Symantec.

INDUSTRY REPORT

2H 2016
Shadow Data Report

CLOUD THREAT LABS

42% PCI
of all PCI in file sharing apps is exposed

43% PII
of all PII in file sharing apps is exposed

82% PHI
of all PHI in file sharing apps is exposed

Enterprise Cloud Applications & Services Adoption, Use, and Threats

PUBLISHED BY

Cloud Threat Labs & Symantec CloudSOC™

176M
Documents

20,000+
Cloud Apps

New Data!
1.3B
Emails

About the 2H 2016 Shadow Data Report

The Shadow Data Report, published by Symantec, addresses key trends and challenges faced by enterprises securing data in cloud apps and services. Covering the second half of 2016, this report is based on the analysis of over 20K cloud apps, 176M cloud documents, and 1.3B emails. All data is anonymized and aggregated to protect Symantec CloudSOC customer confidentiality.

Cloud apps and services provide unprecedented levels of collaboration and business enablement that can empower your employees and your organization to be more productive and efficient. And they can do this while keeping your sensitive data secure – if you take steps to maintain visibility and control over the entire cloud security lifecycle.

This report is focused on the potential risks enterprises may encounter whenever they adopt insecure or non-compliant apps, implement insufficient policies around data governance, allow the accidental sharing of files, or become exposed to malicious insiders and hackers. In addition, this report covers the potential repercussions of data leakage, including compliance and mitigation costs.

Symantec.

What is Shadow Data?

Most IT experts are aware of the risk posed by Shadow IT. In the context of the cloud, it refers to the adoption and use of SaaS apps by employees and business units without the knowledge or explicit consent of an organization's IT department. Gaining visibility and control over cloud apps is a key first step in maintaining cloud security.

Shadow Data, however, poses a much greater challenge to IT's ability to prevent the loss or non-compliant exposure of sensitive corporate data.

Shadow Data comprises all of the unmanaged content that users are uploading, storing, and sharing — not only using unsanctioned cloud apps — but sanctioned ones as well. Even if an organization were to successfully limit employees to the use of enterprise-grade file sharing apps like Box or Office 365, it would not mean they have fully mitigated the risks of data loss or compliance violations. Even with sanctioned apps, it is challenging for organizations to identify and track how their users are using these apps, and what sort of sensitive data they may be uploading and sharing inappropriately. This lack of visibility into Shadow Data may result in risky exposures or compliance violations.

Executive Summary

20×

Organizations use 20 times more cloud apps than they think.

928

An enterprise has 928 cloud apps in use (average); up from 841 in the last report

66% of risky user activity in the cloud indicates attempts to exfiltrate data

13% of suspicious cloud activity indicates attempts to hack into user cloud accounts

2% of users were responsible for all data exfiltration, destruction and account takeover incidents

25% **of all files** stored in the cloud are broadly shared

of these broadly shared **3%** contain compliance related data

27% **of all emails** in the cloud are broadly shared

of these broadly shared **8%** contain compliance related data

CASB

What is Symantec CloudSOC?

Symantec CloudSOC is the leading Cloud Access Security Broker (CASB) solution designed to provide visibility, control, and protection for cloud apps and data. All stats for this report are drawn from last six months of customer activity on the CloudSOC platform. Shadow IT stats are drawn from customers using the Shadow IT Audit app, shadow data stats are drawn from customer usage of the API-based Securlets for the top cloud apps, and the threat stats are drawn from the CloudSOC Gateway threat detection solution.

Shadow IT: Perception vs. Reality

Organizations continue to use about 20 times more cloud apps than they think.

While the average CIO thinks their organization is using between 30 and 40 cloud apps and services, Symantec found that they typically have 928 apps on their extended network, most of which were adopted without IT approval or oversight. This number is up from 841 in the last Shadow Data Report.

What is Shadow IT?

In the context of the cloud, Shadow IT refers to the adoption and use of SaaS apps by employees and business units without the knowledge or explicit consent of an organization's IT department. Gaining visibility and control over cloud apps is a key first step in maintaining cloud security.

