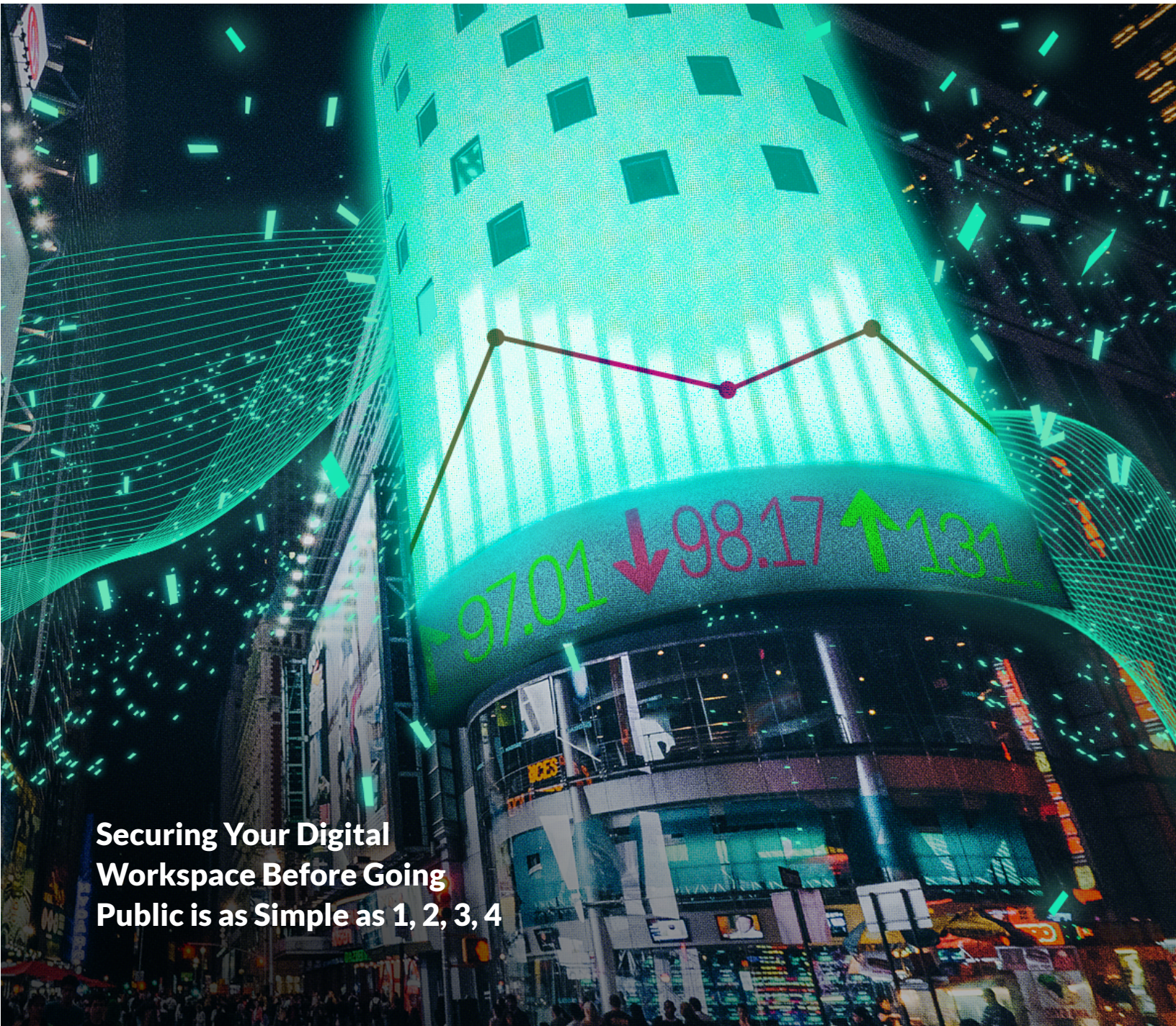
Aware

WHITEPAPER

4 THINGS TO KNOW BEFORE IPO



Securing Your Digital Workspace Before Going Public is as Simple as 1, 2, 3, 4

INTRODUCTION

The number of initial public offerings (IPOs) soared in 2021, with around a thousand companies going public.[1] Collectively, they raised in excess of $315 billion, surpassing the 1996 record set at the start of the dot-com boom.[2] Even discounting special purpose acquisition companies (SPACs), which made up about half of the year's offerings, 2021 was a banner year for IPOs. And that has encouraged more organizations to think seriously about going public.

