place to mitigate any damage. The public cloud ensures that your information is always backed up and encrypted. Encrypting backup files adds a layer of protection against unwanted external parties, like hackers, encrypting your files themselves and asking for money in exchange for the decryption key.

Companies also need to protect themselves against human error. Employees often accidentally delete company files or make unwanted modifications. Imagine if someone edited your favorite PowerPoint slide deck and removed all of the important slides. The file hasn’t been deleted but all of your slides are now gone unless you have a backup. Using public cloud platforms ensures that you can customize permission settings and access previous document versions to resolve any man-made mistakes.

Hopefully, the implementation of other security measures will mean that you’ll never need to worry about accessing your backup data. However, it is still important to cover your bases. If there are secure backups in place, your company will not have to worry about compliance or experiencing a loss of business productivity in the event of a security breach.

08

Compliance

The roll out of the new GDPR regulations in Europe have put data compliance back in the public eye. However, the reality is that companies have been navigating the complex and constantly evolving world of privacy laws for some time. With the latest regulations, companies are no longer able to hide breaches. Governments are also setting standards to ensure that companies aren't cutting corners when it comes to security and privacy.

GDPR, for example, is the EU legislation that applies to any organization that handles the personal data of European residents. Under GDPR, companies must control precisely where and how this information is stored. In addition, the people that they collect it from can ask for it to be updated or deleted at any time. Companies that don't comply with their requests are subject to hefty fines. Financial penalties and lawsuits aside, organizations should comply with GDPR and other government regulations because it's simply good business.

The burden that regulations, like GDPR, places on companies is daunting. Securing your business processes with a cloud platform helps simplify corporate compliance since these public cloud companies are required to maintain their own set of compliance standards.

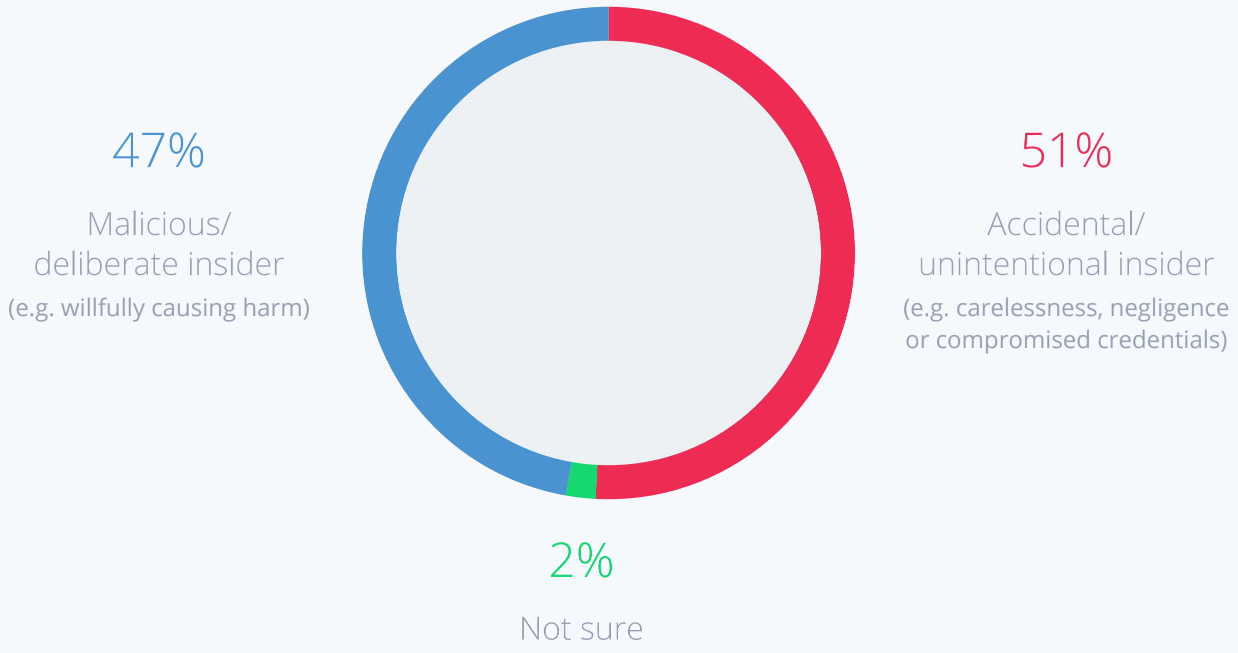
> Companies have been navigating the complex and constantly evolving world of privacy laws for some time.

09

Training & Awareness

Employees, in general, don't have a high level of computer security knowledge. However, they need to exercise caution and avoid risky practices. Companies have a responsibility to bridge the natural skill gap by providing training and awareness programs that help to prevent well-meaning employees from doing things like accidentally uploading a malicious program to the organization’s network or inadvertently sharing a confidential document.

What do you believe are the main enablers of insider attacks?



Source: Insider Threat 2018 Report, Cybersecurity Insiders

Bill Evans, senior director at One Identity, said that the Huddle breach was a two-sided problem. One issue was Huddle, of course, but KPMG also shared some of the blame. “The employees of [KPMG] were likely simply trying to be more productive. In doing so, they may have posted confidential information to a cloud-based service provider. I wonder if the use of that system was sanctioned by KPMG’s IT or infosec departments, or perhaps this was another example of shadow IT, where the line-of-business people took it upon themselves to find a SaaS solution to a productivity problem.”