Symantec.

Top Used Apps

Symantec looked at the top 5 apps in commonly used app categories: Collaboration and File Sharing, Business Enablement, and Consumer. While enterprise and consumer apps differ greatly in their functionality and their adherence to security best practices and relevant compliance regimes, the practical distinction is becoming less relevant as consumer apps are increasingly adopted for business use, as shown below.

TOP 5 APPS BY CATEGORY, 2H 2016

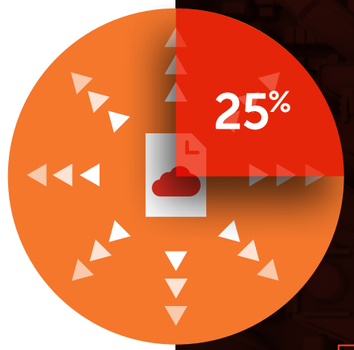
Collaboration Apps by Users	Business Enablement Apps by Users	Consumer Apps by Users
Office 365	GitHub	facebook
Google	salesforce	LinkedIn
Dropbox	zendesk	YouTube
EVERNOTE	servicenow	Twitter
box	amazon web services	Pinterest

Important note: with the exception of YouTube, all of the most popular consumer apps listed above are not Business Ready although they are used in nearly every enterprise.

Shadow Data: Threats from Oversharing

Oversharing is particularly risky when files contain sensitive data. Symantec found that of the 173M cloud-stored documents analyzed, 25% were broadly shared* and at high risk of exposure. This is up 2% from the last report, which indicates that employees are storing a growing percentage of sensitive documents in file sharing apps. The increase is small but, considering leakage of these documents can be very expensive, this is a concerning trend for businesses.

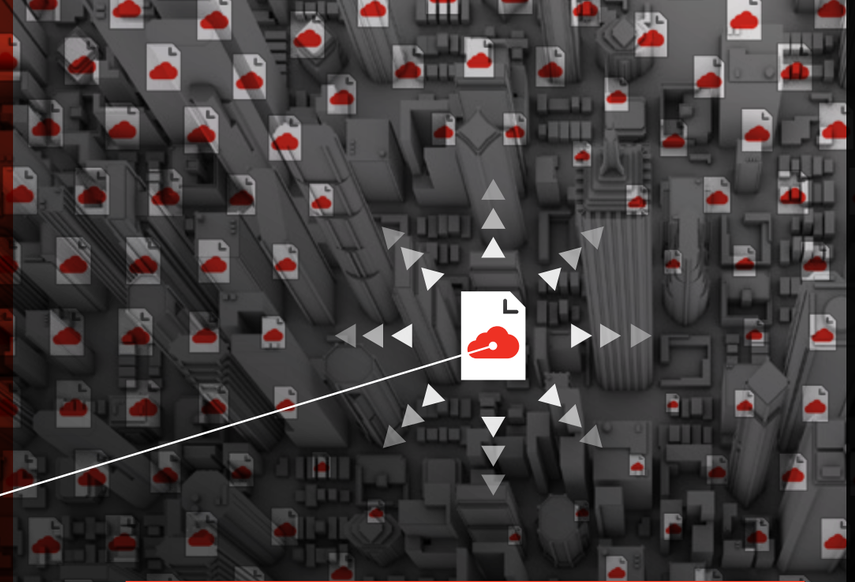
**based on analysis of over 173M files stored in popular file sharing apps such as Office 365, Dropbox, Box, and Google Drive as well as services such as Salesforce, OKTA, AWS and Jive.*



BROADLY SHARED
= High Risk of Exposure

Broadly shared refers to documents that are widely shared with employees within the organization, documents that have been shared externally with specific individuals such as contractors and partners, and documents shared to the public.

25% of all Shadow Data stored in the cloud is broadly shared*



SHARED WIDELY

all employees within the organization can access

SHARED EXTERNALLY

specific individuals or groups such as contractors, partners, or clients

SHARED PUBLICLY

anyone with a link can access or hackers can easily mine from the web

CASE STUDY

78,000 Overexposed Files

A leading US auto and home insurance provider underwent a Symantec Shadow Data Risk Assessment on their Box account and found they had 78K overexposed files.