This primarily involves establishing stakeholders and compliance around financial disclosures. However, it's also a process of identifying and mitigating risks that can dissuade investors. In today's digital workplace, some of those risks can come from unexpected sources.

Company records, communications, and proprietary information no longer reside in secured filing cabinets in locked buildings, but in the cloud. And that means they can be infiltrated or exfiltrated by unscrupulous or negligent employees. From your ecosystem, critical files could be accessed, shared, and distributed around the world at the click of a button. Worse, the proliferation of cloud tools means you may not even know when data is created, much less manage its lifecycle to reduce the risk of breaches.

Understanding where risk exists in your digital workplace, and establishing protocols to reduce and mitigate breaches, is mission critical to demonstrating regulatory compliance and preparing for a successful IPO.

Aware Can Help

Our platform identifies and mitigates risks in enterprise communications using proprietary AI/ML to evaluate short form interactions for unauthorized information-sharing, toxicity, and more.

Whether an IPO is on the radar for your organization yet or not, securing your collaboration data is a consideration that should be faced sooner rather than later.

Based on our experience, we outline four key steps that leaders in Compliance, Legal operations, and IT should take to establish appropriate guardrails that protect sensitive data in a digital environment.

1 **Audit Your Solutions Stack**

2 **Assess the Security of Each Tool**

3 **Defend Against the Most Common Threats**

4 **Consider the Human Difference**

STEP 1

AUDIT YOUR SOLUTIONS STACK

You can't secure your digital data until you have full automated and intelligent oversight of what you have and where it resides. **The average organization uses almost 90 applications; around one in ten uses more than 200**.[3] Every part of the modern enterprise can benefit from software designed to automate tasks, streamline processes, and make collaboration faster and easier, and that makes those solutions highly attractive to employees. However, each tool your workers introduce into your ecosystem must be carefully vetted to ensure it doesn't undermine your data security.

Where does technology exist?

Communication	Slack, Microsoft Teams, Workplace from Meta, Yammer
Audio-Video	Zoom, WebEx, RingCentral, Skype
Collaboration	Monday.com, Asana, Trello, SharePoint
Productivity	O365, Google Workspace, iWork, WPS Office
File Sharing	Box, Dropbox, Google Drive, OneDrive
Customer Relationship Management (CRM)	Salesforce, HubSpot, Zendesk, Zoho
Developer Tools	GitHub, Bitbucket, GitLab, Confluence/Atlassian
HR	ADP, Workday, BambooHR, Sage
Enterprise Resource Planning (ERP)	NetSuite, Syspro, Oracle, SAP

Each department could have its own technology requirements and tools. When auditing your organization's solutions stack, it's essential to talk to employees across the enterprise to gain a true picture of all the products in use.

STEP 1: AUDIT YOUR SOLUTIONS STACK

The Dangers of Shadow IT

Alongside your approved technology stack, it's not unusual to find unauthorized or "shadow IT" in place. With the rapid acceleration of remote work during the pandemic, shadow IT became inevitable for many organizations. Employees want to do their jobs as efficiently and effectively as possible and will gravitate toward tools that enable them to do so. However, few employees consider the ramifications of those products from a data security standpoint. That can introduce weaknesses into an otherwise robust digital environment.

80%
of employees admit to using unauthorized software at work

Shadow IT cloud usage could be
10x
higher than known usage

35%
of employees say they need to circumvent security policies to get their work done

The average company has
975
unknown cloud based services
(vs. 108 known)

67%
of teams introduce their own software solutions[4]

How shadow IT can infiltrate the organization

Example 1

John in Sales uses Teams to communicate with coworkers, but Slack Connect to stay in touch with industry contacts. He links his work email to his personal Outlook account to circumvent security protocols that prevent him from accessing his messages on the road.

Example 2

Sally in Marketing prefers to work in Google Docs rather than company-approved Office 365. She uses her personal account, which saves everything to her Google Drive. She then uses Zapier to automate uploading a copy of her finished work to the company Box account.

Example 3

Greg in Finance needs to split a PDF to remove confidential information ahead of a big meeting. He doesn't want to ask a coworker, so he uploads the file to a free website to modify the document. The site works so well that he downloads the freemium tool for future use.

The goal of a collaboration solution full-stack audit

At the end of an audit, you should have a complete picture of the software solutions in use across the enterprise. This is vital, because the average organization has between 500,000 and 10 million cloud-based assets stored across all tools and applications.[5] Without clear visibility of where data is stored, no enterprise can gain full oversight across everything it creates.