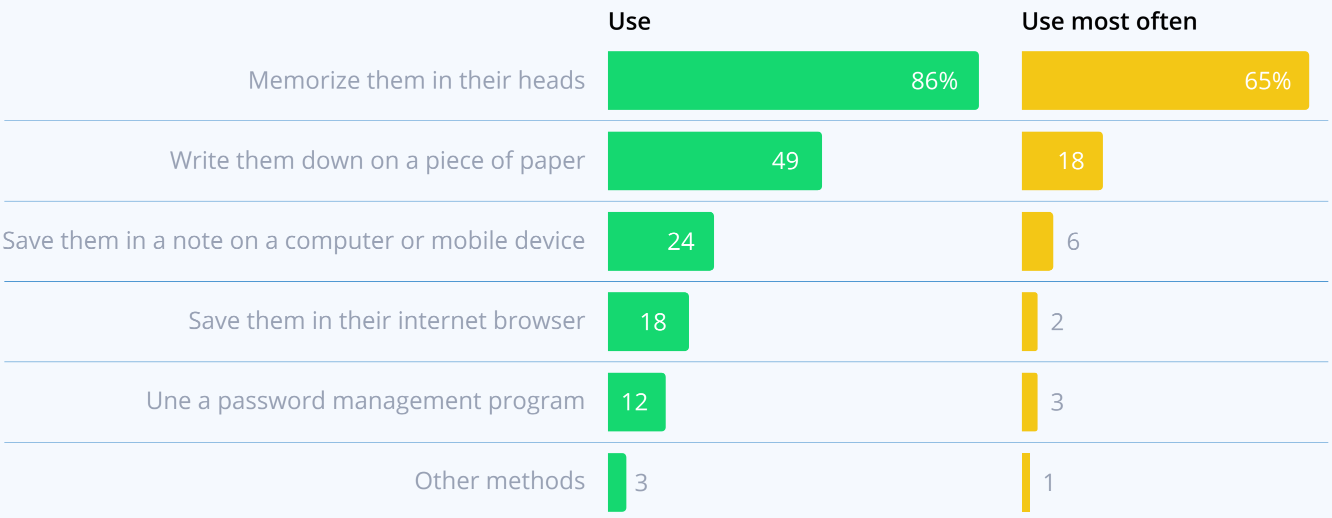
While the IT and executive leadership teams may have buttoned up their network from external threats, unsuspecting internal users can be a hacker’s best friend. Make sure that company-wide training initiatives are conducted regularly and include the best practices for:

- Downloading files and using unauthorized devices
- Suspicious links and email phishing
- Social engineering
- Personal device maintenance and safeguards
- Passwords
- Reporting a security threat

Where should companies focus their peoples’ attention? While a workforce requires training on all of these topics, there is one preeminent security threat: email phishing. With 76% of businesses reporting a phishing attack during the past year, phishing attempts have grown by 65%. While the methods of attack are varied, from posing as retailers or banks to “whale phishing,” where an individual with access to large sums of money or proprietary company information is targeted, these cyber attacks are expensive for companies. The average cost of a successful phishing attack for a mid-sized company is $1.6 million. Informing employees about the warning signs of a phishing attempt and offering clear reporting instructions is essential.

Most Americans keep track of their online passwords by either memorizing them or writing them down

% internet users who keep track of their online passwords in the following ways



Note: Results for “use most often“ category include those who use only one technique to manage their passwords

Source: Survey conducted March 30-May 3 2016. “Americans and Cybersecurity“ PEW RESEARCH CENTER

Summary

Unfortunately, hackers will always try to break into your systems, and human error will continue to put your data at risk. To protect yourself, your employees, and your company, you need to put everything in the public cloud. These solutions are able to keep your company's documents secure by:

- **Using their extensive resources and expertise to ensure that your network and infrastructure stay secure.**
- **Automatically implementing software and security updates without service disruptions or the need to coordinate with other departments.**
- **Allowing you to set up customized document permissions and integrated workflows to increase security and improve productivity.**
- **Automating fie management to minimize the risk of human error.**
- **Providing access controls and change logs to minimize files' exposure to unwanted modifications and sharing.**
- **Using aggregated audit data to identify and investigate suspicious events and creating automated alerts that allow you to immediately respond to security breaches.**
- **Automatically backing up and encrypting your files, protecting you from ransomware and providing you with a secure file repository in the case of a security breach.**
- **Making it easier to stay compliant with your industry's regulations.**
- **Offering user-friendly security controls, like two-factor authentication, that makes training employees easier while also providing your company with an extra layer of security.**

IT security is an arms race and public cloud providers have access to the latest technology and the top experts. They employ the best and brightest whose full time jobs are to protect your data against hackers and malware. While the public cloud will provide you with secure infrastructure, even the best infrastructure is not enough. As we've seen, human error also poses a major security threat. Fortunately, this problem can be solved by proper training and the process automation features from document management tools like AODocs.