Of these, 31K of were at high risk due to being shared publicly, and many contained Protected Health Information (PHI), the leakage of which could have resulted in serious HIPAA violations and the resultant fines. Through the use of CloudSOC, they were able to remediate overly exposed files that contained sensitive data, including PHI, by automatically updating permissions to allow access only to internal employees. In addition, through the use of the detailed audit trail captured by CloudSOC, they were able to determine that no overly exposed data had been inappropriately accessed, therefore eliminating the need for additional investigation. This remediation made a significant improvement in their cloud risk profile.

The Added Risk of Exposing Compliance Related Data

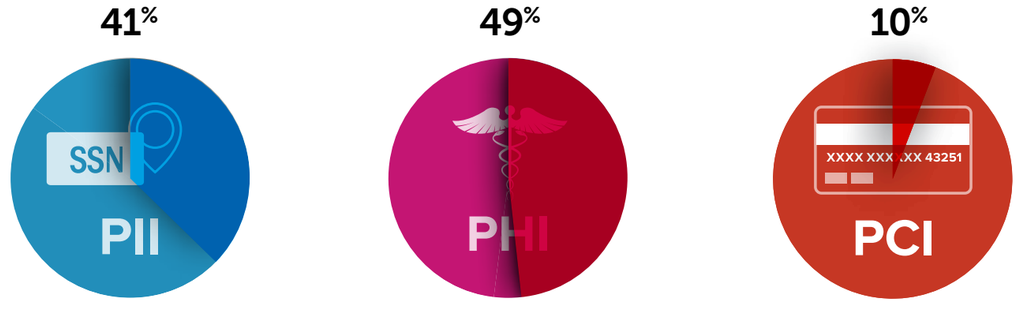
It is interesting to note that 3% of broadly shared documents contain compliance related data, including PII, PCI and PHI. This is down from the 12% identified in the last report. It indicates that the organizations included in this report are improving their security over time and educating their users on the secure use of cloud apps.

What is considered sensitive data?

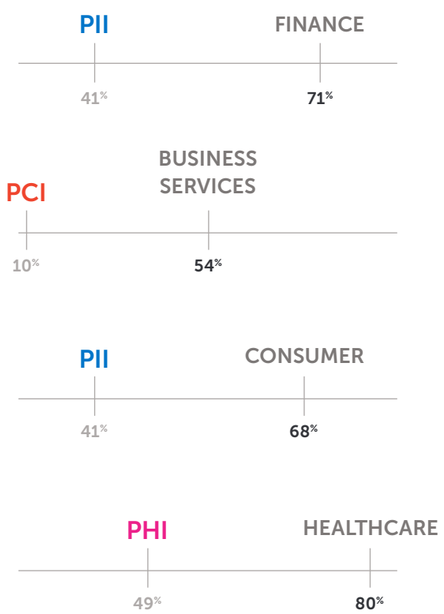
Not all documents stored in file sharing apps are sensitive. The majority are innocuous business files such as meeting notes, non-business critical files, etc. For the purposes of this report, we focus on the most sensitive data types:

Personally Identifiable Information (PII) **Protected Health Information (PHI)** **Payment Card Information (PCI)**

If we look across all industries, we find that of the 3% of broadly shared files that do contain sensitive data, the distribution is as follows:



INDUSTRY DEVIATIONS



Broken down by industry, a few expected deviations are apparent.