STEP 2

ASSESS THE SECURITY OF EACH TOOL

With so many SaaS applications in use, understanding the risks posed by each one is a significant task.

- Does the tool require unique login credentials, or does it employ single sign-on (SSO) through a service provider such as Google, Amazon, or Microsoft?
- Does it restrict views to logged-in users, or does it enable public access?
- Can the tool plug into authorized software and thereby gain access to restricted data?
- Can users invite third-party collaborators to view and edit documents?
- How is data stored, secured, and purged?
- Does the tool have audit trails, granular permissions and access?

In 2021, there were approximately 25,000 registered SaaS companies, serving a combined 14 billion global customers.[6] In preparation for going to market, how many considered the security requirements of potential enterprise users?

Organizations handling Personally Identifiable Information (PII), Protected Health Information (PHI), or Payment Card Information (PCI) should take extra care when vetting their technology stack to ensure that data is appropriately handled. Compliance, Legal, and IT leaders cannot assume that data created and housed within digital environments is adequately secured. Instead, each software solution should be examined to ensure it supports granular data retention and DLP functionality.

Some Factors to Consider to Increase Digital Security

End-to-End Encryption *(E2EE)*

Prevents third parties from accessing data during transfer

Multi-Factor Authentication *(MFA)*

Reduces the risk of a data breach from compromised passwords

Zero Trust

Requires continuous authentication and validation of all users, removing implicit trust

Cloud Access Security Brokers *(CASBs)*

Give organizations granular controls over cloud-based services

STEP 2: ASSESS THE SECURITY OF EACH TOOL

Are your software solutions proactive or reactive?

According to the Ponemon Institute, the average cost of a data breach reached an all-time high of $4.24 million in 2021.[7] The average time to identify a breach was 212 days, and it took a further 75 days to contain.

While no online application can ever be completely secured against threats, working with proactive vendors can greatly reduce the risk of a breach happening, and accelerate discovery and containment when it does.

One way to quickly establish how important data security is to software providers is to check if they're SOC compliant. Developed by the American Institute of CPAs (AICPA), SOC is a voluntary audit that service organizations undertake to verify their compliance with financial reporting, security, availability, processing integrity confidentiality, and privacy best practices. A SOC 2 certification, as held by Aware, demonstrates the highest commitment to safeguarding user data.

Granular Access Controls

Digital collaboration tools are all about removing barriers. This is great for accelerating productivity but can introduce additional risks when sensitive documents or proprietary data is involved. Granular access controls restrict information sharing between users and prevent unauthorized users from accessing all the information the organization holds.

Granular access in action:

- Restricted company storage folders prevent all employees from viewing HR or finance files
- Private Slack channels hide the details of the latest R&D project from everyone outside the development team
- IP address restrictions prevent people outside the enterprise's location from accessing their accounts

Granular access controls are governed by the "six Ws:"

WHO
Who should have access to each part of the system

WHAT
What privileges does each level user need

WHEN
When do users need access to company systems or data

WHERE
Where will users who log into the system be located

HOW
How will users authenticate their identity when logging in

WHY
Always remember why granular access controls are important!

STEP 2: ASSESS THE SECURITY OF EACH TOOL

eDiscovery and DLP

The most secure software platforms don't only protect data from unauthorized access. They also make it easier for authorized users to manage. Selecting software with built-in solutions for eDiscovery and DLP makes it easier to safeguard data, and faster to discover and contain breaches should they occur.

Data security solutions:

Federated search functionality, including by keyword, custodian, and message type

Immutable archiving to capture messages, revisions, and deletions

Granular deletion policies to appropriately retain and purge data

Smart automations to detect and remove common PII , PHI, and PCI information

The goal of proactive security assessments

Following a security audit of your full solutions stack, it's easier to identify the risks involved in using each program — and mitigate them. In 2020, 43% of data breaches were attributed to web application vulnerabilities.[8] Proactively addressing this risk reduces opportunities for negligent or malicious actors to cause harm to the enterprise. With controls in place, organizations can also use platforms like Aware to establish guardrails and workflows that monitor for risky actions and correct them in real time.

STEP 3

DEFEND AGAINST THE MOST COMMON THREATS

The majority of security breaches come from one of five threat types. Addressing each of these specifically can help prevent data losses and safeguard the digital workspace.

Threat 1: Public Sharing

Public sharing is top of mind for most security and IT leaders. One study found that around 18% of company assets are shared publicly, which represents between 90,000 and 1.8 million documents for the average organization.[9] While not every public document exposes the company to risk, how many of them contain proprietary or confidential information?