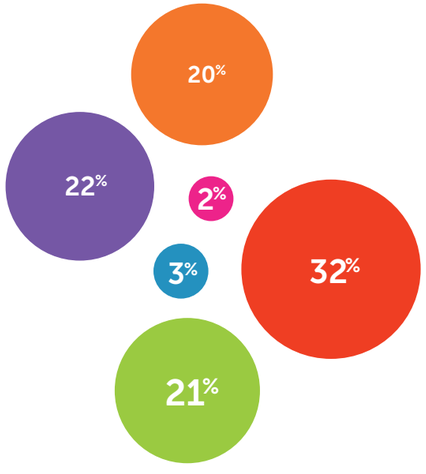
Looking at the data in another way, if we calculate the percentage of compliance related data exposed, we find:

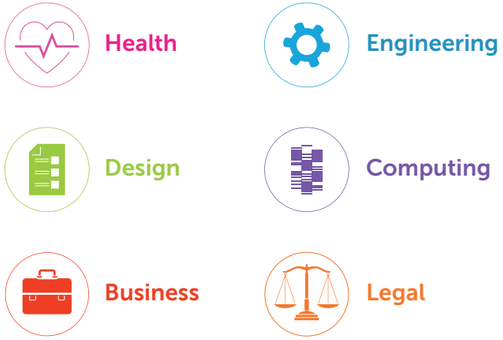
43% of all PII in file sharing apps **is exposed**

42% of all PCI in file sharing apps **is exposed**

82% of all PHI in file sharing apps **is exposed**

These statistics are quite alarming, especially with the vast majority of high value PHI being overexposed.



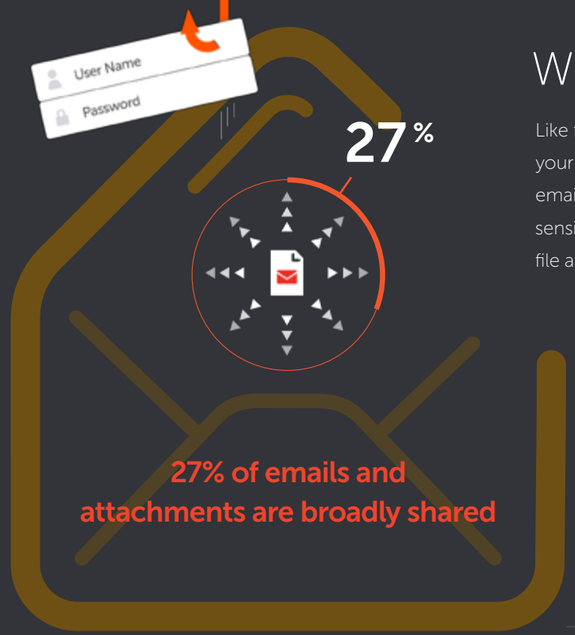


Data Science Powered™ CloudSOC ContentIQ Engine

Symantec uses machine learning and advanced computational linguistics for content analysis, not just regular expression matching, to more accurately classify documents by compliance type (PII, PHI, PCI) as well as category types such as legal, human resources, finance, source code, etc.

Potentially Sensitive Data Also Broadly Shared

In addition to compliance related files and source code, organizations also want to classify and manage broad categories of documents, such as legal, business, computing, and health related files. The distribution across all industries is as follows:



What about Email Threats?

Like file sharing apps which have introduced new opportunities for your sensitive data to be exposed, leaked, or destroyed, cloud based email services can also put this data at risk. Compliance or otherwise sensitive corporate data is often found in the body of an email and in file attachments.

Symantec found that 27% of emails and attachments are broadly shared and therefore at risk of leakage. This percentage is the same as for files shared in file sharing apps. However, 8% of emails, as opposed to 3% of documents in file sharing apps, contain compliance related data. That suggests that while employees are learning to be more cautious about sharing sensitive files in the cloud, they are less aware of the risks of oversharing and sending compliance related data through email.

Threats from Malicious Employees & Hackers

67% of risky user activity in the cloud indicates attempts to exfiltrate data

13% of suspicious cloud activity indicates attempts to hack into user cloud accounts

All organizations included in this report have experienced a minor security incident in the last year. However, according to the Symantec cloud threat detection team, 16% of organizations have shown indications that one or more potentially serious security incidents occurred during that time. Of the common, most destructive activities, three stand out. Anomalous frequent sharing accounts for 38% of these, followed by anomalous frequent downloads at 23%—both of which indicate exfiltration attempts. Combined, they constitute 61% of the most destructive incidents.