Public sharing often happens when employees become frustrated with restricted links preventing them from working effectively with others, especially those outside the enterprise. However, this is where restricted links are most important for data protection. Finding the balance between efficiency and security is an ongoing challenge for Legal and IT professionals.

Some ways to reduce this threat include:

- Disable public links where possible
- Set public links to expire after a set period
- Train employees in the risks associated with public sharing

How Public Sharing Happens

Miranda is working on a project with an external partner, Paul. She creates a document for Paul using a restricted link. Paul shares it with a colleague who requests access permission from Miranda. To expedite the task Miranda changes the link to public access. Paul's company later shares the document with a competitor of Miranda's during a pitch.

STEP 3: DEFEND AGAINST THE MOST COMMON THREATS

Threat 2: External Sharing

Even when employees use restricted links, sharing company data with third parties can introduce risk to the digital workplace. Third parties may duplicate content that they are unable to share natively, or even broadcast their login credentials for fourth parties to use.

External sharing happens frequently and is often a necessary part of doing business. The biggest risk attached to external sharing is the loss of control over how the data is accessed and used. The enterprise can only control its own security, not that of its partners, clients, and vendors. That means each instance of external sharing should be vetted in advance to assess the risk involved.

- Use expiring links to limit the duration of external sharing
- Educate employees to make qualified decisions about what and when to share
- Establish a data protection protocol with external partners in advance

How External Sharing Happens

Ellie hires an agency to create a new whitepaper based on research her company has conducted. She grants access to the research data to the project manager through a restricted link. The agency outsources the project to a freelancer and shares their login credentials for the freelancer to use. The freelancer later uses the project in their public portfolio.

Threat 3: Outdated Vendors and Permissions

Every piece of shared data will eventually outlive its usefulness. When that happens, what happens to the sharing links and access points associated with it? Often, these weak spots remain within the enterprise ecosystem, presenting more unnecessary risk.

Public sharing often happens when employees become frustrated with restricted links preventing them from working effectively with others, especially those outside the enterprise. However, this is where restricted links are most important for data protection. Finding the balance between efficiency and security is an ongoing challenge for Legal and IT professionals.

Some ways to reduce this threat include:

- Disable public links where possible
- Set public links to expire after a set period
- Train employees in the risks associated with public sharing

How outdated vendors and permissions happen

Simone completes a successful collaboration with a partner company. At the end of the project, the shared folder and files are archived in the organization's Box account. However, Simone does not delete the sharing links connected to the folder. Later, a colleague reorganizes the account and uses the shared folder as a general archive. All the files subsequently added to that folder become visible to the third party.

STEP 3: DEFEND AGAINST THE MOST COMMON THREATS

Threat 4: Personal Sharing

Personal sharing happens when employees grant themselves access to company data through personal credentials. Again, this behavior is most often driven by a desire to work efficiently, but it comes at the expense of security controls established by the enterprise.

Personal sharing creates risk by opening a conduit for data exfiltration even after an employee has left the enterprise. Preventing this kind of threat involves training workers on how to appropriately access company data —and giving them opportunities to do so outside of usual parameters in some instances. Additionally, checks and balances can be built into the digital environment to prevent unauthorized entry points.

- Block access attempts by external accounts
- Restrict unknown IP addresses
- Monitor for out-of-hours login attempts

How Personal Sharing Happens

Jose has a major presentation coming up with an important client. He wants to do some additional prep work in his own time, so he shares access to key documents with his personal email account. This way he can continue to review his work from home. Once the presentation is over, Jose forgets to revoke access. Now his personal email account can be used to access company data at any time.

Threat 5: Former or Leaving Employees

Anybody in the process of separating from the company whose access hasn't been rescinded is a potential data security risk. Disgruntled employees acting out of malice to harm the organization are the most obvious consideration, but they aren't the only actors who pose risk. Even loyal and trustworthy workers can breach data security through negligence before they leave.

The safest course of action when an employee begins separating from an organization is to revoke their access from all data repositories as soon as possible. This should be the standard procedure for any company safeguarding their digital security.

- Fully revoke access to each location, don't just shut down employee email addresses
- Change key passwords and access codes
- Reiterate the company's data security policy to separating employees

How Leaving Employee Threat Happens

Austin is leaving Company X for a more senior position with their competitor, Company Y. Austin has been an exceptional employee and his manager does not consider him a security threat. Austin wants to impress his new employer, so he copies some files demonstrating his best work. He doesn't realize they contain proprietary information.