Symantec.

What is considered a security incident?

Security incidents can be broadly categorized as data exfiltration, data destruction, and account takeovers by hackers. Elastica tracks dozens of cloud activities within these three categories, but the most critical of these are as follows:

DATA EXFILTRATION

- Anomalous frequent file previews
- Anomalous frequent file downloads
- Anomalous frequent emails sent
- Anomalous frequent file sharing

DATA DESTRUCTION

- Anomalous frequent file edits
- Anomalous frequent file deletions

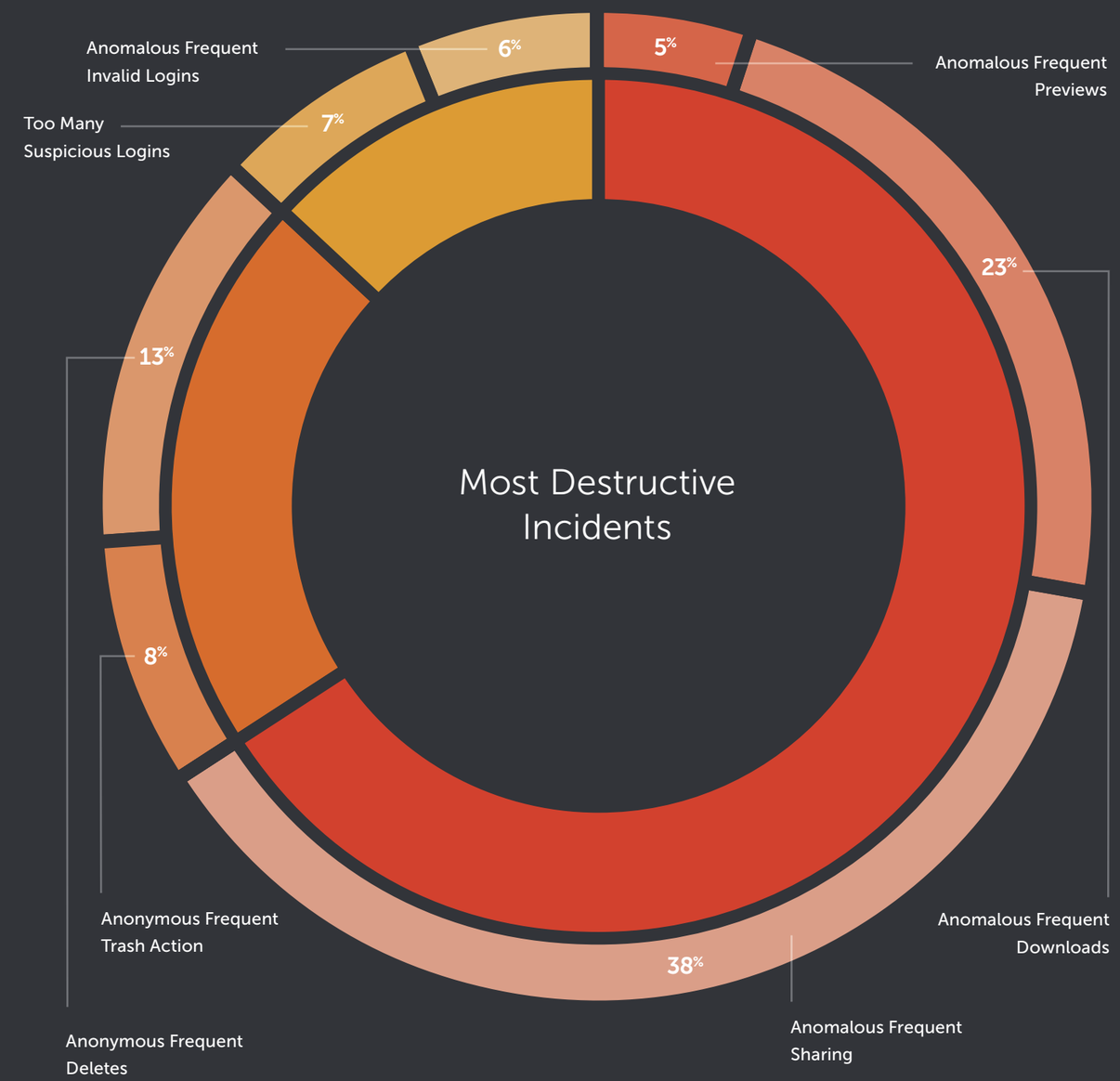
ACCOUNT TAKEOVER

- Anomalous frequent account logins
- Too many suspicious account logins

ACCOUNT TAKEOVER ATTEMPTS **13%**

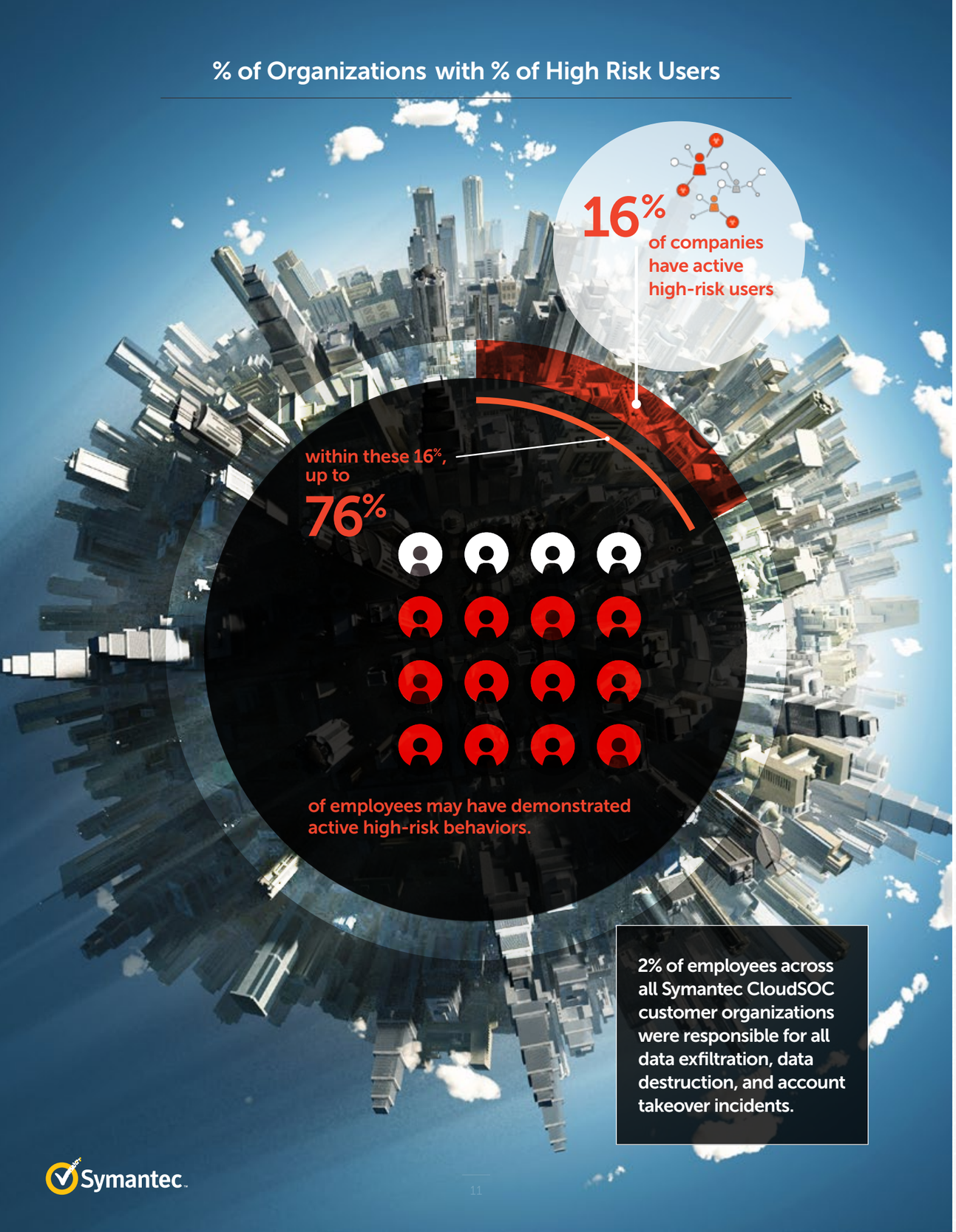
DESTRUCTION ATTEMPTS **21%**

EXFILTRATION ATTEMPTS **66%**



Anomalous frequent previews is also of note as it indicates a malicious user may be taking screenshots of rapidly previewed documents to exfiltrate data—a threat vector that is often overlooked.

% of Organizations with % of High Risk Users



2% of employees across all Symantec CloudSOC customer organizations were responsible for all data exfiltration, data destruction, and account takeover incidents.

Who is exhibiting this risky behavior?

The good and bad news is that high risk users are concentrated, as mentioned earlier, in 16% of companies. If you are among the 84% of companies that currently have no users performing high-risk activities, then the risk to your business is reduced, though not eliminated. But, if you happen to be one of the 16% of companies with active high-risk users, up to 76% of your employees may have demonstrated high risk activity. Please note that the population of data examined in this report comes from organizations who have already demonstrated a higher commitment than average to secure themselves against cloud risks. These risk statistics could easily be higher for businesses who haven't adopted cloud security that identifies suspicious user behavior, and haven't used that information to educate their users on safe cloud usage.

An astonishing 9.7% of all organizations have 10% or more of their employees who are high risk users.

Identifying Threats — Is there malicious activity going on?

Symantec takes a multilayered data science approach to identifying malicious cloud related activity, leveraging machine learning and computational analysis to detect suspicious user behavior. Symantec determines the relative risk of each cloud app user. This individualized risk profile updates dynamically and can provide early identification of malicious insiders or compromised user endpoints and accounts. Automated policy controls can be set to trigger when a user passes certain thresholds for very fast response.

Cost of a Typical Data Breach

Healthcare and Telecom face the highest financial risk from leakage of sensitive cloud data.

Symantec calculated that the potential financial impact on the average organization from the leakage of all of an organization's sensitive cloud data was just over $4.2M. The cost by industry varies substantially, however.

Telecom	$13.7M
Healthcare	$5.4M
Consumer	$2.2M
Business Services	$1.7M
Education	$1.3M
Financial	$1.1M
Technology	$412K

Symantec.

Conclusion

Knowledge is power

As shown in this report, threats to your data abound in the cloud, but they are manageable. Whether it is risky apps, risky users, or insufficient data governance policies, chances are your organization is exposed to possible compliance violations or remediation costs. To keep you secure in the cloud, Symantec recommends the following best practices:

Know your organization

Develop a comprehensive cloud governance strategy. What are your guidelines for approving/blocking cloud vendors? Do you have guidelines on acceptable cloud application use by department and role? What is your data loss prevention policy that defines the types of sensitive data you have as a company and their relative risk if exposed? What is your process for responding to Incidents when they occur?

Know your cloud apps

Determine which cloud apps your employees are adopting and using. Then identify which are business ready and satisfy your specific security requirements, and which have insufficient security controls and must be blocked or replaced with more secure alternatives.

Know your cloud users

Understand how your employees are sharing and collaborating using cloud apps. Are they disciplined about limiting sharing to relevant contacts, or are they sharing indiscriminately? Have they committed a risky exploit such as data exfiltration and, if so, how much risk do they pose to your organization going forward?

Know your cloud data

Understand what data your employees are storing and sharing in the cloud. Does a document contain PHI? PII? Source Code? Accurately classifying your data and setting corporate usage policies around it is critical to avoid data leakage.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

CLOUD THREAT LABS

provides in-depth information and security insights of advanced threats to SaaS apps, including cloud storage services such as Google Drive, Box, Office 365, and Dropbox.

1-650-527-8000

cloudsecurity@symantec.com