STEP 4

CONSIDER THE HUMAN DIFFERENCE

A successful data security policy always starts and ends with people. As we've seen, many organizations have significant blind spots where risk is present, and not all are caused by malicious actors. Insider threats can be deliberate or unintentional, but either way they present potential for large-scale data exfiltration. Especially in digital environments where all the company's data is available from anywhere with the right credentials.

No amount of security will be sufficient if employees consistently circumvent it. For many organizations, finding the sweet spot between security and convenience is critical to ensure compliance. Over-engineered security protocols are more likely to drive shadow IT that dramatically reduces data security, rather than increase data protection. In one survey, two-thirds of employees admitted circumventing company security procedures but did so to work more effectively.[10] Only 3% of cases involved malicious conduct.

Ultimately, Compliance, Legal, and IT leadership need to address security from a human perspective. How easy are the tools the enterprise provides to use? Do they slow employees down or make them more efficient? How many steps does a simple process like logging into a program or sharing a file take?

Employees want to do their jobs well. The harder the enterprise makes that, the more likely it is that workers will find ways around the controls that have been put in place. So how does an organization ensure compliance with data security procedures? At Aware, we've found the most successful organizations proactively seek solutions that will solve employees' problems before they arise.

How to solve for human behavior in data security:

- Define authorized programs to facilitate information sharing, including password managers, collaboration and productivity tools, and code repositories
- Train and retrain employees using real-world examples of how negligent behaviors can introduce risk
- Assume good intent —56% of insider threat incidents in 2021 were caused by negligence, not malice[11]
- Introduce background controls to monitor for and correct unauthorized behavior such as inappropriate data sharing
- Continually audit data use to ensure ongoing compliance
- Create a culture where employees approach Legal or IT departments for the tools they need and work collaboratively to get those needs met

CONCLUSION

WHY DATA SECURITY MATTERS BEFORE IPO

A culture of compliance is easier to create at a foundational level than to implement with hindsight. And the earlier an organization considers their data security, the more cost-effective it becomes. Almost a third (29%) of IT spend on SaaS is underutilized or wasted.[12] Thus, regularly auditing your organization's solutions stack can demonstrate fiscal responsibility as well as appropriate governance, risk, and compliance oversight.

Monitoring your data security and access points also helps organizations to evidence that risky behaviors don't happen. Implementing a full-stack, AI-driven compliance and people insight platform like Aware allows companies to search and discover, monitor and moderate, and get actionable human insights from collaboration data. Ultimately, this can strengthen your risk posture by helping to mitigate inappropriate communications and accidental or planned sensitive data sharing, ensuring regulatory and policy compliance.

Having the ability to demonstrate not only that data security safeguards exist, but that they are adhered to, is invaluable when facing the scrutiny involved in going public. Ahead of an IPO, an organization needs to consider how to build security and trust for auditors and potential shareholders. Tackling GRC through data security is a critical component that must be considered by any business seeking to maximize their initial public offering. By following the four steps outlined above, Legal, Compliance, and IT leaders can take stock of their current position and realign their priorities around securing the enterprise's data in the digital workplace.

SOURCES

[1]Statista, “Number of IPOs in the US since 1999” https://www.statista.com/statistics/270290/number-of-ipos-in-the-us-since-19992

[2]Barron’s, “More than 1000 Companies Went Public in 2021” https://www.barrons.com/articles/companies-ipos-2021-returns-worst-decade-516402948783

[3]Otka, “2020 Businesses @ Work (From Home) Report”https://www.okta.com/businesses-at-work/2020

[4]G2 Track Resources, “Shadow IT Statistics” https://track.g2.com/resources/shadow-it-statistics

[5]DoControl, “Quantifying the Immense Risk of Unmanaged SaaS Data Access” https://www.docontrol.io/resources-whitepapers/get-data-report

[6]Statista, “Leading SaaS Countries Worldwide in 2021”https://www.statista.com/statistics/1239046/top-saas-countries-list

[7]Ponemon Institute, “Cost of a Data Breach Report 2021”https://www.ibm.com/security/data-breach

[8]Verizon, “2021 Data Breach Investigations Report” https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide

[9]DoControl, “Quantifying the Immense Risk of Unmanaged SaaS Data Access”

[10]Posey and Shoss, “Exploring the Cyber Behaviors of Temporary Work-From-Home (TWFH) Employees” https://www.nsf.gov/awardsearch/showAward?AWD_ID=2030845

[11]Ponemon Institute, “2022 Cost of Insider Threats Global Report” https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

[12]Flexera, “2022 State of ITAM Report” https://info.flexera.com/ITAM-REPORT-State-of-IT-Asset-Management